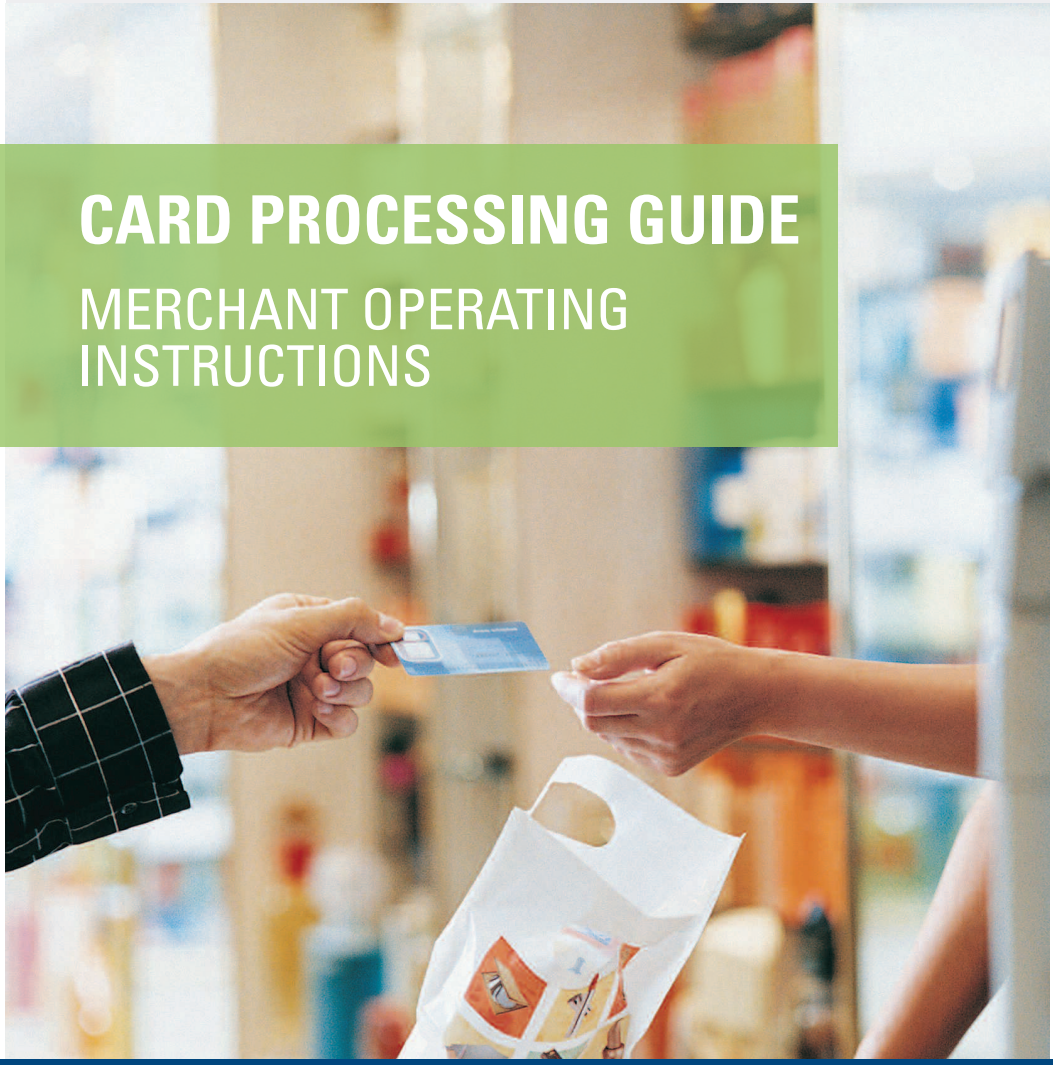
globalpayments

CARD PROCESSING GUIDE

MERCHANT OPERATING INSTRUCTIONS



SERVICE. DRIVEN. COMMERCE

globalpayments

CONTENTS

SECTION	PAGE
Welcome	**1**
Global Payments	1
About This Document	1
An Introduction To Card Processing	**3**
The Anatomy Of A Card Payment	3
Transaction Types	4
Risk Awareness	4
Card Present (CP) Transactions	**9**
Cardholder Verified By PIN	9
Cardholder Verified By Signature	9
Cardholder Verified By PIN And Signature	9
Contactless Card Payments	10
Checking Cards	10
Examples Of Card Logos	13
Examples Of Cards And Card Features	14
Accepting Cards Using An Electronic Terminal	18
Authorisation	19
'Code 10' Calls	24
Account Verification/Status Checks	25
Recovered Cards	26
Refunds	27
How To Submit Your Electronic Terminal Transactions	29
Using Fallback Paper Vouchers	30
Card Not Present (CNP) Transactions	**33**
Accepting Mail And Telephone Orders	33
Accepting Internet Orders	34
Authorisation Of CNP Transactions	36
Confirming CNP Orders	38
Delivering Goods	39
Collection Of Goods	39
Special Transaction Types	**40**
Bureau de Change	40
Dynamic Currency Conversion (DCC)	41
Foreign Currency Transactions	41
Gratuities	42
Hotel And Car Rental Transactions	42
Prepayments/Deposits/Instalments	44
Purchase With Cashback	44
Recurring Transactions	45
Global Iris	**48**
HomeCurrencyPay	**50**
An Introduction To HomeCurrencyPay	50

globalpayments

SECTION	PAGE
Card Present (CP) HomeCurrencyPay Transactions	51
Mail Order And Telephone Order (MOTO) HomeCurrencyPay Transactions	53
Ecommerce HomeCurrencyPay Transactions	56
MasterCard And Visa Regulations	57
Refunds	58
Hotel And Car Rental Transactions	59
Frequently Asked Questions	59
Credits And Debits To Your Bank Account	**63**
Credits To Your Bank Account	63
Rejected Transactions	64
Service Charges	65
Reconciliation	65
Understanding Your Invoice	65
Chargebacks	**66**
Introduction	66
What Is A Retrieval Request?	66
How To Prevent Chargebacks	67
Data Security	**71**
Payment Card Industry Data Security Standard (PCI DSS)	71
Best Practices	71
What You Need To Do	72
Introducing Global Fortress – Level 4 Merchants	73
Level 1, 2 And 3 Merchants	74
Third Party Companies	74
What Happens If You Don't Become Compliant?	74
If You Suspect A Security Breach	75
How To Reduce Fraud	**76**
Types Of Fraud To Look Out For	76
How Can I Protect My Business?	79
Global Iris Integrated Fraud Prevention Tools	83
Additional Important Information	**84**
Keeping You Informed	84
Stationery	84
Tally Rolls For Electronic Terminals	84
Producing Your Own Advertising	85
How To End The Card Processing Agreement	85
How To Contact Us	**86**
Global Payments Helpdesk	86
Our Authorisation Service	87
If You Want To Complain	87

WELCOME

Welcome to Global Payments Card Processing, which has one simple aim… to provide you with a safe and secure service that represents very real value for money for your business.

This means working hand-in-hand with you.

We listen carefully to what you tell us about your needs in order to help us develop a thorough understanding of your business. We'll strive to work with you in a way that's professional, transparent and fair, including explaining how to comment on our service.

GLOBAL PAYMENTS

Global Payments is a trading name of GPUK LLP, which is one of the UK's largest card processing providers and is a wholly-owned subsidiary of Global Payments Inc.

Global Payments Inc. (NYSE: GPN) is a leading worldwide provider of payment technology services that delivers innovative solutions driven by customer needs globally. Our partnerships, technologies and employee expertise enable us to provide a broad range of products and services that allow our customers to accept all payment types across a variety of distribution channels in many markets around the world.

Headquartered in Atlanta, Georgia USA with more than 4,300 employees worldwide, Global Payments is a Fortune 1000 Company with merchants and partners in 29 countries throughout North America, Europe, the Asia-Pacific region and Brazil. We've access to local/regional markets in over 40 countries in Europe and Asia and offer transactional sales in 140 currencies. We process more than 6 billion transactions every year, totalling over $350 billion annually and over 15,000 new customers join us every year.

In the UK, Global Payments is HSBC Bank plc's preferred strategic partner for card processing and together have an exclusive UK Marketing Alliance Agreement.

ABOUT THIS DOCUMENT

This *Merchant Operating Instructions*, together with the other documents listed in clause 1 of the *Terms of Service*, constitutes the Card Processing Agreement you're making with us (the "Agreement").

For your own benefit and protection you should read this document carefully as it forms part of your Agreement upon which we intend to rely. If you don't understand any point, please ask for further information. See page 86 for our contact details.

If you accept card types that you hold a direct agreement with the card issuer to process, for example, you may have a separate contract with American Express, then acceptance of these cards are subject to the terms and conditions of that card issuer as well as our Agreement.

What Do These Merchant Operating Instructions Tell You?

These instructions provide you with:

- an overview of the various ways in which we can support your business
- information on how we credit you and other operational instructions
- critical information about the risks associated with cards as a method of payment and highlights some vital steps that you should follow to help raise your awareness and minimise your exposure to these risks
- a guide enabling you to effectively accept card transactions so that you'll benefit from your new card processing facility.

Please read this document carefully as it contains critical information to help you avoid fraud.

You should also keep a copy of these *Merchant Operating Instructions* somewhere convenient so that you and your employees can easily access them when required, but **where customers or any other parties cannot access them**. If you cannot find the information you need please contact us (see page 86 for our contact details).

Please Keep Us Informed If Your Business Changes

There are risks involved with card processing and we feel that it's our duty to ensure that you're aware of these risks. We'll keep you informed of developments in the industry, including trends in fraudulent activity and advances in anti-fraud processes and technology. This will help you maintain your security at the highest level and reduce the potential risk to your business.

To ensure we can keep you informed and ensure you're receiving the services appropriate to your situation, please let us know if any of your business details change, such as:

- your contact details (including email address or telephone number);
- your address (including your trading address, correspondence address, head office address etc.);
- the type of business being conducted by you;
- significant changes in the volume of business you're experiencing;
- you intend to change the way you conduct business, for example, starting to trade on the internet or start using a new Payment Service Provider (PSP);
- change in significant shareholding (usually defined as 25% or more); or
- you sell your business or change its legal entity.

To advise us of any of the changes listed above or others, please call our helpdesk (see page 86).

Please Contact Us If You Have Any Questions Or Feedback

Our aim is to provide you with the highest possible level of service. As such, we welcome all your comments and feedback. Please feel free to get in touch if you have any questions or comments about these instructions, or any aspects of the card processing service we provide. See page 86 for our contact details.

AN INTRODUCTION TO CARD PROCESSING

Global Payments will work hand in hand with you to find the card processing solution that fits your business and provides a quality service at the right price.

You're able to choose from an extensive range of card processing solutions to increase your revenue, reduce your costs and minimise fraud, all of which are supported by first-class, personalised customer service.

THE ANATOMY OF A CARD PAYMENT

To help you understand card processing, we've broken down the process into easy to follow steps from taking a card transaction in a face to face sales environment, to receiving the funds for that transaction. This will help you see what happens in the background to make a card payment work. We will explain this in more detail throughout this document.

Purchase

1. Your customer places their card in your card terminal and enters their PIN to verify the transaction.
2. While the purchase is processed, usually in seconds, we send a message to the Card Scheme of the card (for example, MasterCard or Visa) to authorise the payment with your customer's card issuer.
3. Your customer's card issuer checks the card's security features, your customer's credit limit and looks to see if the card has been reported lost or stolen.
4. The card issuer approves the purchase, advised to you through the terminal by providing the authorisation code.
5. The purchase is complete and your customer receives a receipt.

End Of Day

1. You perform your end of day routine on your terminal.
2. All authorised purchases are batched and automatically sent to us for processing.

Clearing

1. We sort your batch into the different Card Schemes, for example, MasterCard, Visa.
2. We send your sorted transactions to the relevant Card Scheme for processing.
3. The Card Schemes forward the transactions to your customers' card issuers.
4. The transactions are debited to your customers' accounts.

Funding

1. We receive payment from the Card Schemes for the transactions we have sent for processing.
2. We create a payment for the transactions you have taken.
3. We send the payment to your bank.
4. Your bank account is credited for your transactions.

TRANSACTION TYPES

Card processing enables you to accept card payments from your customers in a number of environments and can be broadly split into two groups of transaction types:

Card Present (CP) transactions, which means any transaction where the card or Contactless payment device (see page 10) and the cardholder are physically present at the time of the transaction and where you can evidence the presence of the card tendered either by chip read or card swipe or tap on an electronic terminal and includes the following types of transaction:

- sale transactions for the sale of goods or services (see page 9)
- purchase with cashback (debit card only) – transactions for the sale of goods or services together with the provision of cash (see page 44).

Card Not Present (CNP) transactions, which means any transaction where the card and cardholder aren't physically present at the time of the transaction and includes the following types of transaction:

- mail/telephone sale transactions conducted by post telephone or any other similar form of communication (see page 33)
- internet sale transactions via computer networks including the internet (see page 34)
- recurring transactions (certain card types only), where the cardholder gives you authority to charge fixed or varying amounts at intervals (whether specified or not) to his/her card and includes subscriptions, membership renewals and regular premiums (see page 45).

Some transactions can be either CP or CNP transactions. These include the following types of transaction:

- pre-payments/deposits – transactions where the whole value or part value of the transaction is made prior to the provision of goods or services (see page 44)
- Instalments – three or more payments toward a single purchase (see page 44)
- currency – transactions in any currency other than sterling (see page 41)
- refunds – a refund of a sale you've previously undertaken (see page 27)
- bureau de change – transactions under which you provide foreign currency or travellers cheques to cardholders (see page 40)
- dynamic currency conversion payments (DCC) – allows you to offer your non-UK cardholders the ability to purchase goods in their home billing currency. Our DCC service is called HomeCurrencyPay (see page 41)
- card activated transactions – transactions through a Cardholder Activated Terminal (CAT) operated by the cardholder independently of you
- status checks (zero value) – allowing you to validate a customer's account (see page 25).

Note: Some transaction types cannot be performed on all card types or on certain terminal types.

Your *Service Schedule* details the transaction types and card types you're authorised to accept. You must have our written authority before you can process any other transaction types or accept any other card types that don't appear.

RISK AWARENESS

We want your business to accept cards without problems, however, it's vital that you're aware of, and understand, the risks associated with accepting cards.

Chargebacks

One such risk is a chargeback, which is an unpaid card transaction that has been returned to us by the card issuer. We may debit the chargeback to your account, however, this section highlights some of the ways you can minimise the risk of chargebacks to your business.

There's no guarantee of payment for any transaction, even if you obtained authorisation. Authorisation checks that at the time of the transaction, the card isn't reported lost or stolen and that the genuine cardholder has sufficient funds available. Authorisation cannot verify that the genuine cardholder is conducting the transaction.

Note: Never spread the value of the sale over more than one card, or split the sale into smaller amounts to achieve a successful authorisation. This is prohibited. This is not to be confused with splitting the sale between multiple cardholders, for example, when paying for a meal. This isn't prohibited.

CP Transactions

CP transactions can be accepted and verified in a variety of ways, including:

- Chip and PIN
- Chip and signature
- Contactless
- Magnetic stripe and PIN
- Magnetic stripe and signature.

The best way to minimise the risk of CP chargebacks is to carefully follow the prompts provided by your terminal. If the terminal authorises a payment and prompts the cardholder to sign, then this should be allowed, subject to the normal checks associated with a signature-verified transaction (refer to 'Checking Cards' on page 10).

Your terminal will automatically seek authorisation of the transaction depending on the floor limit set in the card by the card issuer and method of acceptance, for example, magnetic stripe verified by signature. However, if you're using Fallback paper vouchers due to a terminal fault, power failure etc., you must obtain a telephone authorisation for each transaction. Refer to 'Authorisation' on page 19.

Note: Paper vouchers cannot be used as Fallback if a Mobile POS Solution fails. You must ask the cardholder for an alternative means of payment.

Chip And PIN Transactions: Chip and PIN cards and terminals have made substantial advances in preventing card fraud and are now the norm. All CP transactions must be completed using a chip and PIN terminal when presented with a chip and PIN card.

When your electronic terminal is unable to read the chip, it will prompt you to revert to the magnetic stripe on the card.

Contactless Transactions: Where your terminal is enabled to accept Contactless payments, the Contactless symbol will be displayed for low value transactions. The cardholder simply taps their card to the reader to make the payment. If the card or the terminal aren't enabled for Contactless, or the cardholder prefers to use the chip and PIN functionality, then the transaction can be

completed via chip and PIN by inserting the card into the card reader.

From time to time your terminal may request that a PIN transaction is completed instead of a Contactless one. This is an added security feature, designed to confirm that the cardholder is in possession of their card and you must continue with a chip and PIN transaction in the usual way.

For more information on Contactless, refer to 'Contactless Card Payments' on page 10.

Magnetic Stripe Transactions: There are still many legitimate cards in circulation that contain no chip and you'll have to swipe the magnetic stripe. You may then have to use the cardholder's signature to verify the transaction, subject to the normal checks (refer to 'Checking Cards' on page 10).

When using the magnetic stripe as a result of problems with the chip, pay particular attention to these transactions as the chip could have deliberately been interfered with to avoid validation via the PIN. Check if there has been any visible attempt to remove, replace or damage it.

Key-entered Transactions: When the cardholder is present, and the electronic terminal cannot read the card via the chip or magnetic stripe, then you may key-enter the details into your terminal. You must still seek online authorisation.

Note: This option isn't permitted for Maestro or UnionPay card transactions and you should ask the cardholder for an alternative method of payment.

To prove the card was present, always take an imprint of the card using your manual imprinter, complete the voucher in full and obtain the cardholder's signature on the paper voucher. This is in addition to key-entering the card details into the electronic terminal. You'll automatically be credited for key-entered transactions on your terminal, so you must not submit the paper voucher for processing. Retain the signed voucher securely for five years along with the terminal receipt so that it can be produced as proof that the card was present when the transaction was undertaken, should it be required.

Note: While taking an imprint of the card will help minimise your risk of financial loss, if a chip and PIN card is accepted using this method and the transaction turns out to be fraudulent, you'll be liable for a chargeback and financial loss to your business. In this scenario, you may wish to ask for an alternative method of payment.

CNP Transactions

These situations are ideal for fraudsters because the card, signature and personal identification number (PIN) cannot be checked as you, the card, and the cardholder are not all present together. The majority of chargebacks result from transactions being undertaken fraudulently. If you proceed with a transaction that you're unsure of, you're doing so at your own risk. If the transaction has been completed, but the goods not despatched, you're still in a position to carry out a refund. Refer to page 33 for further information on CNP.

To minimise your risks:

- Be cautious of customers who give mobile phone numbers as their only form of contact.
- Be wary of an order emanating from an email account where the customer's name isn't reflected in the email account address.

- Be suspicious with transactions that have an unusually high value or volume for your type of business or the sale is 'too easy'. In our experience these are the more likely ones to be fraudulent.
- When performing a refund, always refund to the same card used for the original transaction.
- Keep a database of chargeback history to help identify patterns of fraudulent transactions. If a sale seems too good to be true then it probably is. Don't be afraid to contact the cardholder to ask further questions or request additional identification. A genuine customer should be pleased you're security minded and trying to protect them from fraud.
- Where possible, perform Address Verification Service (AVS) and Card Security Code (CSC) checks (see page 80). Refer to your terminal manual or terminal supplier for assistance on using this security feature. Remember that you're not allowed to store the CSC data.
- For ecommerce transactions, an additional layer of security can be incorporated into websites. MasterCard SecureCode and Verified by Visa (VbV) have been developed to allow customers to authenticate themselves as the genuine cardholder (see page 80). **To accept Maestro cards over the internet, you must support MasterCard SecureCode.**
- Always send goods by recorded or special delivery or by a reputable security carrier. Insist on a signed (preferably by the cardholder) and dated delivery note. Tell the courier not to make the delivery if the premises appear to be vacant. Please note that proof of delivery alone isn't sufficient evidence to defend a chargeback.
- Don't release goods to third parties such as taxi drivers and messengers.
- Be cautious of transactions where the billing address is different to the requested delivery address. Avoid delivering to addresses other than the cardholder's, such as hotels, internet cafes and 'care of' addresses.
- Be wary of requests for next-day delivery, requests to alter the delivery address at short notice, or telephone calls on the day of delivery requesting a specific delivery time.
- If a customer requests to collect the goods, perform the transaction at the time of collection through your point of sale equipment.

Please see page 79 for further information on how to protect your business.

Note: You risk receiving a chargeback if the transaction is successfully disputed. We may debit the value of the transaction to your business. If you're at all suspicious, make a 'Code 10' authorisation call (see page 24).

Remember authorisation is not a guarantee of payment (see 'Authorisation' on page 19).

Copies Of Sales Vouchers

We may request copies of sales vouchers at any time. Please respond immediately to any such request as failure to do so may result in a chargeback. Always retain a copy securely for your own records. Please note that you should retain all transaction vouchers for five years following the delivery of goods or completion of the service provided (see page 71 regarding security of data).

Processing Third Party Transactions

Processing transactions on behalf of another business can severely damage your financial wellbeing. If you're either offered a lump sum for allowing unlimited access and usage of your card processing facility or a commission for each payment you process, be wary that it's very rare for the third party to deliver the service that was promised. Often these entities, whilst appearing to be genuine and providing plausible reasons for requiring assistance, are fronts for organised

criminal gangs engaged in timeshare or ticketing scams.

You must **never** accept transactions on this basis. These transactions are usually disputed or fraudulent, and could result in chargebacks and financial losses to your business. Should this be the case you'll be fully liable for reimbursing the cardholders where non-provision of the goods or services has occurred.

Third party processing also breaches your Card Processing Agreement with us, and identification of such activity may result in immediate suspension and eventual termination of your card processing facility. This type of processing can also lead to criminal proceedings.

If a third party approaches you, or your staff, to process their transactions, say no and contact us straight away with as much detail as possible. If you feel your business may have already succumbed to such a deception, or has recently received an approach, then please call us immediately for assistance with as much information as possible so that we can take appropriate action.

Terminals

Whether you rent a terminal from Global Payments or not, you're responsible for the terminal equipment and we strongly recommend that due consideration is given to the positioning and control of such equipment. You'll be responsible for any losses resulting from interference by third parties not authorised to manipulate the equipment in any way other than in the normal course of the transaction, for example, entering a PIN. Therefore, please consider the length of time you give to the cardholder to input their PIN details.

Note: Ensure that any surveillance equipment you have isn't able to record a cardholder entering their PIN.

Data Security

Security of personal data is a growing concern. Criminals are always looking at ways of getting this type of information from different sources. A vulnerable point of compromise which fraudsters have identified is card financial data which has been collected during the acceptance of cards. The Payment Card Industry Data Security Standard (PCI DSS) is a global mandated standard which has been introduced by the Card Schemes to bring a greater level of security to this type of data.

As you're accepting card transactions, you need to be aware of the value of the data you collect when undertaking a card transaction and the need to secure it. If you were to suffer a security breach, there's a significant risk of financial and reputational loss to your business.

Note: Under your Card Processing Agreement with us, you're required to achieve and maintain PCI DSS compliance.

For further details on PCI DSS, please go to page 71 or you can visit www.pcisecuritystandards.org. This site holds the latest version of the PCI DSS specifications and guidance on how to become compliant.

CARD PRESENT (CP) TRANSACTIONS

Card Present (CP) transactions are any transaction where the card and cardholder are physically present with you at the time of the transaction and where you can evidence the presence of the card tendered through an electronic terminal.

CP transactions can be accepted and verified in a variety of ways, including:

- Chip and PIN
- Chip and signature
- Contactless
- Magnetic stripe and PIN
- Magnetic stripe and signature.

Your terminal will provide prompts to tell you what you should do.

CARDHOLDER VERIFIED BY PIN

Depending on your terminal type, either you or the cardholder will insert the card into the terminal's card reader or PIN pad.

The requirement to undertake physical and visual validation checks on the card will depend upon whether you actually handle the card at any time during the transaction. If you do handle the card, then you must follow the procedures detailed in 'Checking Cards' on page 10. However, there's no need to obtain a customer signature on the terminal receipt or voucher.

CARDHOLDER VERIFIED BY SIGNATURE

There are certain circumstances when the identity of the cardholder cannot be verified by the use of a PIN. These include:

- a card with no chip (for example a magnetic stripe card). which must be swiped through an electronic terminal
- a chip card that doesn't use the PIN as its verification method.

In these circumstances the cardholder won't be prompted to enter a PIN, instead the cardholder must be verified by their signature. As you'll be handling the cards you'll be required to undertake the physical and visual validation checks detailed in 'Checking Cards' on page 10.

Note: Most Discover Global Network and other internationally issued cards are magnetic stripe cards. However, some Discover Global Network cards are now issued with a chip. If you're presented with one of these cards, you should process it in the same way as any other chip and PIN transaction.

CARDHOLDER VERIFIED BY PIN AND SIGNATURE

There are some cards that while they are magnetic stripe cards requiring a signature verification, they may require a PIN to verify them as well. For example, UnionPay cards are magnetic stripe but in most cases, also require an online 6 digit PIN as well as a signature.

Note: Some UnionPay cards are now issued with a chip. If you're presented with one of these

cards, you should process it in the same way as any other chip and PIN transaction.

CONTACTLESS CARD PAYMENTS

Contactless card payments allow low value transactions to be made without the need for the card to be inserted into the card reader or swiped. A Contactless reader is required to process these payments, which may be a separate reader or integrated into your electronic terminal.

Note: A Contactless reader is not available with a Mobile POS Solution.

Special technology is incorporated into a card to enable it to work in a Contactless environment. Ordinary magnetic stripe and chip and PIN cards won't work with a Contactless reader. In general, if the card displays the following symbol on the front or back of the card, it will incorporate the Contactless technology.

The current Contactless payment limit can be found on our website at:

https://www.globalpaymentsinc.co.uk/terminals-contactless.html.

Although a PIN isn't required for a Contactless card payment, from time to time your terminal will request that a PIN transaction is completed instead of a Contactless one. This is an added security feature, designed to confirm that the cardholder is in possession of their card and you must continue with a chip and PIN transaction in the usual way.

Contactless technology can also be embedded into other devices, for example, smart watches, wristbands, smart phones, tablets and key fobs. Please note, smart phones, tablets and smart watches provide the ability to make higher value payments (above the existing Contactless limit) via the use of a security code or other means, for example, finger print recognition, on the cardholder's device.

Note: Discover Global Network and UnionPay cards cannot currently be accepted via Contactless.

CHECKING CARDS

The type of card will determine which validation checks are needed.

How To Perform Card Validation Checks

There are many different designs of credit and debit cards. Please see the following section for some examples of card types. The validation checks listed below apply to the majority of cards issued by any bank or other financial institution. Failure to follow these checks may result in you being subject to a chargeback:

1. Chip

- If there's a chip on the card, check if there has been any visible attempt to remove, replace or damage it.

2. Card Number

  - The cardholder account number begins with:
  - 2 or 5 for MasterCard, Maestro cards can also begin with a 6
  - 4 for Visa
  - 36 for Diners Club International cards
  - 6011, 64 and 65 for Discover cards
  - 65 for BC Card, DinaCard and RuPay
  - 6 for standard UnionPay debit and credit cards. For cards dual branded with MasterCard the account number may begin with a 5 and for those dual branded with Visa the number may begin with a 4
- account numbers are generally 16 to 19 digits long, however, some can be shorter. For example, Diners Club International cards are 14 digits long and UnionPay debit cards are 13 to 19 digits long. All other UnionPay card types are 16 digits long
- the first four digits of the account number may be repeated above or below the beginning of the embossed card number – make sure they match the first four digits of the embossed number if they're present
- the last four digits of the card number on the front of the card must match the number on the reverse on the signature strip, if present, and also the last four digits of the card number printed on the terminal receipt
- for embossed cards, check the numbers. If the area around these is distorted, the original numbers may have been flattened and fake numbers added
- the account number on the front of the card may be printed rather than embossed, and so feels smooth rather than raised. Whether cards are embossed or not, Visa Electron, Maestro, V PAY, Discover Global Network and UnionPay cards cannot be accepted using paper vouchers
- if the card states 'Electronic Use Only' it cannot be accepted using paper vouchers.

3. Cardholder Title And Name

- Check for obvious discrepancies between the cardholder and card, such as a woman using a card with the title 'Mr', or a teenager using a card with the title 'Doctor' or 'Sir'
- some cards include a photograph of the cardholder. You must check that the photograph matches the person presenting the card and that it has not been tampered with.

4. Valid From/Expiry Dates/Valid Thru

- The card should be carefully examined for the effective validity date. You must not accept cards presented before their 'valid from' date (where shown) or after their expiry/valid thru date. The terminal will perform certain checks on the card, but we cannot be held liable if the terminal accepts a pre-valid or expired card.

5. Hologram

- Check that it has not been tampered with. The hologram should be smooth to the touch, should not have a rough or scratched surface and the 3D image should move when tilted. Counterfeit cards often feature poor hologram reproductions
- the hologram can be on the front or back of the card unless a Holomag tape (holographic magnetic stripe) is used in place of the traditional magnetic stripe

- the most common designs are:
  - MasterCard - the world
  - Visa - a dove, which appears to fly
  - Visa Electron - not all cards contain a hologram. When present, the hologram will appear as a flying dove
  - UnionPay – UnionPay issued credit and debit cards have a 3D image of the Temple of Heaven on a background of two-coloured wording that says 'bankcard interoperability' in Chinese arranged in rows. A magnifier is on the top left and a stamp of 'UnionPay' in Chinese characters is on the top right. Dual branded cards have the hologram image of MasterCard or Visa as detailed above.

6. Signature Strip

- The signature should be written clearly and be smooth to the touch. Be suspicious if the card isn't signed, if the signature appears to have been erased, if the card appears to have been re-signed, or if the signature is written in block capitals or felt pen
- check that the signature agrees with the name on the front of the card
- check that the signature strip has not been tampered with or that the word 'void' isn't visible
- check that the signature on the card matches the one on the terminal receipt or voucher
- if you're presented with an unsigned card, for MasterCard and Visa cards, ask the cardholder for identification and make a 'Code 10' call (see page 24). Don't allow the customer to sign the card until you've been advised what to do. For other card types, advise the cardholder that you cannot proceed with the transaction.

7. Card Security Code (CSC)/Card Verification Value (CVV2)

- A three or four-digit validation code. For MasterCard, Visa and Maestro cards the CSC is the last three digits printed on the reverse of the card after the last four digits of the cardholder account number, if these are present. The CSC can appear on the signature strip itself or in a white box to the right hand side of the signature strip. For American Express cards this number has four digits and is printed on the front of the card.

8. Magnetic Stripe

- Ensure that the card has a magnetic stripe on the back. Be suspicious of a counterfeit if the magnetic stripe feels unusually rough or scratched
- some cards may have a Holomag tape (holographic magnetic stripe) in place of the traditional magnetic stripe. When the Holomag is present it must always be on the back of the card, and no other hologram appears on the card.

9. Ultra Violet Feature

- If you have an ultraviolet light box for checking banknotes, you can check for the presence of an ultra violet marker on the front of these cards:
  - MasterCard - the letters M and C
  - Visa - dove
  - Maestro - the Maestro logo.

10. Photographs

- Some cards have a photograph of the cardholder on the front right of the card. If you're presented with a card that has this feature, check the photograph matches with the person presenting the card for payment. Be suspicious if there's no resemblance.

11. Card Logos

- Card logos – these appear on the front of the card and can also appear on the reverse. They should be clearly reproduced with sharp colours – be suspicious of a counterfeit if the logo is ragged around the edges or poorly reproduced.

EXAMPLES OF CARD LOGOS

MasterCard Logos

Visa Card Logos

Discover Global Network Card Logos

UnionPay Card Logo

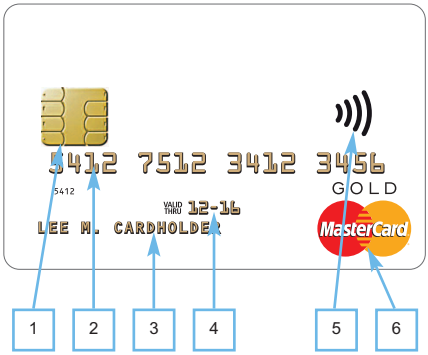
EXAMPLES OF CARDS AND CARD FEATURES

Key to card images:

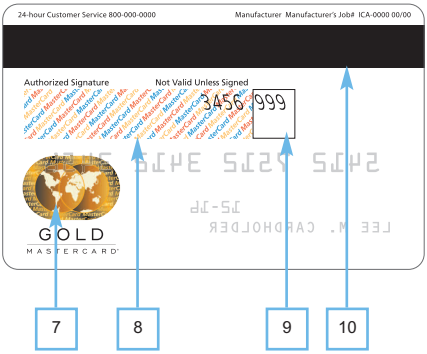
1. Chip
2. Card Number
3. Cardholder Title and Name
4. Valid From/Expiry Date ('Valid Thru' indicates the last month in which the card is valid)
5. Contactless Logo (where present)
6. Card Logo
7. Hologram
8. Signature Strip
9. Card Security Code
10. Magnetic Stripe/Holomag tape
11. Other acceptance marks

MasterCard

Front



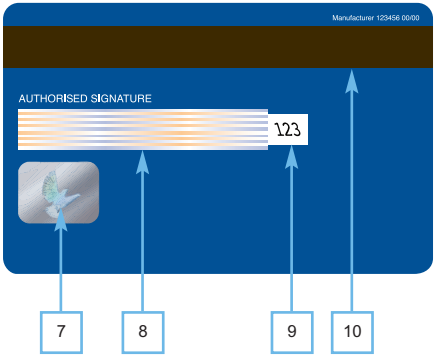
Back



Visa

Front

Back

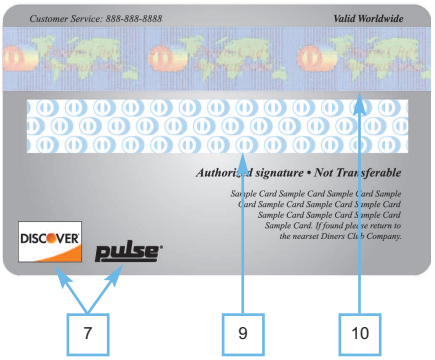


Discover Global Network

Diners Club International

Front

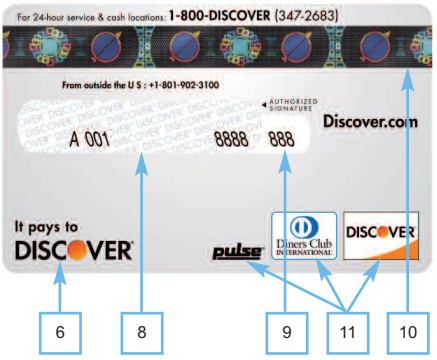
Back



Discover

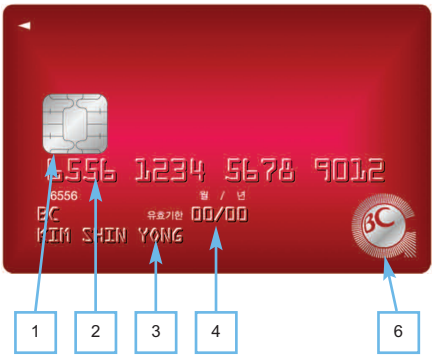
Front

Back

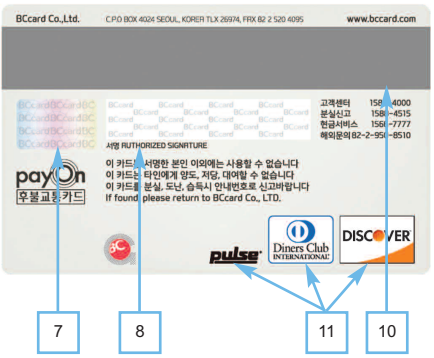


BC Card

Front



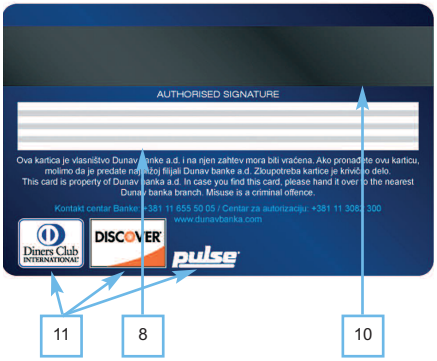
Back



DinaCard

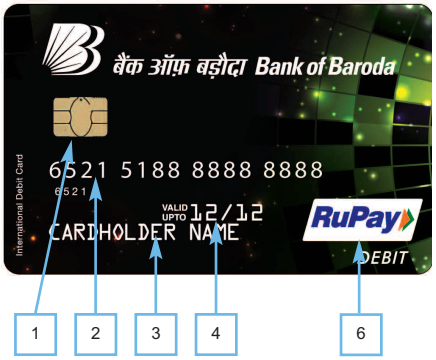
Front

Back

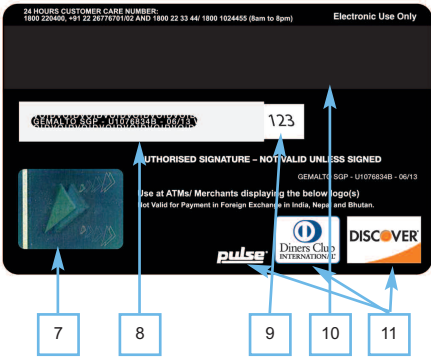


RuPay

Front



Back



For more information on the Discover Global Network, visit https://www.discovermerchants.com/

UnionPay

Fronts (with UnionPay written in English or Chinese)

Cards can also be dual branded with MasterCard and Visa logos.

Backs

ACCEPTING CARDS USING AN ELECTRONIC TERMINAL

You can accept cards either by using a terminal supplied by us, or by using your own equipment, subject to our prior agreement.

Using A Terminal Supplied By Us

Before you begin:

- read the terminal user guide before you start using your terminal, as this will provide you with information on the acceptance of cards
- check that the date and time on your terminal are correct. If they're incorrect, reset them following the instructions in your terminal user guide
- when positioning the terminal or PIN pad, bear in mind the accessibility and privacy of all cardholders, including those with disabilities
- ensure that you have easy access to your card terminal's power and telephone sockets in case you experience any technical problems and we need you to undertake tests to identify the problem
- power:
  - mains powered terminals (including base units that support portable terminals) must be plugged into a 13 amp socket no more than 1.5 metres away. Power to the terminal must be a continuous 24 hour clean supply and should not be disconnected under any circumstances unless we agreed in writing that your terminal can be used occasionally or seasonally, in which case, you must, when requested by us, connect the terminal to enable a maintenance call and/or software download. If your terminal is disconnected from the power supply/phone line, maintenance and downloads may not be completed
  - battery powered terminals (including portable and mobile terminals) must be returned to their base/charging units to recharge their battery. To ensure full battery power, the battery should be fully charged as soon as it's received and then overnight going forward
- telephone signal:
  - desktop and portable terminals should be permanently connected to a dedicated two way analogue telephone line via a socket no more than 1.5 metres away from the terminals. Terminals will not work plugged directly into a digital line, however if a ADSL adaptor is purchased this converts the digital line into an analogue line
  - mobile terminals require a GPRS signal for use
- terminals should be kept in an operating environment of 0°C to 40°C and with a humidity of 15% to 90% at 25°C and non-condensing
- for the Mobile POS Solution:
  - only download the payment app from reputable sources, for example, Apple Store, Google Play. Links to this are available on the GLOBAL MPOS website
  - log into the app to initiate the One Time PIN process and enable the Mobile POS Solution
  - carry out the Bluetooth Pairing and Key Loading processes
  - more detailed information is available on the GLOBAL MPOS website: www.globalmpos.co.uk
  - ensure that any surveillance equipment you have isn't able to record a customer entering their PIN

Please discuss, and agree with us, any changes to your terminal, including replacing, removing or relocating it. In the case of GPRS/mobile terminals, day to day relocation is permitted as part of business as usual use.

Note: You'll be liable for the cost of making changes in the telecommunications set up including equipment sharing the telephone line with the terminal, or the addition of a switchboard through which the terminal must operate.

Note: If you're using a Mobile POS Solution, please advise us of any change to your registered mobile phone number.

Please call us if you need any help (see page 86 for our contact details).

Using Your Own Equipment

We provide a processing service to many businesses that accept cards using their own equipment or card acceptance system (including any part of it provided by a third party).

We can support either of the two main types of card acceptance systems, which are:
- electronic point of sale (EPOS) systems capable of accepting cards
- electronic card acceptance terminals which operate independently of your other point of sale equipment.

For either of these systems, we can provide you with:
- technical help and advice - our technical team has extensive experience including supporting well over 5,000 successful customer implementations
- system specifications - detailing our requirements and interfaces.

Any equipment must be tested and approved by us prior to implementation. When using your own equipment, you must follow all the procedures described in these instructions, unless we agree alternative and/or supplementary procedures and document these to you separately.

You must make sure you keep us informed of all proposed changes to the terminals, configurations and transmission links. If you fail to do so we may be unable to process your transactions and there'll be a delay in crediting these transactions to your bank account.

If you use a third party provider, you must keep us informed of any change in provider. You must also ensure they're Payment Card Industry Data Security Standard (PCI DSS) compliant (see page 74).

It's your responsibility to ensure that your card processing equipment meets industry security standards. You must carry out, and bear the cost of all upgrades to your equipment which we, or your terminal supplier, may reasonably request from time to time. This includes any developments required to meet changes to Card Scheme Rules. Failure to meet these changes will result in non-compliance with some of these regulations and may incur charges or penalties and increase your chargeback exposure.

AUTHORISATION

Authorisation must be obtained at the time of the sale whilst the cardholder is present, in the case of Card Present transactions.

Don't hand over any goods to the cardholder until you've obtained authorisation.

What Is An Online Authorisation?

Online authorisation is when your terminal automatically:
- checks certain card details
- seeks confirmation that the cardholder has sufficient available funds on their account at the time of the transaction
- checks that the card has not been reported lost or stolen at the time of the transaction.

However, it does **not**:
- confirm the cardholder's identity
- guarantee payment.

Your terminal will seek authorisation automatically:
- if the sale exceeds your floor limit, the value of individual transactions above which authorisation is required as set out in the *Service Schedule* for the type of transaction in question
- if the sales exceeds the floor limit set on the card by the card issuer, which can override the floor limit on your terminal. This is unknown by the cardholder and automatically detected by the terminal
- on some transactions below your floor limit to help prevent fraud
- on certain transactions types, for example, all transactions accepted via a Mobile POS Solution are subject to authorisation
- when a chip and PIN card is signature-verified
- when a card contains no chip, only a magnetic stripe
- when a transaction has been key-entered
- when a chip and PIN card is accepted using the magnetic stripe.

When a chip card is inserted into a chip reader, additional security checks relating to data stored on the chip take place and may result in your terminal seeking automatic authorisation. Keep the terminal in your control while this action is being performed.

If you're in any way suspicious about the card or cardholder, make a 'Code 10' call (see page 24).

Note: Never spread the value of the sale over more than one card, or split the sale into smaller amounts to achieve a successful authorisation. This is prohibited. This is not to be confused with splitting the sale between multiple cardholders, for example, when paying for a meal. This isn't prohibited.

MasterCard Authorisations

MasterCard have specific requirements in the way authorisations are handled for MasterCard Credit, Debit MasterCard, and Maestro. MasterCard authorisations must be defined as either a "Final Authorisation" or a "Pre-Authorisation" and also flow Scheme Reference Data (SRD). If you rent a terminal from us or you use Global Iris, your transactions will contain this data. However, if you use your own equipment or use a Payment Service Provider (PSP) to process your transactions, you're responsible for ensuring that all transactions contain Scheme Reference Data.

Final Authorisations

Final Authorisations are used in most face to face environments, where goods or services can be

dispatched and settled within four business days of the original authorisation. A Final Authorisation is categorised as:

- An authorisation on a transaction (greater than zero) for the final or known amount.
- The transaction may no longer be cancelled after the authorisation is requested other than by performing a refund. This excludes any technical failures before the transaction completes.
- The transaction must be cleared (sent to the card processor) within four business days of the authorisation date.

Note: An authorisation marked as a Final Authorisation that doesn't meet the above criteria, for example, you don't send your transactions to us within four days, will attract a Processing Integrity Fee (PIF); this is in addition to the Service Charge applied to the transaction. Similarly, a transaction not flagged as a Final Authorisation that falls into the qualifying criteria above will attract an Unknown Finality Fee (UFF). To avoid either of these fees being applied it's vital to select the correct authorisation type for the transaction you're undertaking. Details of these charges can be found on your *Service Schedule* or any more recent communication from us.

Pre-Authorisations

Pre-Authorisations are used in the travel and entertainment sectors or anywhere that the final amount of the transaction may not be known at the point of original authorisation. For example, an online business that isn't able to fulfil an order in a single transaction. These transactions will attract a payment guarantee period of up to 30 days (please note that all Maestro card authorisations only have a payment guarantee period of seven days). Any transaction processed outside of these timescales requires another authorisation. A Payment Guarantee Period is the length of time that an authorisation request holds funds in a cardholders account, it doesn't confirm the cardholder's identity or guarantee payment.

A Pre-Authorisation is categorised by any of the following characteristics:

- An authorisation for an 'estimated' amount (greater than zero).
- Where a transaction isn't cleared (sent to Global Payments to debit the card holder) within four business days of the original authorisation date.
- Where a payment guarantee period is required for up to 30 days. For example, online orders where it's not clear at the point of sale when goods will be dispatched.
- Where the cardholder will be offered the option to pay by an alternate means at completion. For example, a hotelier may hold a room open for a period of time against an authorisation code but may offer the customer the choice to 'checkout' by paying cash.

It's your responsibility to ensure you select the correct type of authorisation for the transaction you're carrying out. You must also ensure if you're carrying out a Pre-Authorisation, that you keep the cardholder informed of any amounts that may be held on their card. This can be done verbally, by displaying a sign or via the screen on a terminal. Failure to define an authorisation as either a Final Authorisation or a Pre-Authorisation could result in fines being levied by MasterCard, for which you'll be liable.

Where you select to perform a Pre-Authorisation, a Pre-Authorisation Fee (PAF) will be applied in addition to the Service Charges applied to the transaction. Details of these charges can be found on your *Service Schedule* or any more recent communication from us.

Note: Zero Value Authorisations that check whether a card is valid and not lost or stolen won't attract the PAF charge as a Zero Value Authorisation doesn't 'ring fence' any funds in the cardholder's account. See 'Status Checks' on page 25 for more details on this.

Completing Pre-Authorisations And Flowing SRD

When you're ready to complete a Pre-Authorisation, a clearing record must be created that contains the SRD from the Pre-Authorisation(s), the authorisation code from the first Pre-Authorisation and the actual transaction value. The clearing record may relate to a single Pre-Authorisation, or a Pre-Authorisation and several incremental authorisations.

Clearing is where you send all your card sales transactions to us for that day. If you have a physical card terminal this usually happens when you complete your end of day banking.

If the value of the clearing record (the total transaction amount) is greater than the total value of any Pre-Authorisation plus any incremental authorisation(s), a further incremental authorisation must be performed for the difference to ensure the value of the clearing record is equal to the total value of the Pre-Authorisation and any incremental authorisations.

What Authorisation Messages Will I See On My Terminal?

When an authorisation request has been generated automatically, the terminal will display a response message. There are five possible message types:

'authorisation code xxxx(xx)'
This is a successful authorisation. The code should print automatically on the receipt. If your terminal doesn't print the authorisation code, write it onto the receipt.

Note: For high value transactions of £5,000 and over on a UnionPay card, we recommend you ask for proof of identity (for example, a valid passport or driving licence) and note on the transaction receipt what you've seen.

'call auth centre', 'call acquirer' or 'call card issuer'
If one of these messages appears on your terminal when you're trying to obtain automatic authorisation, you must call our authorisation service (see page 87 for contact details). These messages indicate that we need to make additional security checks that are required by the card issuer. You must call our authorisation service before accepting another means of payment.

If the transaction is authorised, enter the authorisation code you've been given into the terminal. If the transaction isn't authorised, cancel the transaction and hand the receipt to the customer.

Note: Telephone authorisations, including 'Code 10' requests, are **not** available for transactions on Discover Global Network cards, UnionPay cards, Maestro cards issued outside the UK and any transaction accepted via a Mobile POS Solution. These cards and transaction types can only be authorised or declined via the terminal. If you're at all suspicious, **do not** proceed with the transaction(s) as to do so will be at your own risk. You must ask the cardholder for an alternative means of payment.

'declined'
The card issuer has refused to authorise the transaction. Advise the cardholder to contact their card issuer if they want to know why the transaction has been declined. If you and the cardholder want to continue with the sale, ask for an alternative means of payment. You are prohibited from proceeding with a transaction on a declined card and if you do so, it may result in a chargeback and a financial loss to your business.

Note: MasterCard and Visa have strict rules to limit the number of authorisations that can be attempted on the same card, in the event of a decline response. You must not attempt to authorise the same card again if you have already received two decline responses within the last 24 hours.

'cannot authorise'
It has not been possible to obtain an authorisation code. If you and the cardholder want to continue with the sale, you must ask for an alternative means of payment.

'invalid card'
Check you're authorised to accept this card type. If you're unsure, you should contact our helpdesk (see page 86 for contact details). If you're authorised to accept the card presented, please make a 'Code 10' call (see page 24).

If your terminal isn't set up to seek authorisation automatically, or there's a fault that prevents your terminal from obtaining an authorisation automatically, you must call our authorisation service (see page 87 for contact details).

When Is Telephone Authorisation Sought?

You must call our authorisation service (see page 87 for contact details) if:
- you're unable to obtain automatic authorisation
- the sale exceeds your floor limit
- you're in any way suspicious about the card or cardholder (see 'Code 10 Call' on page 24)
- prompted by the terminal
- you've reverted to Fallback paper vouchers due to your terminal being faulty (see page 30)
- we've agreed to you processing paper vouchers (see page 30).

What Does Telephone Authorisation Do?

Telephone authorisation:
- seeks confirmation that the cardholder has sufficient available funds on their account at the time of the transaction
- checks that the card has not been reported lost or stolen at the time of the transaction.

As with online authorisations, telephone authorisation doesn't:
- confirm the cardholder's identity
- guarantee payment.

International Cards

Time differences can sometimes delay authorisation on international cards. We may ask for your name and telephone number so we can call you when we've obtained authorisation. We'll ask you

if your customer is prepared to wait.

Changing The Transaction Amount After Authorisation

You must call our authorisation service if the value of the transaction changes after you've obtained authorisation, but before the transaction is completed. The original authorisation must be cancelled and a new authorisation obtained for the new amount. This will ensure the cardholder's available funds are adjusted accordingly.

If the value of the transaction increases, you must **not** obtain an authorisation for the increased amount. A new authorisation for the whole amount must be obtained. Failure to do so may result in a chargeback if the cardholder disputes the original transaction.

Note: If you fail to cancel an unused authorisation on a MasterCard branded card, you'll be subject to a PIF charge (see 'MasterCard Authorisations' on page 20 for more details on this charge).

Call our authorisation service (see page 87 for contact details) to cancel the authorisation.

Floor Limits

Floor limits are set by the Card Schemes and these can be found on your *Service Schedule*. However, the card issuer can also set their preferred floor limit within the card and this can override what is set in the terminal.

We may need to change your floor limits from time to time as part of our drive to combat fraud or at the request of the Card Schemes. We'll advise you of any change should this need to happen.

'CODE 10' CALLS

A 'Code 10' call should be made to our authorisation service (see page 87 for contact details) if:

- you're suspicious of the card, the cardholder or the circumstances of the transaction
- you've been instructed to do so by us as a fraud prevention measure.

Note: 'Code 10' calls are **not** available for transactions on any Discover Global Network and UnionPay cards and Maestro cards that issued outside the UK. These cards can only be authorised or declined via the terminal. If you're at all suspicious, **do not** proceed with the transaction(s) as to do so will be at your own risk. You must ask the cardholder for an alternative means of payment.

Note: 'Code 10' calls should only be made in conjunction with a card transaction. You must not make 'Code 10' calls merely to verify name and address details, for example, as part of an application for credit. See 'Status Checks' on page 25 for more information.

What You Need To Make The 'Code 10' Call

- Your merchant number
- the transaction amount rounded up to the nearest pound; if the transaction isn't in sterling, state the currency and amount
- the authorisation code if a code was granted with the original transaction, for example with an

online authorisation
- you'll need to be clear about why you're suspicious of the card and/or cardholder
- you should ensure that you handle the call as discreetly as possible
- you may be instructed to ask the cardholder a number of questions for security purposes.

You need to complete these security checks even if your customer offers an alternative form of payment. It's also important to complete the 'Code 10' call even if the customer asks for the card to be returned or leaves the premises without completing the transaction.

If we're satisfied with the information given by your customer, we may authorise the transaction. If we're not satisfied, we'll give you further instructions, which may include asking you to cancel any transaction and possibly to retain the card if it's safe to do so.

Remember to:
- advise the cardholder that a routine security check is to be undertaken or that your card processor has requested a routine security check on the transaction. Hold on to the card and goods until the security checks have been completed
- turn on any surveillance equipment you may have
- telephone our authorisation service (see page 87 for contact details)
- ensure that a manual imprint of the card is taken whenever you process a transaction following a 'Code 10' call
- obtain the authorisation code directly from us, and not from either the cardholder or anyone else, such as the card issuer, who may be involved with the call
- don't telephone any number given to you by the cardholder
- don't make a 'Code 10' call if you feel threatened or consider it's unsafe to do so, for example, if you're alone in the shop; in this case call us immediately after the cardholder has left, as this may help to prevent potential fraudulent activity elsewhere.

You should not put yourself or your colleagues in danger when trying to retain the card. If the person presenting the card becomes violent or abusive, always return the card to them, even if we've asked you to retain it.

Note: Making a 'Code 10' call doesn't guarantee payment.

If You're Still Suspicious

After completing a 'Code 10' call and obtaining authorisation, you're under no obligation to complete the transaction. However, in such circumstances you must not retain the card.

ACCOUNT VERIFICATION/STATUS CHECK

MasterCard and Visa have a 'status check' service that allows you to verify a cardholder's account without reserving funds. Status checks must be performed with a zero value Account Verification. Status checks with nominal amounts, for example £1, are not allowed.

Refer to your terminal user guide on how to complete this check or call our authorisation service (see page 87 for contact details).

Note: A status check transaction isn't the same as a pre-authorisation transaction and doesn't apply to sectors such as hotels and car hire where pre-authorisations are made.

RECOVERED CARDS

Retaining A Card

If we ask you to retain a card, please try to do so. A reward of £50 may be paid to you if a MasterCard or Visa card is recovered as a result of a 'Code 10' call.

For a reward to be payable, there must have been an attempt at authorisation.

You should not endanger yourself or your colleagues in endeavouring to retain a card.

If the person presenting the card becomes violent or abusive, always return the card to them, even if we've asked you to retain the card. In these circumstances, you should always:

- try to record details of the appearance of the person presenting the card and use any surveillance equipment that you may have
- telephone our authorisation service (see page 87 for contact details) and explain to us that you were unable to retain the card as requested.

In some circumstances we'll contact the police. If the police ask for the card:

- hand the card to the police officer
- take the officer's name, number and police station telephone number
- ask for a receipt and send it with the completed Recovered Card Reward form
- tell the investigating police officer if you use surveillance cameras, and please preserve the video evidence for at least 30 days.

Once a card is recovered:

- immediately complete a Recovered Card Reward form
- give as much detail as possible about the person presenting the card, including other relevant details like their car registration number
- cut the card horizontally, but leave the signature strip, magnetic stripe, embossed card number, hologram and chip intact
- immediately return both parts of the card and reward form to the address below
- keep a copy of the Recovered Card Reward form.

Merchant Rewards Programme
Global Payments
51 De Montfort Street
Leicester
LE1 7BB

We'll advise you how to obtain a copy of the Recovered Card Reward form during the 'Code 10' call.

Finding A Card Or A Card Is Left At Your Premises

Please keep any cards left by customers in a safe place for 24 hours.

When a card is claimed, don't hand over the card until you've verified the cardholder's identity:

- ask for satisfactory identification, such as a driver's licence
- check the signature on the card against a specimen signature of the person claiming the card

- if you're in any doubt, contact our authorisation service (see page 87 for contact details).

If the card has not been claimed within 24 hours:
- cut the card horizontally, leaving the signature strip, magnetic stripe, embossed number and chip intact
- obtain a Recovered Card Reward form from our website at www.globalpaymentsinc.co.uk. It can be downloaded by logging into the 'Customer Centre' and selecting the option for 'Global Payments', followed by 'Documentation'
- return both parts of the card together with a Recovered Card Reward form to address above.

Note: A reward won't be paid for cards that have been found.

REFUNDS

Refunds can only be made on the card used for the original sale transaction
- the value of the refund cannot exceed the original transaction amount
- never make cash or cheque refunds for card transactions.

We recommend that you carry out regular checks to confirm that all refunds made using your terminal/point of sale equipment are genuine. To assist with this, the number and value of refunds made are included in the daily terminal summary report. You may also want to consider restricting the ability to make refunds to certain staff members.

To make a refund undertake the following procedure:
- ask to see the original sales receipt or locate the original sale transaction on your Mobile POS Solution – check that the last four digits of the card number on the original sales receipt/transaction match those on the card being presented. Crediting a different card account may result in the original transaction being charged back to you
- validation checks – carry out the card and cardholder validation checks as for a normal sale transaction (see page 10)
- process the refund on your terminal – see your terminal user guide.

Please note that it's not necessary to obtain authorisation for a refund.

If you're unable to perform a refund electronically on a MasterCard, Visa, Visa Debit or Debit MasterCard card because your terminal has failed, you need to fully complete a Fallback paper refund voucher (see page 30). You may need to hand-write the card details if the card isn't embossed. When your terminal is working again, key-enter the refund details. You'll be debited automatically via your electronic terminal, so you must not submit the Fallback paper voucher to us for processing as well. You must retain the voucher for your records.

Refunds for Maestro, Visa Electron, V PAY, Discover Global Network and UnionPay cards and any transaction accepted via a Mobile POS Solution can only be processed electronically.

You must state your refund policy clearly to cardholders. Failure to do so increases your vulnerability to chargebacks.

Exchanging Goods

Give a refund for the original sale and complete a new electronic transaction for the full amount of

the new goods/services provided.

Cancelling A Transaction

If a cardholder decides not to purchase the goods or services, you must cancel the transaction. The action you need to take depends on how you've accepted the card and the stage you've reached in the transaction when the cardholder changes their mind.

If you haven't completed the transaction:

- verified by PIN - you can cancel the transaction when you key in the amount. Alternatively the cardholder can cancel the transaction when entering their PIN
- verified by signature - you can cancel the transaction when the terminal prompts you to confirm the cardholder's signature.

Once the cancellation is complete, you should provide the cardholder with a copy of the receipt confirming the cancellation.

If authorisation has been obtained for a MasterCard, Visa, Visa Electron or V PAY transaction, the authorisation must be reversed. See 'Authorisation Reversals' below.

If the cardholder wants to cancel the transaction after it has been completed, perform a refund as outlined on page 27.

Reversing A Transaction

If a sale or refund transaction is completed in error, you can reverse the transaction, thereby cancelling it. The reversal must be performed within 30 seconds and on the same terminal the original transaction took place.

However, if the cardholder wants to cancel the transaction after it has been completed, a refund must be completed.

Note: If a purchase reversal transaction fails; this may result in a chargeback.

Authorisation Reversals

It's a requirement that an authorisation reversal is carried out for any excess authorisations gained above the final authorised transaction amount, unless you send the clearing record to us within 24 hours of the actual transaction amount being confirmed.

For cancelled transactions, the authorisation(s) must be reversed within 24 hours of the transaction being cancelled.

Wherever an authorisation code is generated and that transaction isn't sent for clearing, you'll need to complete a reversal of the authorisation to ensure that the cardholder is able to draw on their funds.

Note: If you fail to cancel an unused authorisation on a MasterCard branded card, you'll be subject to a PIF charge (see 'MasterCard Authorisations' on page 20 for more details on this charge).

If you operate an automated fuel dispenser or accept Contactless transactions, the reversal of authorisations isn't required.

Call our authorisation service (see page 87 for contact details) to reverse the authorisation.

HOW TO SUBMIT YOUR ELECTRONIC TERMINAL TRANSACTIONS

If you rent your terminal from us it will be an online terminal. If you own your own terminal or rent it from someone else, it may be either an online or offline terminal.

Online Terminals

These terminals submit transactions to a host system throughout the business day. Overnight the host system will release all stored transactions for processing. Online terminals don't store transactions.

To make sure that we can process your transactions, you must ensure that:

- your terminal is permanently connected to a power supply or its battery is always charged
- your terminal's telephone line is able to make calls 24 hours per day or for mobile terminals a GPRS signal is available
- you perform a 'banking' procedure (sometimes called an end-of-day procedure) each business day (see your terminal user guide for instructions)
- the terminal produces a summary report which should match the number and value of transaction receipts taken since the last 'banking' procedure was performed.

Note: It's your responsibility to perform a 'banking' procedure at the end of every business day. Failure to do so will result in delays crediting your bank account, and may result in chargebacks. For terminals rented from us, this procedure needs to be completed by 2.00am daily.

Mobile POS Solution (Online Terminal)

Transactions are submitted to a host system throughout the business day. Overnight the host system will release all stored transactions for processing. Therefore, so long as you've followed the procedures in the Mobile POS Solution user guide, you don't need to do anything more to submit your transactions.

Offline Terminals

These terminals store transactions in their memory during the business day. Overnight your terminal will be contacted to collect the stored transactions. This is known as polling.

Note: You must check that the terminal has been polled every night. Failure to do so will result in delays crediting your bank account, and may result in chargebacks.

Processing Of Transactions

Where you rent a terminal from us, providing your transactions have been successfully released by the host system, we'll transmit the transactions to the relevant card issuers to request payment from them on the business day after we receive your transactions. If the transactions aren't

released by the host system until after 6.00am on a business day, or on a day which isn't a business day, then your transactions will be treated as having been received on the following business day. For example:

- if the host systems releases transactions overnight on a Monday, we'll transmit them to the card issuers on Tuesday
- if the host systems releases transactions overnight on a Friday, we'll transmit them to the card issuers on Monday (unless this is a public holiday, in which case they will be transmitted on Tuesday).

Where you own your own equipment or rent a terminal from someone else, you or your Payment Service Provider submit your transaction details directly to us by file transfer. The date on which the file is received, providing it's received before 6.00am, is the day we transmit the transactions to the relevant card issuers. If we receive your file on a day which isn't a business day, or after 6.00am on a business day, then your transactions will typically be treated as being received on the following business day.

Note: UnionPay transaction processing is subject to a different system cut-off time and Chinese public holidays as well as the public holidays in England. UnionPay processes transaction data daily after Beijing time 23:00 (15:00 GMT, 16:00 BST). No action is required by you and there'll be no impact should you wish to process a UnionPay transaction at this time.

USING FALLBACK PAPER VOUCHERS

You must not use paper vouchers if your terminal is working and you've signed an agreement for electronic card processing. However, in exceptional circumstances you may need to use paper vouchers if:

- we've agreed to you processing paper vouchers
- your terminal is out of use due to a fault
- your telephone line is faulty
- you have key-entered a transaction and you want to prove the card was present, however, this is for your records only and not to be submitted for processing (key entry is not possible on all card types - see page 6).

Note: It's not possible to process Maestro, Visa Electron, V PAY, Discover Global Network or UnionPay cards or Mobile POS Solution transactions using paper vouchers.

Please ensure you retain an adequate supply of Fallback paper vouchers and have the Fallback equipment provided in your starter pack (see page 84) to hand.

All transactions taken via Fallback paper vouchers require authorisation, therefore a voice authorisation will need to be undertaken (see 'Authorisation' on page 19).

Please bear in mind that the Card Schemes require all face to face transactions, where you're presented with a chip and PIN card to be performed using a chip and PIN terminal. Transactions where this isn't the case (paper vouchers), which turn out to be fraudulent, can be returned by the card issuer. As a result, using Fallback paper vouchers for chip and PIN card transactions increases your risk of chargebacks (see page 66) due to fraudulent transactions, so you may prefer to avoid this risk by requesting an alternative form of payment from your customers.

How To Complete A Fallback Paper Voucher

Undertake validation checks (see page 10)
- imprint the card
- fully complete the Fallback paper voucher - use a black ballpoint pen and provide details of the goods/services purchased
- ask the customer to check all the details on the voucher and sign it
- check the signature
- you must obtain authorisation (see 'Authorisation' on page 19). Call our authorisation service (see page 87 for contact details).

How To Cancel A Fallback Paper Voucher Transaction (Before The Voucher Is Submitted For Processing)

To cancel a Fallback paper voucher you must have the card and voucher in front of you to check that the signature on the voucher is the same as that on the reverse of the card.

If you've obtained authorisation call our authorisation service (see page 87 for contact details) to cancel.

Destroy all copies of the voucher in the presence of the cardholder before returning the card.

How To Make A Fallback Paper Voucher Refund

Ask for the original sales voucher - check that the last four digits match those on the card being presented
- undertake validation checks (see page 10)
- imprint the card
- fully complete the Fallback paper refund voucher - use a black ballpoint pen and provide details of the refund required
- ensure all details are correct and legible
- cancel the sales authorisation obtained previously (see 'Authorisation Reversals' on page 28)
- you must sign the voucher
- when you're satisfied that everything is in order complete the refund.

How To Submit Fallback Paper Vouchers For Processing

Completing The Summary Fallback Voucher

- Imprint the summary Fallback voucher with the merchant card (both are contained in your starter pack)
- don't batch Card Present (CP) and Card Not Present (CNP) vouchers together on the same summary
- the maximum number of paper vouchers per summary is 100
- complete the front of the summary - please tick to indicate whether the transactions were undertaken in a CP or in a CNP environment
- sign and date the summary voucher
- separate your copies of the summary and paper vouchers
- arrange the vouchers in the correct order:
    - summary - process copy

- sales vouchers - processing copies
- refund vouchers - processing copies

Submitting The Fallback Vouchers For Processing

Send the prepared summary Fallback voucher and sales/refund vouchers using our Freepost facility below:

Freepost RSGY-GYLY-GGEA
Global Payments
De Montfort Business Centre
51 De Montfort Street
Leicester
LE1 7BB

Note: This address must not be utilised for any other purpose than the sending of Global Payments vouchers for processing. Global Payments won't be held responsible for other paperwork sent to this address.

Every batch of vouchers must be posted before the end of the third business day (Monday to Friday, excluding public holidays) following the transactions. Delays may cause cardholder queries and chargebacks (see page 66).

Note: Consider data security when storing copies of your vouchers (see page 71). They should be securely retained for five years following delivery of goods or completion of the service provided. Please also ensure imprinters are kept securely in your sole possession. They must not be given to any other business.

Processing Of Transactions

Allowing for postage, it will typically take a further business day from the date of receipt of the vouchers for them to be input. This enables us to transmit the transactions to the relevant issuers in order to request payment from them.

We'll credit your account with the summary total, subject to our advice of any adjustments.

CARD NOT PRESENT (CNP) TRANSACTIONS

Note: Requirements in this section are provided in addition to those in the remainder of these *Merchant Operating Instructions* and you'll need our written agreement to undertake any CNP transactions.

Card Not Present (CNP) transactions are any transaction where the card and cardholder aren't physically present with you at the time of the transaction.

These transactions present an opportunity for fraud, as the card, signature and personal identification number (PIN) cannot be checked.

Note: It's vital that you understand the risks associated with CNP transactions. All CNP transactions are accepted at your own risk. Please read the 'How To Reduce Fraud' section on page 76 which provides important advice on CNP fraud and how to minimise your risk of financial loss.

Note:

- Maestro cards issued outside the UK cannot be used for mail order and telephone order (MOTO) transactions
- Maestro can only be accepted over the internet if you have MasterCard SecureCode implemented
- Maestro cards cannot be used for recurring transactions.
- Cards from the Discover Global Network and UnionPay cannot be accepted for any type of CNP transaction.

ACCEPTING MAIL AND TELEPHONE ORDERS

Mail order and telephone orders (MOTO) can be accepted by key-entering the transaction into your terminal (see 'Accepting Cards Using An Electronic Terminal' on page 18) or your PC.

We offer a solution for accepting MOTO transactions on your PC via our Global Iris service (see page 48). For details on accepting transactions using Global Iris please refer to the user guides at https://resourcecentre.globaliris.com/ or contact us (see page 86 for contact details).

Regardless of how you accept the MOTO transaction, you must ensure that you have the following information from the cardholder:

- card type
- Card Security Code (CSC) (see page 80)
- card number
- name and initial(s) exactly as they appear on their card
- valid from date (if on card)
- expiry date
- statement name
- statement address
- contact telephone number (we recommend that you don't accept a mobile telephone number).

Note: You must destroy any record of the CSC once it has been checked as the retention of the CSC post-authorisation is strictly forbidden under Card Scheme security requirements (see the 'Data Security' section on page 71).

You must inform the cardholder of the total transaction value (including the currency) and obtain their authority to debit this amount from the card.

You must also ensure that:
- any written orders contain the cardholder's signature
- you establish a process for checking to see if different transactions relate to the same address, or if the same card number is being used for different addresses
- for deliveries to the cardholder's address, if possible obtain the telephone number for the delivery address from the directory enquiries service or a local directory, before despatching the goods, telephone the customer back on the number provided to confirm the order.

ACCEPTING INTERNET ORDERS

These instructions apply in addition to the other CNP instructions detailed in this section.

Please note, you'll need a separate merchant number to undertake transactions over the internet.

Note: You **must not** accept transactions over the internet by key-entering card details into an electronic terminal or using paper vouchers.

You can accept internet transactions by any of the following methods, but irrespective of your chosen internet solution, we encourage you to undertake fraud transaction screening (see page 81).

We strongly recommend the deployment of MasterCard SecureCode and Verified by Visa (see page 80).

Note: To accept Maestro internet transactions you must support MasterCard SecureCode. This is a mandatory requirement.

We offer our own hosted payments service, Global Iris, which can be integrated with your website (see 'Global Iris' on page 48).

For details on accepting transactions using Global Iris please refer to the guides at https://resourcecentre.globaliris.com/ or contact us (see page 86 for contact details).

Website Requirements

You're responsible for creating the order and payment page(s) within your website, and you must ensure that the following information is reflected clearly:
- the name of your business - your legal business name should also be included if it's different to your trading name
- the full postal address of your business, including country
- your landline phone number and email address to help resolve any cardholder complaints and therefore minimise any potential chargebacks
- a full description of the products or services provided. You must not advertise or accept orders for goods that you're unable to supply. In particular you must monitor and update your website, removing any items you're unable to supply and offer immediate refunds to cardholders where you're unable to supply goods and the cardholder is unwilling to accept the delay. You must display your policy on split shipment of goods

- your refund/returns policy and have a 'click to accept' button or other acknowledgment on your website to evidence the cardholder has accepted your refund/return policy
- the delivery details, including despatch dates and delivery policy, for example not accepting temporary or 'care of' addresses. Indicate the ability to support global deliveries and any relevant export restrictions
- the total price, including any additional charges for delivery, handling and tax charges
- the currency of the transaction, which must be sterling unless we've agreed you may accept currency payments, in which case the total price should be in the relevant currency (if you state an exchange rate you should advise customers if this is only indicative)
- the details of your data privacy policy and/or of the security measures you have in place to protect customer and transaction details, including your compliance with the card data security rules (see page 71)
- the information required by law including the Consumer Protection (Distance Selling) Regulations 2000 and Electronic Commerce (EC Directive) Regulations 2002 and any other information necessary for compliance with data protection legislation
- your purchase terms and conditions including any guarantees or warranties, either on the same screen used as the checkout screen or within the pages accessed by the cardholder prior to the final checkout
- the logos of the cards you accept
- allow the cardholder to confirm the purchase before completion of the sale.

Payment Service Providers (PSPs)

PSPs are companies who can act as your agent, either providing you with the ability to accept card payments and/or forwarding them on to us for authorisation and processing. They may also be able to assist in designing and hosting your website. If you choose a PSP(s) to process your card transactions we must give you our prior written approval.

You won't normally receive card numbers for internet transactions processed by PSPs, and this may impair your ability to detect multiple transactions on the same or similar card numbers. Some PSPs provide fraud screening or fraud prevention services and we strongly recommend that you make use of a PSP offering fraud management services.

PSPs will make a charge for their service, which is in addition to our monthly service charge. The service that they offer and the charges that they make may vary and you'll need to choose the company which best meets your needs. The contract is between you and the PSP and is separate from your Agreement with us.

You'll also be responsible for ensuring that the PSP is compliant with the necessary Card Scheme Rules. In particular, any third party you use for processing needs to be compliant with the card data security rules (see page 71).

Using Your Own Equipment/Systems For Internet Transactions

You can use your own card processing equipment and/or systems to obtain authorisation and send card transaction details to us. We'll process the transaction and credit the proceeds to your nominated bank account. This is a more specialised solution and can be more expensive than other options. Please contact us if you would like more details on suppliers who can advise you on equipment and software requirements. Any equipment must be tested and approved by us prior to implementation.

Electronic Commerce Indicator (ECI)

If you use Global Iris for your internet transactions, all these transactions and authorisations will automatically carry an Electronic Commerce Indicator (ECI) flag.

If you use your own equipment or use a PSP to process your internet transactions, you're responsible for ensuring that all such transactions and authorisations have the correct ECI flags.

Failure to do so could result in fines being levied by the Card Schemes, for which you'll be liable.

Electronic Commerce Security Measures

You must implement and maintain security measures to prevent unauthorised access to cardholder and transaction details. Minimum security requirements are:

- encryption of cardholder data (minimum 40 bit)
- firewall and anti-virus software
- physical security of your business PCs
- unique IDs and passwords for all users of your systems (don't use default settings).

We recommend that encryption, anti-virus and firewall software is installed and configured by experienced personnel, or as an alternative the installation is reviewed by an independent third party to ensure that it's correctly configured. You must also be compliant with the Payment Card Industry Data Security Standard (PCI DSS) (see page 71), and if your website is to be hosted by a third party (PSP), you must ensure that they conform to these standards.

AUTHORISATION OF CNP TRANSACTIONS

In a CNP environment there are different regulations covering the processing of a transaction. A Maestro transaction should be processed on the day of receipt or acceptance of an order, while a MasterCard or Visa transaction should be processed when the goods are despatched.

There are rules surrounding the processing of a transaction and the length of time for which an authorisation code remains active. The authorisation is made on the card details that are provided at the point of the call, which includes the expiry date. Authorisation only checks that there are available funds in the cardholder's account at that time, and that the card has not been reported lost or stolen. It also reserves the funds on the cardholder's account, which stay reserved until the corresponding debit is received. Please note that the funds will stay reserved for a minimum of seven days depending on the card type, and the authorisation will be not be removed if the actual transaction isn't received. To cancel the authorisation code, please call our authorisation service (see page 87 for contact details).

Note: Once you've completed the authorisation, you must destroy any record of the cardholder's Card Security Code (CSC) as the retention of the CSC post-authorisation is strictly forbidden under Card Scheme security requirements (see page 71).

Note: Never spread the value of the sale over more than one card, or split the sale into smaller amounts to achieve a successful authorisation. This is prohibited.

If all the goods aren't available to despatch, then you need to process a partial transaction. You're required to process the value of the goods that are available using the original authorisation code

that was obtained for the full amount. If the subsequent goods are available for despatch within seven days, you should also use the original authorisation code to process this transaction. However, if the subsequent goods aren't ready to despatch within this period, you should initiate another authorisation for the value of the outstanding goods when they're ready to be despatched.

As a matter of courtesy you should contact the cardholder and check that they're willing to wait for the goods. Explain any options available to them, for example:

- partially fulfilling the order and sending the remaining goods by the advised delivery date, with the full transaction value being processed as originally agreed
- partially fulfilling the order and sending the remaining goods by the advised delivery date, with the original transaction being refunded/authorisation cancelled and a new transaction being processed for the value of the goods being delivered (follow the guidance provided in the previous paragraph). When you're in a position to despatch the remainder of the goods, you should complete a new transaction for the balance.

In all cases, you **must** retain evidence of the option agreed with the cardholder in case a chargeback is later received.

Note: There are additional requirements for MasterCard authorisations. Please ensure you refer to 'MasterCard Authorisations' on page 20 to be aware of the fees you may be charged for these authorisations.

Excessive Authorisations

MasterCard and Visa have strict rules to limit the number of authorisations that can be attempted on the same card, in the event of a decline response. This is to restrict businesses processing excessive authorisations to the disadvantage of the cardholder.

You must not attempt to authorise the same card again if you have already received two decline responses within the last 24 hours. If the card continues to decline on the following day we recommend you contact the cardholder to discuss an alternative method of payment.

MasterCard and Visa regularly monitor all authorisations and identify those businesses found to be processing excessive authorisations. Any customer in breach of this rule may be subject to escalating penalties until the position is resolved.

To remain compliant, make sure that you have a process in place to monitor the number of authorisation requests that you are submitting.

Visa Europe Payment Stop Service – VEPSS

Visa has a service that enables the cardholder to instruct their card issuer to stop any CNP future dated payment. This includes recurring transactions, instalment transactions and payday loan repayments.

This currently applies to UK issued Visa cards but will eventually be rolled out to European issuers.

When you attempt to authorise a transaction on a card that has a stop instruction against it, you will receive a decline response and our authorisation system will also include a description of 'Consent Revoked'. If you receive this response, under no circumstance are you allowed to

represent the transaction for authorisation and you must contact the cardholder to discuss alternative payment arrangements.

So there is consistency across MasterCard and Visa we will provide the same response for both Card Schemes.

CNP Telephone Authorisation For MOTO Transactions

You can seek telephone authorisation for a maximum of five transactions in any one call. Please call our authorisation service (see page 87 for contact details) and you'll be asked for:

- merchant number
- Card Security Code (CSC) (see page 80)
- Address Verification Service (AVS) information (see page 80)
- cardholder account number
- transaction amount rounded up to the nearest pound
- card expiry date
- in certain circumstances the cardholder's name, initial(s) and statement address.

If the transaction is authorised we'll provide you with an authorisation code, which you'll need to enter on the terminal.

If authorisation is declined, ask the cardholder for an alternative form of payment.

We, or the card issuer, may sometimes want to make further checks which could involve a delay.

CONFIRMING CNP ORDERS

When an order and payment have been accepted, a transaction receipt or confirmation must be provided to the cardholder either by email or post. This must contain the following:

- a unique identification number to assist investigations if the transaction is disputed
- your trading name, full postal address, including country, and telephone number
- your website address if you're accepting orders over the internet
- the purchaser's name
- the amount and currency. If you quote an exchange rate applicable to your prices, you must state that it's an indicative rate only and you must explain that the cardholder may be debited with a different amount
- a description of the products or services bought
- the transaction date and type of transaction (for example, purchase or refund)
- the authorisation code for the transaction
- your return/refund policy
- the despatch date and delivery method. Goods should be despatched or services supplied either before or when the transaction is presented to us. You may, however, despatch goods or supply services after presentation provided you've advised us of this and displayed this information on your website. Such customer information should indicate the normal and maximum period for despatch
- card type and truncated card details (don't include the expiry date and only the last four digits of the card number).

DELIVERING GOODS

We recommend that you follow the guidance below. This is particularly important if the goods are of high value.

When delivering goods:

- Always send goods by recorded or special delivery or by a reputable security carrier. Insist on a signed (preferably by the cardholder) and dated delivery note. Tell the courier not to make the delivery if the premises appear to be vacant. Please note that proof of delivery alone isn't sufficient evidence to defend a chargeback.
- Don't release goods to third parties such as taxi drivers and messengers.
- Be cautious of transactions where the billing address is different to the requested delivery address. Avoid delivering to addresses other than the cardholder's, such as hotels, internet cafes and 'care of' addresses.
- Be wary of requests for next-day delivery, requests to alter the delivery address at short notice, or telephone calls on the day of delivery requesting a specific delivery time.

COLLECTION OF GOODS

If the cardholder collects the goods, the transaction will become card present (CP). Ask the cardholder for their card and follow the normal CP procedures. The cardholder must enter their PIN or sign a new terminal receipt. Any previous CNP transaction and associated authorisation must be cancelled, and any record of the CSC and other sensitive card data securely destroyed (see page 71 regarding 'Data Security').

SPECIAL TRANSACTION TYPES

This section will introduce you to a number of special types of transaction that you may need, depending on the way in which you propose to accept card payments. Refer to your *Service Schedule* for the transaction types you're authorised to undertake. If you subsequently decide you would like to undertake any of these special transaction types, you'll need our written agreement.

Note: Not all of these transaction types are available on all types of cards. A Mobile POS Solution cannot be used to accept these special transaction types.

Requirements in this section are provided in addition to those in the remainder of these *Merchant Operating Instructions.*

BUREAU DE CHANGE

You need our prior written approval to accept card payments to provide foreign currency or travellers cheques to cardholders.

Your business must be registered with the appropriate government agency for anti-money laundering purposes, and you must comply with their rules.

You must undertake all necessary card validation checks (see page10).

In addition to these checks, when undertaking Bureau de Change transactions you're required to identify the cardholder and keep a record of the identification seen. Precise requirements depend on the card type used and please note that chargebacks may still occur.

For these transactions, you must verify the cardholder's identity by inspecting their passport or driving licence. Check the document has not expired and that it has been signed by the cardholder. The following information must be recorded on the front of your copy of the terminal receipt or voucher:

- type of identification
- number of identification
- expiry date of identification
- place of issue of identification
- name and address of cardholder
- authorisation code (all cash advance transactions must be authorised)
- the four digits printed below the embossed number on the card must match the first four digits of the number embossed - failure to record digits which match may lead to a chargeback
- cardholder's signature
- your cashier's initials.

For MasterCard and Visa cards (except Visa Electron), if your terminal fails to read the card and/or you obtain telephone authorisation for the transaction, you must take a paper voucher imprint that must be signed by the cardholder. If the card is a Visa Electron card and your terminal fails to read the card, you must ask for another means of payment. Visa Electron cards can only be processed electronically.

Note: Maestro, Discover Global Network and UnionPay cards must not be accepted for Bureau de Change transactions.

DYNAMIC CURRENCY CONVERSION (DCC)

You may wish to consider offering your international MasterCard and Visa cardholders the ability to purchase goods in their local billing currency, as opposed to sterling.

DCC offers your customer the benefit of being able to make an informed decision and fix the exchange rate used at the time of the transaction. If the cardholder doesn't wish to proceed with the rate offered at the point of sale, they can revert to the traditional process of accepting the exchange rate applied by their card issuer, when the transactions are posted to their statement.

Whilst the cardholder's account is debited in their local currency, your bank account will be credited in sterling so there's no need for you to hold currency accounts.

Please refer to 'HomeCurrencyPay' on page 50 for further details on our own DCC service.

FOREIGN CURRENCY TRANSACTIONS

Note: You can only accept MasterCard Credit, Visa Credit, Debit MasterCard, Visa Debit, Visa Electron, V PAY and Maestro cards issued outside the UK to undertake sales and refund foreign currency transaction types.

We can arrange for you to accept payment in a selection of foreign currencies, such as euro and US dollars. You can choose to have all your currency transactions credited directly to a nominated foreign currency account held with HSBC Bank plc, or to your sterling account. We cannot credit in currency amounts to a non-HSBC bank account, and you'll therefore need a foreign currency account with HSBC Bank plc for each applicable currency. If you choose to have your transactions credited to a sterling account, transaction amounts will be converted on the day the transaction is processed. MasterCard and Visa daily spot exchange rates for that day plus a variable margin will apply for all conversions. Details of the conversion charge and any subsequent changes will be notified where applicable. Charges will be converted on the date of calculation (usually the last business day of the month). We'll provide details of the rate on request.

Unless otherwise agreed, credits will be combined per currency, so that you'll have a single credit for each.

There are two methods for undertaking currency transactions:

- if you want to accept payments over the internet or by mail or telephone order, we recommend that you use our Global Iris service. See page 48 for more information on this service
- you can develop your own equipment to meet your specific currency requirements. We'll provide you with technical help and advice, system specifications and an approval process to make sure your equipment meets our requirements.

You must not use paper vouchers as Fallback for currency transactions if your equipment fails to read the card. Either undertake the transaction in sterling or ask the customer for another means of payment.

Remember that paper vouchers cannot be used as Fallback for Maestro, Visa Electron, V PAY Discover Global Network and UnionPay cards and Mobile POS Solutions, regardless of the currency of the transaction.

Each currency transaction should be authorised in the usual way. When obtaining telephone authorisation, you must quote the exact amount in the relevant currency. You must conduct transactions in foreign currencies within the UK only.

At the beginning of the month, we'll provide, or make available to you, an invoice for the previous month detailing the service charges relating to the transactions in all the currencies that we've processed for you that month. Charges for currency transactions will be shown and debited separately to your normal charges for sterling transactions.

If you would like further information about accepting transactions in foreign currencies please contact us on the number provided on page 86.

GRATUITIES

A gratuity is an additional amount added to a transaction by the cardholder, for example adding a tip when a cardholder settles a restaurant bill.

See your terminal user guide for further information.

HOTEL AND CAR RENTAL TRANSACTIONS

The Card Schemes have rules relating to these kinds of transactions. This section details the special procedures you need to follow when accepting these transactions. Your terminal must be configured for pre-authorisations. If you rent a terminal from us, please contact us (see page 86 for contact details) if you require this facility. Please also refer to your terminal user guide.

Note: Pre-authorisations are not available on Discover Global Network cards and UnionPay will only allow pre-authorisations on hotel transactions.

There are additional requirements for MasterCard authorisations. Please ensure you refer to 'MasterCard Authorisations' on page 20 to be aware of the fees you may be charged for these authorisations.

For the purposes of this section the guest or hirer is assumed to be the cardholder.

Reservations And 'No Shows'

- When taking the booking for both hotels and car rentals be sure to obtain the cardholder's name, statement address and phone number, their card number, and its start date (if available) and expiry date
- advise the cardholder of the accommodation or reserved vehicle rate, the exact name and physical address of the hotel or car collection location, and provide a confirmation code
- written confirmation of the reservation must be provided, including the transaction currency and your reservation and cancellation procedures, with any charges for 'no shows' that may be applied
- if you take a room reservation by MasterCard or Visa then you must guarantee to provide alternative accommodation of a similar or better standard, at no extra cost, if the reserved accommodation subsequently becomes unavailable
- if the cardholder cancels a reservation, a cancellation code must be provided
- for Visa – the cardholder should be allowed at least 72 hours prior to the scheduled arrival

date to cancel a reservation. A cardholder wishing to cancel a reservation that has been made within 72 hours of the arrival date must be allowed up to 6.00pm on the arrival day to make a cancellation. Unless the cardholder has cancelled the reservation, the reserved accommodation must be held until the check-out time on the day following the scheduled check-in date

- for MasterCard – the cardholder is required to cancel a reservation before 6.00pm on the day of arrival
- you can only charge a 'no show' fee for **one** night's accommodation or **one** day's rental (plus applicable tax). You must advise the cardholder of your policy at the time of reservation. A no show transaction isn't a guarantee of payment. Your hotel will be liable for any chargeback if the cardholder successfully disputes the transaction
- if a cardholder has paid a deposit in advance, but has decided to cancel or did not arrive, you may retain the advance deposit. However, you must not charge a 'no show' fee in addition
- when undertaking a 'no show' transaction, fill out a paper voucher as normal (see page 30) and write the words 'hotel reservation no show' or 'car rental/no show' on the signature line. This information will be useful if the transaction is charged back.

Check-in

- On arrival, ask the cardholder to sign the registration form, which states that they authorise you to debit their card. Check the signature matches the card
- a pre-authorisation should be made for either the full estimated bill amount (if above your floor limit) or £0 (if below the floor limit)
- advise the cardholder of the funds you've pre-authorised and explain how you calculated this amount (for example, length of stay/hire, room/car rental rate, applicable taxes, service charge rates/mileage rates)
- you can revise your initial estimate. On each occasion you should obtain a pre-authorisation for the **additional** amount.

Check-out

- You should key-enter the original pre-authorisation code and pre-authorised amount. You may need to undertake an additional authorisation if the final amount is:
  - above your floor limit for the first time
  - above the sum of your previous pre-authorisations (Visa allows a tolerance of plus 15%, MasterCard has no tolerance). Only obtain an authorisation for the difference between any pre-authorisation(s) and the final amount
- where possible, try to settle the final bill with the cardholder present and perform the transaction using PIN verification
- remember to cancel any unused authorisation codes, or if you've overestimated the pre-authorisation by more than 15% in the case of Visa transactions
- a priority check-out service can be offered but you will need to hold a Priority Check-Out contract with us. Once agreed, the cardholder must sign your company's 'Priority Check-Out Agreement' form, which must include the cardholder's mailing address. When the cardholder has checked out key enter the card details into the terminal adding 'priority check-out' to the signature line. Post a copy of the receipt to the cardholder within three business days of their departure.
- you're **not** allowed to store the Card Security Code (CSC). If you've stored this information, and at a later date it's compromised, you may be liable for a Card Scheme fine.

Note: MasterCard requires that the amount authorised is the same as the final transaction value that is sent for processing.

Additional Charges

Hotels may **not** submit an 'additional charge' transaction for loss, theft or damage at the hotel without the cardholder's permission. Such additional charges aren't guaranteed and can be charged back if the cardholder disputes the transaction, meaning financial loss to your business.

Visa permits delayed or amended charges due to rental car damage, for fuel, insurance, parking tickets, fines, rental fees and taxes, but you must be able to provide **all** of the following:

- copy of the rental agreement
- estimate of the cost of the damages from an organisation that can legally provide repairs in the car rental company's country
- police accident report (if applicable)
- documentation showing the cardholder's consent to pay for damages with their Visa card
- any other pertinent documentation available to demonstrate cardholder liability
- copy of the car rental insurance policy, if you require the cardholder to pay an insurance deductible for damages. In lieu of the car rental insurance policy, you may provide a copy of the car rental agreement confirming the cardholder's consent to be responsible for the insurance deductible. The cardholder must have signed or initialled close to the part of the form that details the insurance policy.

MasterCard and Maestro don't permit delayed or amended charges to be applied for car rentals. Any charges for loss or theft must processed separately and you must obtain the cardholder's permission.

PREPAYMENTS/DEPOSIT/INSTALMENTS

Pre-payments and deposits take place in advance of delivery of goods or services. This is also sometimes known as a 'delayed delivery' and is typically used for transactions where it's not possible to immediately supply the purchased goods, for example, a large piece of furniture that has to be made to order. In these instances you may require the cardholder to make the payment in advance for the whole amount in the case of a pre-payment or as two separate transactions, the first for the deposit and the second for the outstanding balance.

Instalment payments on the other hand are where three or more payments are taken towards a single purchase and may occur before or after shipping.

As these payment types pose additional risk to you, you'll require written approval from us before you can start to process these transaction types.

Note: These type of transactions are not possible on Discover Global Network and UnionPay cards.

PURCHASE WITH CASHBACK

Purchase with cashback (PWCB) transactions allow the cardholder to obtain cash at the same time as they purchase goods or services. This service is only available on debit cards and not on any UnionPay cards.

See your terminal user guide for further information.

Note: For Maestro cards, it's not possible to perform PWCB transactions using either the key entry functionality on your terminal or by swiping the magnetic stripe on a card. Any transactions accepted in this way will be declined when your terminal attempts authorisation of the transaction. If the cardholder wishes to obtain cash at the same time as they purchase goods or services they will need to present you with an alternative debit card.

RECURRING TRANSACTIONS

Recurring transactions refers to when the cardholder has given you authority to debit their account on a pre-determined basis (for example, monthly, quarterly or annually) to cover the provision of goods or services. The amount can always be the same, as for most insurance premiums or can fluctuate from one payment to the next, for example as with a telephone or utility bill.

Note: Recurring transactions are only allowed on MasterCard (excluding Maestro) and Visa (excluding internationally issued Visa Electron) cards.

Understanding The Risks

- Any recurring transaction processed after the cardholder has cancelled their authorisation will result in a chargeback
- recurring transactions offer no guarantee of payment and are undertaken at your own risk
- if the cardholder queries the transaction, you must not process any further transactions.

How To Set Up A Recurring Transaction Agreement

You must have your customer's written consent to the recurring transaction before you process the initial transaction. We recommend you design a recurring transaction agreement form for this purpose. The agreement form must include:

- cardholder's name, address and contact telephone number and the method of communication for all your correspondence with them
- card type, card number and expiry date
- transaction amount and whether the payments remain fixed or are variable and if they are subject to change, for example, because of VAT or tax variations
- frequency of payment including the date the recurring transaction will be processed and whether the date is fixed or variable
- agreement term and the date when the agreement expires
- cardholder's consent to the agreement.

Once the cardholder has given their consent, you must provide them with confirmation of the recurring transaction agreement within two business days using the agreed method of communication.

If you accept transactions over the internet, you can include agreement information on your website and the customer can confirm their acceptance either in an email or via an 'I agree' option on your web page. The customer's electronic response must be recorded and be capable of being provided in the event of a disputed transaction or chargeback request.

Please also ensure that:

- for non-specific amounts, the cardholder must be advised in writing of the exact value at least 14 days prior to each charge being made
- you keep the cardholder's written/email authority for five years from the date of the final charge or cancellation of the authority (see page 71 regarding 'Data Security')
- you advise the customer that they can cancel the agreement at any time and you provide details of how they should notify you of the cancellation
- you act on cancelled instructions promptly
- the card data is held securely and doesn't include the cardholder's CSC.

How To Undertake Recurring Transactions

The first transaction must be taken in the most secure way, for example using chip and PIN for card present (CP) transactions, using Address Verification Service (AVS) and Card Security Code (CSC) for mail order or telephone order (MOTO) transactions (see page 80) and using MasterCard SecureCode or Verified by Visa for ecommerce transactions (see page 80).

If no payment is required when the recurring transaction is being initiated, you must submit a zero value status check (see page 25). If the card issuer provides a non-approval response to the status check, no subsequent recurring transaction can be submitted under the recurring transaction agreement. You will need to contact the cardholder to provide an alternative form of payment.

Additional authentication isn't required for subsequent transactions.

Note: You **must not** undertake subsequent recurring transactions by key-entering card details into our electronic terminals or using paper vouchers. They can only be processed using our Global Iris service (see page 48), a Payments Service Provider (PSP) (see page 35) or using your own equipment/systems (see page 35).

Important additional points to note are as follows:

- if the cardholder tells you their card has been lost or stolen, you must cancel the existing arrangement and make sure no further transactions are undertaken
- a new authority must be completed if transactions are to continue on a different card account
- you must provide a simple and easily accessible cancellation procedure
- you must ensure that cancellation instructions are actioned immediately at the customer's request. This will ensure that no more claims are originated and will help avoid chargebacks
- you must notify customers of any changes to a recurring transaction (see following section)
- if customers are offered a free trial introductory period, the cardholder must be given sufficient notification of the expiry of the fee-free period (see following section)
- once a card has expired, you must contact the cardholder asking for details of their new card and confirm that they wish to continue with the agreement
- you should only attempt to authorise a recurring transaction once per day. If you receive a decline you should not attempt to authorise the transaction again until the following day. Attempts to authorise can be made for a maximum of 31 consecutive days. After this time, you must cease and contact the cardholder for an alternative method of payment
- you must allow customers to choose their preferred date for regular payments, so that they can select a date when they're confident they will have funds in their account
- transactions must not include any additional finance charges or one-off payments for products or services purchased
- wherever possible, include the correct expiry date for these transactions. Authorisation may

be declined if the expiry date is incorrect, invalid or missing
- the transaction must be correctly flagged as a recurring transaction.

Notification Of Changes To A Recurring Transaction Agreement

You must notify the cardholder, using the agreed method of communication, at least seven business days prior to the recurring transaction being taken in any of the following situations:
- more than six months have elapsed since the last payment
- a trial period, introductory offer or promotional activity has expired
- there are changes to the recurring transaction agreement, including but not limited to:
  - any change to the amount and/or
  - any change to the date of the recurring transaction.

Recurring Transaction Enquiry Service

Global Payments is able to support you using the Recurring Transaction Enquiry Service.

The Recurring Transaction Enquiry Service is a solution to enable you to cross-reference your portfolio of card details against the card issuers' records, and receive up-to-date information on expired and re-issued cards. The service is designed to reduce the amount of chargebacks and rejected transactions encountered from processing recurring transactions. It also serves to reduce the operational impact of having to contact the cardholder directly to request the correct card details.

Cardholders can stop payment of these recurring transactions via their card issuer. Any instruction received to stop a recurring transaction authority must be actioned, otherwise the transactions can be charged back. The service provides an early warning of a cardholder's intention to stop a recurring transaction authority and therefore enables you to contact the cardholder to discuss the arrangement. Please also refer to VEPSS on page 37.

Note: This is a mandatory solution required by MasterCard and Visa. We'll contact you if you're affected by this requirement.

globalpayments

GLOBAL IRIS

The Global Iris service is designed to offer you the ability to accept CNP transactions by integrating the system into your own PC based systems. The service allows you to accept two types of orders from your customers:

- ecommerce transactions – orders taken online from your website
- mail and telephone order (MOTO) transactions – orders that are manually entered to Global Iris.

Global Iris is a browser-based solution, which means you can set up with no need for software installation and you benefit from automatic updates, including the latest in security and PCI DSS compliance requirements.

Following your enrolment to Global Iris, you can benefit from:

- **Simple payment processing.** The online payment screens are simple and easy-to-follow. Likewise, your administrative and management information (MI) pages have been designed for maximum ease of use.
- **Comprehensive service.** Global Iris provides many features including payer authentication and web-based reporting.
- **Transactional security.** The system supports both MasterCard SecureCode and Verified by Visa for internet transactions.
- **Accepts multiple currencies.** Global Iris supports payments in a variety of international currencies.
- **Reduced PCI DSS compliance effort*.** The service is hosted by Realex Payments who are fully accredited with Level 1 PCI DSS by MasterCard and Visa. Their systems and security controls are based on current industry standards and have several layers of technology in place to ensure confidentiality, authentication and integration of information, making your journey to achieve PCI DSS compliance easier.
- **Increasing control.** You maintain control over the payment page, including the design of the website checkout.

*This isn't the case if you're using the Remote platform (see below). You'll be required to achieve and maintain your own PCI compliance.

The Global Iris service options:

- **Virtual Terminal** – a solution for merchants taking credit and debit card payments over the phone, either in a small office or a larger operation such as a call centre. The Virtual Terminal application allows an agent to enter card details and then authorises the card for payment.
- **Re-direct** – a hosted application which allows you to redirect customers from your website to a secure payment environment, where the customer can enter his/her card details to complete

the payment. Once the transaction has been processed, we'll return the response of the transaction to a nominated response page on your servers so that your system can automatically update with the details of the transaction. The customer can then be returned to a page on your servers.

- **Remote** – Global Iris can be integrated remotely into your site giving you control over the screen flow. This is possible using an Application Programming Interface (API) via the secure exchange of XML messages. The API allows for the remote submission of a number of different request types which allow you to process card payments.

Global Iris comes complete with the tools to manage and greatly reduce the exposure to fraud faced in a CNP environment, including:

- 3D Secure Payer Authentication
- fraud scoring/transaction screening
- Card Security Code (CSC) checking
- Address Verification Service (AVS) checking.

If you would like to know more about Global Iris, please contact us (see page 86 for contact details).

For further information on how to utilise the Global Iris service, refer to the customer guides located online at: https://resourcecentre.globaliris.com/.

HOMECURRENCYPAY

AN INTRODUCTION TO HOMECURRENCYPAY

HomeCurrencyPay is Global Payments' Dynamic Currency Conversion (DCC) service and offers an opportunity for you to welcome international cardholders who prefer to pay for MasterCard or Visa purchases in their home currency.

Whether cardholders are on holiday, travelling on business or visiting your website, HomeCurrencyPay gives your customers the **choice** to pay for goods and services in their home currency or sterling.

HomeCurrencyPay helps your international customers to easily calculate how much they're spending. When you accept a payment card that is issued in another country, your HomeCurrencyPay enabled Point of Sale (PoS) equipment or website payment page will detect a supported foreign currency on the card. The PoS or the payment page will then present the cardholder with the option of which currencies they can pay in. The choice is theirs.

Regardless of what your customer decides, you'll be credited in sterling so your reconciliation process is unaffected.

Cardholder Benefits

Providing HomeCurrencyPay to your international customers eliminates the uncertainty over the actual cost of the purchase because the cardholder can pay in their home currency. The sale amount the cardholder sees on their till receipt or on your website payment confirmation page and email is the exact sale amount that will be charged for the purchase to their account.

If HomeCurrencyPay isn't chosen and the transaction is completed in sterling, the exchange rate applied to the transaction is unknown to the cardholder as this will be done later by the card issuer. This means the cardholder has no way of knowing the actual cost on the day of purchase.

We also closely monitor the exchange rate to ensure the rates used are comparable with those used by card issuers.

In summary, the benefits to the cardholder are:

- instant conversion to their home currency
- up-to-date exchange rates
- improved customer service at the point of sale
- helps to simplify business travellers' expense claims
- full costs easily identified.

Merchant Benefits

HomeCurrencyPay improves your appeal to those travelling on holiday or business. By giving international cardholders choice to pay in either sterling or their home currency they're informed of exchange rates while making purchases.

With no set-up fees or ongoing fees for HomeCurrencyPay, every time a cardholder completes a purchase with HomeCurrencyPay; you receive a Merchant Commission.

Merchant Commission: This is a percentage of each HomeCurrencyPay transaction you take, and the rate agreed will appear on your *Service Schedule* or any more recent communication from us. A credit for the total Merchant Commission paid on HomeCurrencyPay transactions will appear in the 'Other Fees' section of your monthly invoice.

The commission you'll receive is calculated at the beginning of each month for the HomeCurrencyPay transactions you've submitted in the prior calendar month and credited to you on your monthly invoice in the subsequent month. Thus, by way of example, for transactions submitted in January, the total of your Merchant Commission will be calculated at the beginning of February and be reflected on your February monthly invoice received at the beginning of March.

What Currencies May Be Converted?

All major international currencies can be converted via HomeCurrencyPay. An up to date list of the currencies is available on our website at www.globalpaymentsinc.co.uk. The list can be found on the 'HomeCurrencyPay' page, under 'Products & Services'.

If a currency doesn't qualify for HomeCurrencyPay, it will be processed in sterling.

Exchange Rates

HomeCurrencyPay exchange rates are updated regularly and are based on Reuters' wholesale rates, a globally recognised rate provider in the financial market. The rates we use are comparable with those used by card issuers.

The rate of exchange applied to a transaction is provided to the cardholder at the point of sale or on the website payment confirmation page, prior to completing the sale. It's then printed clearly on all transaction receipts.

Every foreign currency transaction converted by a payment card processor uses a margined rate. The margin applied by Global Payments to the wholesale rate in a HomeCurrencyPay transaction is clearly indicated on the transaction receipt.

CARD PRESENT (CP) HOMECURRENCYPAY TRANSACTIONS

Your PoS equipment will be updated to include the HomeCurrencyPay software when you've signed up for this additional Service.

A HomeCurrencyPay transaction will start the same as any other card payment. Ensure you follow the guidance provided in these *Merchant Operating Instructions* for all CP transactions. You'll still enter the sterling transaction amount as normal. When the cardholder presents their card for

payment and it's swiped, inserted, or hand-keyed etc. on the PoS device, the software on the device will detect that the card is an eligible card.

The following will then take place:
- the PoS device identifies the cardholder's home currency
- the sale amount is displayed in both the cardholder's home currency and sterling
- if you're equipped with an electronic PoS system, a dialog is displayed indicating the sterling amount, cardholder's home currency amount, exchange rate, exchange rate date, exchange rate source and the rate margin
- you must inform the cardholder that DCC is an **optional** service while at the same time describing the benefits of the Service. Refer to the 'Cardholder Benefits' section on page 50 and some 'Suggested Phrases' on page 52
- if the cardholder has any questions about the DCC service, refer to the 'Frequently Asked Questions' section on page 59
- ask the cardholder how they would like to pay – either in sterling or in their home currency.

Cardholder Chooses To Pay In Their Home Currency

The cardholder must verify their selection on the PIN pad (if applicable).

Depending on whether the card presented is MasterCard or Visa, the type of PoS device you use and who you rent it from, a receipt will be generated showing some or all of the following information:
- sale amount in sterling
- exchange rate
- exchange rate date
- sale amount in cardholder's home currency amount
- rate margin
- rate source, for example, Reuters
- the DCC provider, which in this case is Global Payments
- acknowledgement that the cardholder was presented with a payment choice.

Cardholder Chooses To Pay In Sterling

The cardholder must verify their selection on the PIN pad (if applicable).

The transaction will be completed in sterling and the cardholder won't know what the final cost of the purchase is until they receive their account statement in their own currency. For MasterCard and Visa transactions, no disclosure on applied rates is provided at the point of sale.

Suggested Phrases

The following suggested phrases may be used when offering currency choice to cardholders at today's conversion rate. In these examples, the transaction is for an Australian tourist shopping in London.

- "Would you like to pay in sterling or in your home currency?"
- "Sir/Madam, do you wish to pay in Australian Dollars or in sterling?"
- "In which currency would you like to pay, Australian Dollars or sterling?"
- "Dynamic Currency Conversion (DCC) removes the exchange rate risk from your transaction."
- "The Australian Dollar sale amount for your purchase is the same sale amount that will appear

on your account statement should you choose to pay in your home currency."
- "Please confirm your selection on the PIN pad."
- "Please confirm the amount and enter your PIN."

DO
- offer the cardholder the choice to pay in either sterling or the cardholder's home currency
- use the aide we provide to explain the DCC service to cardholders in all major languages. Please contact us (see page 86 for contact details) for further supplies of this HomeCurrencyPay Language Card.

DON'T
- confuse the cardholder when choosing the payment currency
- assume the cardholder's preference. The cardholder must make the choice themselves and must opt in to the HomeCurrencyPay Service.

MAIL ORDER AND TELEPHONE ORDER (MOTO) HOMECURRENCYPAY TRANSACTIONS

If you process MOTO transactions by key-entering the transaction into your PoS device you can offer the HomeCurrencyPay Service to your customers as long as you incorporate a way of communicating the information in this section. This can either be communicated verbally over the phone or written on an order form.

Your PoS device will be updated to include the HomeCurrencyPay software when you've signed up for this additional Service.

Mail Orders

The following considerations must be included on your Mail Order form:
- a statement that international cardholders may have the option to pay in their home currency when the transaction is being processed by you at the point of sale
- a statement that the facility to pay in his/her home currency is only available to MasterCard and Visa cardholders
- the reference exchange rate sourced daily by (name of organisation that rates are sourced from, currently Reuters). The actual name cannot be included/hard coded due to potential future reference rate source changes. Your contact details must be included on the form for cardholder queries regarding rate source etc.
- the international conversion margin applied to the reference exchange rate, for example 3.5%
- a statement advising the cardholder that the exchange rate used will be determined at the time the transaction is processed at the point of sale and without further consultation
- the cardholder is required to indicate whether they accept or decline DCC by either:
- ticking their preferred option, for example:

Please tick preferred payment option:

Pay in my home currency (euro, US dollar, etc.) ☐

Please indicate your home currency here: _____

Pay in sterling ☐

Note: The click/tick box must not automatically default to any particular option. The cardholder is required to make a selection.

- ticking a box indicating that they accept DCC (i.e. opt-in to DCC). For example:

> If you are an international cardholder paying by MasterCard or Visa, you may have the option to pay in your home currency when the transaction is being processed at the point of sale. Please tick below to utilise this facility.
>
> **Conversion into my home currency accepted** ☐
>
> My card currency (insert): _____

Note 1: A tick box to decline DCC (opt-out) isn't acceptable.
Note 2: The tick/click box must not be ticked, clicked or highlighted by default.

- a statement advising cardholders that if their chosen card currency isn't identified when processing the transaction at point of sale, the transaction will be processed in sterling
- a statement advising cardholders that if no box has been ticked, the transaction will be processed in sterling
- details of the DCC provider, which is Global Payments in this case.

Sample Order Form Text

If you are an international cardholder paying by MasterCard or Visa, you may have the option to pay in your home currency when we process the transaction at the point of sale. Please tick your preferred payment option below.

I choose to pay in my home currency ☐

(insert currency here):_____

Currency conversion will be based on a wholesale exchange rate plus a 3.5% international conversion margin. The exchange rate used will be determined when the order is processed and without further consultation. Exchange rates are sourced from (Reuters*). The Dynamic Currency Conversion service is provided by Global Payments.

I choose to pay in sterling ☐

The transaction will be converted into your home currency at a rate of exchange on the day the transaction is presented to your card issuer. Currency conversion charges normally apply.

Note 1: We can perform currency conversion on cards that have been issued in certain currencies only. A card issued in any other currency will be processed in sterling.

Note 2: Where a box has not been ticked; the transaction will be processed in sterling.

Note 3: Please contact us if you require details of the wholesale exchange rate used. The exchange rate source will be printed on the order confirmation.

*This must not be hard coded in case rate source changes in future.

Telephone Orders

A HomeCurrencyPay transaction will start the same as any other card payment. Ensure you follow the guidance provided in these *Merchant Operating Instructions* for all MOTO transactions. You'll still enter the sterling transaction amount as normal. When you key-enter the card details on the PoS device, the software on the device will detect that the card is a HomeCurrencyPay eligible card and identify the cardholder's home currency. The terminal will display the sale amount in both the cardholder's home currency and sterling.

Advise the caller of the following:

- that you have the facility to charge them in their home currency

- the sale amount in the cardholder's home currency and sterling
- inform the cardholder that DCC is an **optional** service whilst describing the benefits of the Service. Refer to the 'Cardholder Benefits' section on page 50
- if the cardholder has any questions about the DCC service, refer to the 'Frequently Asked Questions' section on page 59
- the rate of exchange used for the transaction is sourced daily from Reuters (a recognised supplier of foreign exchange rates) and is competitive and is comparable with the rate applied by card issuers
- an international conversion margin is included in the rate. Every foreign currency transaction converted by a payment card processor uses a margined rate
- if the transaction isn't processed at the time of the call, the sterling amount will be converted to their home currency at the rate of exchange (including conversion margin) in use when the order is processed.

DON'T
- confuse the cardholder when choosing the payment currency
- assume the cardholder's preference. The cardholder must make the choice themselves and must opt in to the HomeCurrencyPay Service.

Confirming Orders

The order confirmation that is sent as part of the MOTO transaction must also include the following when HomeCurrencyPay has been chosen.

- the amount in sterling
- the exchange rate applied
- the exchange rate date
- the total price in the chosen currency (including the currency symbol), accompanied by the words "Transaction Currency"
- "Reference exchange rate sourced daily by (name of organisation that rates are sourced from, currently Reuters)". This must not be hard coded in any standard emails, letter etc. in case rate source changes in future
- the international conversion margin applied to the reference exchange rate, for example 3.5%
- declaration that cardholder had a choice of currencies for payment including sterling and the cardholder chose to pay in their home currency (currency must be identified)
- declaration that cardholder's choice of currency is final
- "Dynamic Currency Conversion is provided by Global Payments."

Note: Where possible, we recommend that the cardholder is sent the customer copy of the transaction receipt as the correct declaration is detailed there.

ECOMMERCE HOMECURRENCYPAY TRANSACTIONS

If your pricing currency on your website is sterling, you can offer the HomeCurrencyPay Service to your customers. Your ecommerce facility will be updated to include the HomeCurrencyPay software when you've signed up for this additional Service.

Ensure the transaction amount of goods and/or services you supply are displayed on your web page in sterling.

When the cardholder enters their card number on the secure web page for payment, the software on the web page will detect that the card is a HomeCurrencyPay eligible card.

The following will then take place:

- the currency recognition software on the web page identifies the cardholder's home currency
- the sale amount is displayed in both the cardholder's home currency and sterling
- the exchange rate and the rate margin are clearly displayed
- the web page displays a statement that informs the cardholder that DCC is an **optional** service and the interface presents the cardholder with the **option** to select payment either in sterling or in their home currency
- terms and conditions are clearly available to the cardholder, and the cardholder must confirm they've read and accept to authorise the card payment.

Cardholder Chooses To Pay In Their Home Currency

Depending on whether the card presented is MasterCard or Visa and the provider of your ecommerce solution, the payment confirmation page/email will show some or all of the following information:

- sale amount in sterling
- exchange rate
- exchange rate date
- cardholder's home currency amount
- rate margin
- rate source, for example, Reuters
- DCC provider, which in this case is Global Payments
- declaration that cardholder had a choice of currencies for payment including sterling and the cardholder chose to pay in their home currency (currency must be identified)
- declaration that cardholder's choice of currency is final
- this confirmation information will be sent by email to the cardholder's email address.

Cardholder Chooses To Pay In Sterling

The transaction will be completed in sterling and the cardholder won't know what the final price of the purchase is until they receive their account statement in their own currency. For MasterCard and Visa transactions, no disclosure on applied rates is provided.

A confirmation page will be displayed showing the sale and payment in sterling. This confirmation information will also be sent by email to the cardholder's email address.

MASTERCARD AND VISA REGULATIONS

All DCC services are regulated by MasterCard and Visa and as HomeCurrencyPay is a DCC service it's subject to these DCC regulations. The fundamental principles are:

- the cardholder has a **choice** to pay in sterling or their home currency
- the cardholder is given the **choice** to accept or decline DCC
- the terms and conditions associated with DCC are fully disclosed.

We provide the HomeCurrencyPay Service in compliance with the regulations by ensuring you satisfy the requirements as follows:

- you must make cardholders aware that your DCC service is an optional service and that the

cardholder has the choice to pay in sterling, if they prefer. Don't use any language or procedures that cause the cardholder to choose DCC by default

- don't make claims for the DCC service that are incorrect or cannot be substantiated
- the cardholder's home currency must be confirmed before authorisation takes place. The currency recognition software does this automatically
- sterling remains the default currency on any transaction. However, where an eligible card is identified, the cardholder will be given the choice to decide which currency to pay with. Don't use language or procedures that may make paying in sterling difficult
- the DCC service is fully transparent and the DCC receipt is printed with the transaction amount in sterling, the cardholder's home currency, exchange rate, the exchange rate date, the rate source, the rate margin, and the service provider, which is Global Payments in this case. For online transactions, these details must also be displayed on the website payment confirmation page, and they must also be included on the order confirmation sent by email or post for online and MOTO transactions
- all relevant DCC information must be made available to the cardholder before the transaction is completed. This information is readily available at the point of sale to you and the cardholder, and subsequently printed on the receipt
- to assist you with this process, this document includes the optimum ways to offer HomeCurrencyPay, depending on the type of transaction you process, i.e. Card Present, MOTO or ecommerce
- training for all staff at the point of sale offering HomeCurrencyPay is a Card Scheme requirement. Training is provided by us (or a third party on our behalf) as part of the set-up process or by completing the training module, which is available on our website at www.globalpaymentsinc.co.uk. The module can be found on the 'HomeCurrencyPay' page, under 'Products & Services'. You must ensure that the appropriate staff are trained and the training is kept current, including training for any new staff employed after the initial staff training has taken place
- as a result of the training, you ought to be comfortable and confident with explaining the process to your customers so they can understand the benefits to them. See the 'Cardholder Benefits' section on page 50.

Note: From time to time MasterCard and Visa audit merchants who are enabled with a DCC service to ensure these regulations are being followed.

REFUNDS

MasterCard and Visa have mandated that refunds must, where possible, be performed in the currency of the original transaction at the prevailing rate. For example, if the cardholder has paid in US dollars then the refund must be processed in US dollars.

As part of the refund process you're required to have sight of the original transaction receipt or refer to the original transaction in the case of MOTO or ecommerce transactions, before completing a refund. This will confirm the currency that was used for the original transaction and ensure the refund is completed in the correct currency.

Note: The HomeCurrencyPay option must not be applied if you cannot confirm the charging currency of the original transaction.

HOTEL AND CAR RENTAL TRANSACTIONS

In addition to the guidance provided in the rest of this document for all HomeCurrencyPay transactions, you must also the follow the sections below for those completed in a hotel and car rental environment.

Check-in

At check-in:

- you must explain the DCC service
- verify the card billing currency and ensure the cardholder is offered the choice of paying in sterling or in their home currency. Give the cardholder the day's exchange rate as an indication and you must advise that the exchange rate may be different at the time of final payment due to currency fluctuations
- tell cardholders who agree to DCC in advance that they will be able to change their currency billing preference before payment is made
- if a cardholder changes their mind about the currency they use to settle their final bill, you must cancel the authorisation code provided for the preauthorisation
- advise the cardholder of the exchange rate source (for example, Reuters) and the rate margin.

Check-out

As it isn't always possible to provide the cardholder with information on the transaction currency amount or the exchange rate that will be used when booking or checking in, if you provide an 'Express Check Out' service, you may need to perform some additional steps when processing DCC HomeCurrencyPay transactions.

Where required, you must obtain written agreement from the cardholder that demonstrates the following points:

- the cardholder is provided with the option to pay in either sterling or their home currency (the currency in which the card is issued)
- the accepted choice of home currency payment is final
- the transaction currency is agreed to by the cardholder
- the exchange rate, rate source, and the rate margin are clearly indicated
- the cardholder is aware that the exchange rate used for future charges will be determined, without further consultation, when the transaction is processed.

FREQUENTLY ASKED QUESTIONS

This section covers off some typical questions asked by merchants and customers about what the HomeCurrencyPay/Dynamic Currency Conversion (DCC) service is and how it works.

General Questions

What is HomeCurrencyPay?
HomeCurrencyPay is the name for Global Payments' DCC service.

What is DCC?
DCC stands for Dynamic Currency Conversion and describes the service whereby international

cardholders can pay for goods and services in the currency of their card rather than the pricing currency of the merchant.

What card types support HomeCurrencyPay?
The service is offered to MasterCard and Visa cardholders only.

What currencies are supported by HomeCurrencyPay?
This service is available on all major currencies. The software is designed to identify these currencies automatically. An up to date list of the currencies is available on our website at www.globalpaymentsinc.co.uk. The list can be found on the 'HomeCurrencyPay' page, under 'Products & Services'.

Who provides the DCC service?
Global Payments.

Merchant Questions

How much training is required for my team(s)?
Your point of sale team will need about 15 to 20 minutes to understand how the process works and how to offer the service.

It sounds complicated – will my staff have to understand the financial markets to support this service?
The service is driven by the software and pops up automatically when a HomeCurrencyPay eligible card is identified. All your team has to do is offer the DCC service to the cardholder.

How are refunds processed?
Refunds must, wherever possible, be processed in the currency of the original transaction. The exchange rate used must be the prevailing rate on the day of the refund. This may be different from the rate use in the original sale transaction.

Why can't I just put all refunds through in sterling?
If the original transaction was processed via HomeCurrencyPay, then the refund must also be processed via HomeCurrencyPay. However, if you're not sure, MasterCard and Visa insist you default to sterling for refunds.

How do I know when a card is eligible for DCC?
The software has a card look up facility that identifies the country the card was issued in. This happens automatically so there's no need for you to remember what currencies are supported.

What do I do if the cardholder says no?
It's the cardholder's right to choose to process the transaction in sterling. If they say no to the service then you must process it as a non HomeCurrencyPay transaction.

Will my customers be surprised when I offer DCC?
DCC has become very popular over the past few years and your international customers won't be surprised to be offered the choice to pay in their home currency.

Do I have to tell/show my customers how much the bill is in both currencies?
Yes, you must tell the cardholder how much their purchase costs in both currencies. This information must be clearly shown on your website payment page and also on the till receipt.

Will my customers have come across DCC before?
Most likely. This product is available worldwide and most international travellers will have used it before.

Why is DCC a good option for my corporate/business customers?
DCC makes their expense claim process much simpler. It also helps when a businessman is restricted to adhering to a budget as DCC ensures the cardholder knows the exact sale amount of each purchase.

Why is DCC a good option for my tourist customers?
The amount for which the customer signs or enters their PIN number is the exact sale amount that is charged for their purchase and what will appear on their account statement.

Note: Some card issuers may apply a fee.

How do I reconcile my DCC transactions?
As DCC transactions are simply sterling credits to your bank account they're not dealt with differently to your other MasterCard and Visa transactions and you'll receive one combined credit. If you want to know which transactions are DCC, you can find this out by looking at your sales receipts. If you have any other queries about reconciliation, please contact us (see page 86 for contact details).

Systems

Will I need a separate processing system to support HomeCurrencyPay?
No. The software sits on a HomeCurrencyPay compatible PoS device, which can be rented from us. If you utilise our Global Iris facility, HomeCurrencyPay is also available for online card processing. If you own your own PoS equipment or rent from another terminal provider, or use a PSP to accept your online transactions, please contact us (see page 86 for contact details) to see if it's compatible. You won't see any processing differences.

Rates And Margins

Can I set my own rates and margins?
No. The rates are derived by Global Payments and distributed throughout the day. These rates are carefully monitored and controlled to ensure your customers get the best service available.

Do I have to enter the rates and margins manually each day?
No. The PoS device is updated automatically.

How often is the rates file updated?
The rates are updated throughout the day.

Where do the rates come from?
The rates we use are based on Reuters' wholesale rate, a globally recognised rate provider in the financial market.

Regulations And Compliance

Do MasterCard and Visa audit this service?
Yes. MasterCard or Visa may undertake site checks to ensure you're offering the service correctly.

Cardholder Questions

Why would I choose Currency Conversion at point of sale?
By choosing conversion at the point of sale, your transaction will be converted into your card currency at the rate of exchange (including the rate margin quoted) in use at the time the transaction is being processed.

Where do the exchange rates come from?
The rates we use are based on Reuters' wholesale rate, a globally recognised rate provider in the financial market.

Is there a charge associated with this service?
The HomeCurrencyPay Service itself is free of charge.

Note: Every foreign currency transaction converted by a payment card processor uses a margined rate to cover the cost of the conversion. Equally if you choose to pay in sterling and not utilise the Service, your card issuer will usually add a margin when they do the currency conversion of the sterling transaction to your home currency before debiting it to your account.

What if I decide to pay in sterling?
The transaction will be processed at the point of sale in sterling. The transaction will be routed via MasterCard and Visa to your card issuer who will convert the transaction at a rate of exchange on the day the transaction is presented to them. The rate of exchange applied may be less favourable depending on currency fluctuations between the time of the transaction and the time it's presented to your card issuer for a conversion.

Does my card issuer charge a margin?
Normally, a card issuer will apply a margin/fee/charge for processing transactions that are presented to them in a foreign currency.

If you have any other questions about HomeCurrencyPay, please call us (see page 86 for contact details)

globalpayments

CREDITS AND DEBITS TO YOUR BANK ACCOUNT

CREDITS TO YOUR BANK ACCOUNT

Timescales For Our Processing

Following receipt of your transactions, we'll transmit them to the relevant card issuers to request payment on your behalf (see 'Processing of Transactions' on page 29). Amounts which we receive from card issuers in respect of your transactions will be held to your account in our books and records on the same business day that we receive them. Payment will be made to your bank account, or otherwise, as set out in the *Terms of Service*, for example, into any Reserve Account which we maintain for you. Timescales for the payment will be in accordance with the *Service Schedule*, or as agreed otherwise in writing, but generally you'll receive cleared funds in your bank account by the third business day after we receive your transactions for processing. The date the credit appears on your account is dependent on your account holding bank.

Timescales For Your Credit

The following is a guide to when you should expect any payments to be credited to your bank account:

- if you process cards electronically, and your bank account is held with HSBC Bank, you should be credited with uncleared funds the next business day following successful receipt of your transactions. These funds should clear within the next two business days and will be available for withdrawal the business day **after** they've cleared
- if you bank elsewhere, you should be credited with cleared funds the third business day following successful receipt of your transactions and will be available for withdrawal the business day **after** they've cleared.

Examples of typical Crediting Timescales are:

Monday	- transaction undertaken
late Monday/early Tuesday	- transaction sent to us
late Thursday	- funds clear
Friday	- funds are available for withdrawal.

Note: Typically, Crediting Timescales for Discover Global Network and UnionPay transactions take a day longer than the above example.

Crediting days are Monday to Friday, excluding public holidays.

Note: UnionPay transactions are also subject to the Chinese public holidays listed below. These are non settlement days. For the specific dates of these holidays please contact us (see page 86 for our contact details).

- New Year's Day
- Spring Festival, Chinese New Year
- May Day/Labour Day
- Dragon Boat Festival
- National Day of China.

If you've processed cards using Fallback paper vouchers, you should receive cleared funds within

three business days of our receiving the paper vouchers. These funds will be available for withdrawal the same day as they're credited to your account.

Examples of typical Crediting Timescales are:

Monday	- transaction undertaken
Tuesday	- Fallback paper vouchers received
Wednesday/Thursday	- transaction processed
Friday	- funds are available for withdrawal.

Crediting Timescales may vary if:

- a different Crediting Timescale has been agreed as per your *Service Schedule* or otherwise in writing
- you don't complete your terminal 'banking' procedures every day
- we've agreed any other arrangements in writing
- you haven't followed the *Merchant Operating Instructions*.

Bank Statement Entries

MasterCard And Visa: Unless we've agreed otherwise with you in writing, we'll credit your nominated bank account with a single credit for these card types, irrespective of whether the transactions have been processed both electronically and using Fallback paper vouchers or solely electronically.

Unless we've agreed otherwise, the narrative that appears on your bank statement will be 'CARD TRANS DDMMYY', where DDMMYY is the transaction date.

If you only process cards using paper vouchers, you'll receive a single credit for MasterCard, Visa Credit and Visa Debit. Each credit will represent the total value of all transactions for that group of card types processed by us on a given day.

Discover Global Network And UnionPay: The narrative that appears on your bank statement will be 'DI NNNNNNNN DDMMYY' or 'UP NNNNNNNN DDMMYY', where:

- DI = Discover Global Network or UP = UnionPay
- NNNNNNNN = your outlet ID/Merchant Number
- DDMMYY = the date the transactions are submitted to BACS for processing.

You'll see a bulk net credit for each card type containing the relevant days' transactions.

Transactions taken during non-banking days will be included in the next business day's settlement file. For example, any transactions accepted after the cut off time on Friday, together with all the transactions taken on Saturday and Sunday, will be included with the transactions taken up to the cut off time on Monday.

REJECTED TRANSACTIONS

As part of our transaction validation process, we'll reject and return any transactions that fail validation, for example, an expired card has been used. Rejected transactions will result in financial loss to you.

Before this happens, we'll check the transaction details and our systems. If we identify any errors,

these will be corrected. If this doesn't resolve the problem, we'll advise you by letter and the amount credited to your bank account will be adjusted accordingly.

Where a complete transaction file is rejected, we'll contact you by telephone and advise you of the corrective actions you'll need to take to avoid no funds being credited to you.

SERVICE CHARGES

This is the amount payable by you for our card processing services.

Please refer to your *Service Schedule* for details of your service charges, or any more recent communication from us.

How Will We Collect Service Charges?

MasterCard And Visa: At the beginning of the month, we'll provide, or make available to you, an invoice for the previous month detailing the service charges relating to the transactions that we've processed for you that month. It will also include other charges due, such as terminal rental, authorisation fees or stationery charges. We normally collect all service charges one month in arrears.

One combined debit will then be taken from your nominated bank account on or around the 15th of each month. The description appearing on your bank statement will be 'GLOBAL PAYMENTS'.

Discover Global Network And UnionPay: A separate monthly statement will be posted to you during the first week of the new month detailing the Discover Global Network and UnionPay credit entries and charges made by us.

Service charges for these card types are deducted from the value of the transaction before being credited to your nominated bank account. This is known as Net Settlement. Therefore, you won't see a separate debits for these charges.

RECONCILLIATION

We strongly recommend that you reconcile all your bank account entries on a monthly basis. Please call us (see page 86 for contact details) at the earliest opportunity if you have any queries about your card processing statement entries.

UNDERSTANDING YOUR INVOICE

If you have any queries regarding your invoice, we have a guide called *Your Invoice Explained*, which can help you understand and reconcile your invoice. You can view this by visiting our website at www.globalpaymentsinc.co.uk and logging into our Customer Centre. A copy can also be found in the 'Help' section of our eStatements service.

CHARGEBACKS

INTRODUCTION

A chargeback is a transaction that has been disputed by the cardholder or card issuer and returned to us. A chargeback is also known as a 'dispute'.

Each chargeback has specific rules, regulations and time limits within which Global Payments must operate. These are set by MasterCard and Visa and influence the actions we're able to take when dealing with chargebacks. We'll do everything possible within the rules to defend the chargeback on your behalf.

There are a number of different reasons why a transaction can be charged back, but they mainly fall into five categories:

- request for information (see 'What Is A Retrieval Request?' below)
- fraud – the transaction was completed for an illegal or fraudulent purpose and you were or should have been aware of such illegality or fraud (see page 76)
- authorisation related – for example, the transaction exceeds your floor limit and was completed without authorisation (see page 19), authorisation has been declined etc.
- processing error – for example, duplicate processing of a transaction
- cancelled/returned goods or service – cardholder has cancelled an order or returned goods and has not received a refund, or a refund has not been processed, or a refund has not been credited to the same cardholder account that was originally debited (see page 27)
- non-receipt of goods/services - for example, in the case of late delivery of goods or services, or the wrong goods have been delivered.

We'll always advise you by letter of the chargeback prior to the debit being applied to your account. Whether we can defend the chargeback depends on whether the transaction has complied fully with the rules set by MasterCard or Visa. Where possible, for example, where a transaction has been authenticated by chip and PIN and you're not liable, we'll automatically defend the chargeback on your behalf. In the event additional information/documentation is required from you, you'll receive notification in writing and the disputed amount will be debited to your account.

If we write to you, it's crucial that you return the requested information, in a clear format, to us within the timescale stipulated in our letter. Failure to do so may prevent us from taking any further action in defending the chargeback within the time allowed.

Requests for such documentation can be received up to 180 days after the transaction has been debited to the cardholder's account or the service received. However, in some circumstances, for example when fraud is involved, documents can be requested up to two years after the transaction date. It's therefore essential that you're able to retrieve such documents easily. Remember, card data must be stored securely (see page 71 regarding 'Data Security').

Please contact us (see page 86 for contact details) if you need to discuss a chargeback letter or if you're unsure what documentation is required.

WHAT IS A RETRIEVAL REQUEST?

A retrieval request, also known as a request for information, is when a cardholder queries a credit

or debit card transaction. This is often because the cardholder cannot remember undertaking the transaction.

A retrieval request isn't a chargeback. This means we don't debit any money from your account. However, a retrieval request can turn into a chargeback if the information the card issuer receives from us is illegible or insufficient to satisfy the cardholder's enquiry.

It's important that you reply to a retrieval request immediately because if you fail to do so, under the rules set by MasterCard and Visa, we may lose the right to defend any subsequent chargebacks.

HOW TO PREVENT CHARGEBACKS

Card Present (CP) Transactions

Chip and PIN cards and terminals have made substantial advances in preventing card fraud and are now the norm.

Card Schemes require all CP transactions to be performed using a chip and PIN terminal when presented with a chip and PIN card. Fallback from chip to magnetic stripe is allowed if, after inserting the chip, your terminal prompts you to follow this process.

There are still many legitimate cards in circulation that contain no chip and you'll have to swipe the magnetic stripe. You may then have to use the cardholder's signature to verify the transaction. Additionally, there are cards that have a chip but ask for the cardholder's signature as verification. Many of these cards have been issued overseas or to cardholders unable to use a PIN.

The best way to minimise the risk of CP chargebacks is to carefully follow the prompts provided by your terminal. If the terminal authorises a payment and prompts the cardholder to sign, then this should be allowed, subject to the normal checks associated with a signature-verified transaction (see page 10).

Please note that **all** non-chip transactions are subject to authorisation. Your terminal will prompt for this. However, if you're using Fallback paper vouchers due to a terminal fault, power failure etc., you must obtain a telephone authorisation for each transaction. Please see page 87 for our authorisation service number.

Note: Authorisation isn't a guarantee of payment. If a chip and PIN card is accepted using Fallback paper vouchers and the transaction turns out to fraudulent, you'll be liable for the chargeback.

Card Not Present (CNP) Transactions

In a CNP environment, it's important to remember that you're liable for chargebacks. If you follow the points listed below together with the important information listed in the 'How To Reduce Fraud' section on page 76, your risk will be minimised:

- if a customer asks to collect the goods, perform the transaction at the time of collection as a cardholder present transaction through your point of sale equipment
- always send goods by recorded or special delivery or by a reputable security carrier. Insist on a signed (preferably by the cardholder) and dated delivery note. Tell the courier not to make

the delivery if the premises appear to be vacant. Please note that proof of delivery alone isn't sufficient evidence to defend a chargeback
- don't release goods to third parties such as taxi drivers and messengers
- be cautious of transactions where the billing address is different to the requested delivery address. Avoid delivering to addresses other than the cardholder's, such as hotels, internet cafes and 'care of' addresses
- be wary of requests for next-day delivery, requests to alter the delivery address at short notice, or telephone calls on the day of delivery requesting a specific delivery time
- be cautious of customers who give mobile phone numbers as their only form of contact
- be wary of an order emanating from an email account where the customer's name isn't reflected in the email account address
- be suspicious with transactions that have an unusually high value or volume for your type of business or the sale is 'too easy'. In our experience these are the more likely ones to be fraudulent
- when performing a refund, always refund to the same card used for the original transaction
- keep a database of chargeback history to help identify patterns of fraudulent transactions. If a sale seems too good to be true then it probably is. Don't be afraid to contact the cardholder to ask further questions or request additional identification. A genuine customer should be pleased you're security minded and trying to protect them from fraud
- where possible, perform Address Verification Service (AVS) and Card Security Code (CSC) checks (see page 80). Refer to your terminal manual or terminal supplier for assistance on using this security feature. May we remind you though that you're not allowed to store the CSC data
- for ecommerce transactions, an additional layer of security can be incorporated into websites. MasterCard SecureCode and Verified by Visa (VbV) have been developed to allow customers to authenticate themselves as the genuine cardholder (see page 80). **To accept Maestro cards over the internet, you must support MasterCard SecureCode.**

The majority of chargebacks result from transactions being undertaken fraudulently. If you proceed with a transaction that appears suspicious, then you're doing so at your own risk. If the transaction has been completed, but the goods haven't been despatched, you're still in a position to carry out a refund of the transaction.

Obtaining A Successful Authorisation

Please see the 'Authorisation' section on page 19 for information on card authorisations.

A credit or debit card authorisation is a way of verifying the card has not been reported lost/stolen and the cardholder has sufficient funds at the time of the call. It does **not**, however, guarantee the transaction.

When contacting our authorisation service please be sure to select the correct telephone option, or your chargeback risk may increase.

The options are explained on page 87.

Proof Of Receipt

Please see 'Delivering Goods' on page 39 for information on the delivery of goods and the importance of obtaining proof of delivery. Please note that proof of delivery alone is **not** sufficient

evidence to defend a chargeback.

If you complete a sale for goods or services away from your business premises, we recommend using a mobile terminal to validate the transaction. If you don't have this facility we strongly recommend that you take an imprint of the card and request the customer to sign the voucher. Make a note of the card details and then input them on your terminal when you return to your business premises. If the transaction is later charged back, we'll require evidence that the card and cardholder were present at the time of the transaction.

Note: While taking an imprint of the card will help to minimise you risk of financial loss, if a chip and PIN card is accepted using Fallback paper vouchers and the transaction turns out to fraudulent; you'll be liable for the chargeback.

Deposit Taken - Goods Ordered, But Not Immediately Delivered

This is also sometimes known as a 'delayed delivery' and is typically used for transactions where it's not possible to immediately supply the purchased goods, for example, a large piece of furniture that has to be made to order. In these instances you may require the cardholder to make the purchase as two separate transactions, the first for the deposit and the second for the outstanding balance.

When completing a sale using this method, it's important that the two transactions are processed separately and the second receipt isn't processed before the goods have been despatched. If you do process the receipt for the balance earlier than the date that the goods have been despatched, a cardholder may view this as 'goods not received' and request their card issuer to chargeback the transaction.

Under Card Scheme Rules, the transaction receipt for the deposit may be submitted for processing before the delivery of the goods or services. However, the transaction receipt for the balance must not be submitted until after the goods have been despatched. If the difference between the goods being ordered and despatched is less than 30 days, this rule doesn't apply. In all instances, to help identify the order, the word 'deposit' or 'balance' must also be written on the appropriate transaction receipts.

Non-receipt Of Goods Or Services Not Rendered

- Don't process a card transaction until the goods have been sent or the services have been provided
- don't process any credit or debit card transactions where the cardholder has already paid for the goods or services using an alternative method of payment
- obtain the cardholder's signature on your delivery notes or service sheet following the completion of the service
- if you're unable to deliver all good or services in full, keep the cardholder informed of your actions at all times
- if you've debited a cardholder for goods that cannot be despatched, only process a partial transaction. Obtain an authorisation for the value of the goods that you're able to send. The original authorisation code for the full amount should be cancelled through our authorisation service (see page 87 for contact details) and a second call made for the full value of the goods that are then available to be sent. Keep detailed records.

Goods Not As Described

- You must ensure that the goods ordered by a cardholder are delivered or provided exactly as described in your brochure or advertisement. If you're unable to provide the exact specification including colour, size, quality and quantity, then you **must** notify the cardholder of the change and seek their approval to accept the revised option
- the goods should be delivered in a timely manner and be suitable for the purpose for which they were ordered, for example theatre tickets that arrive after the date of the performance aren't acceptable
- if goods are received by a cardholder and are damaged, broken or otherwise unsuitable for the purpose for which they're required, then the cardholder will have the right to chargeback the transaction
- if the cardholder returns the goods to you then you're required to reimburse the cardholder with the total value of the returned goods immediately.

Recurring Transactions – Additional Procedures

Please see 'Recurring Transactions' on page 45 for general information of recurring transactions.

When we request evidence of a recurring transaction, we must receive the following information within 14 days of the date of the letter:

- copy of cardholder's written authority
- transaction date
- transaction amount
- authorisation code, if applicable
- your business name and address
- type of goods or service provided
- delivery address, if different from the cardholder's statement address.

A recurring transaction will automatically be charged back to you if:

- the cardholder has closed their account, irrespective of whether they've notified you
- the cardholder disputes the transaction for any reason
- you're advised that the cardholder is deceased, in which case you must cancel the authority immediately.

Other Chargeback Reasons

Some other common reasons for chargebacks are listed below. This isn't meant to be an exhaustive list and providing you follow the guidelines provided in these *Merchant Operating Instructions*, chargebacks should be avoidable.

- Late processing – the transaction was submitted late and was processed outside the Card Scheme permitted timeframe
- transaction processed on an expired card
- incorrect transaction amount – cardholder charged more than receipt or advice.

DATA SECURITY

As you're accepting card transactions, you need to be aware of the value of the data you collect when undertaking a card transaction and the need to secure it. If you were to suffer a security breach, there's a significant risk of financial and reputational loss to your business.

The Payment Card Industry Data Security Standard (PCI DSS) is a global mandated standard which has been introduced by the Card Schemes to bring a greater level of security to this type of data.

Note: Under your Card Processing Agreement with us, you're required to achieve and maintain PCI DSS compliance.

PAYMENT CARD INSECURITY DATA SECURITY STANDARD (PCI DSS)

PCI DSS is a set of 12 comprehensive requirements for enhancing customer card data security, including requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

Its purpose is to help organisations proactively protect their customer card data. Essentially, this is the personal, sensitive data stored on or in the card that is key to making a transaction. If you don't properly protect this data, fraudsters may find your system's vulnerabilities and hack in to steal it. The data is very valuable to them as they can use it to fund further illegal activity.

This is a very real risk. Every year merchants of all sizes suffer data breaches. These can result in fines from the Card Schemes because customer card data was not secured effectively and to the PCI DSS standards. These penalties start at €5,000 but dependant on the specific circumstances can be much more.

BEST PRACTICES

To help you achieve PCI DSS compliance the fundamental principle you must follow is to treat card financial data as you would cash. You should ensure this data is held as securely as possible by:

- never releasing card information to anyone except us
- restricting your employees' access to card data.

Don't store the following information under any circumstances:

- full content of data from the card magnetic stripe or chip - also known as Track 2 Data, for example the Card Verification Value (CVV), Card Validation Code (CVC), PIN Verification Value (PVV).
- the Card Security Code (CSC) (see page 80) - should be deleted as soon as you've authorised the transaction, even in the case of CNP transactions, such as mail order and telephone order (MOTO) or internet transactions.

It's essential that you implement the following procedures:

- store only the customer's account information that is essential to your business
- store all material containing card information (for example, transaction receipts) in a locked, secure area

- destroy or delete all media containing obsolete transaction data with cardholder information
- ensure that any third parties that are engaged in, or propose to engage in, the processing or storage of transaction data on your behalf have confirmed they're PCI DSS complaint
- store transaction receipts securely for five years following delivery of goods or completion of the service provided, and then ensure that they're safely destroyed
- only store cardholder data when absolutely necessary, but if you have to, it must be stored in a secure encrypted manner.

If you're developing, reviewing or designing computer systems yourself, or purchasing them via a third party, who store, process or transmit sensitive card data, it's important that you ensure the system and the third party is PCI DSS compliant.

If you use vendor supplied off-the-shelf software in your point of sale equipment, you're mandated by the Card Schemes to only use valid Payment Application Data Security Standard (PA-DSS) compliant software. Using non-compliant software breaches Card Scheme Rules and could leave you exposed to significant penalties, with any costs or fines being your responsibility. You're also at an increased risk of a data breach which would have a significant financial impact on your business were it to happen.

All equipment provided by us is compliant with current, applicable PCI Data Security Standards. This will help your business achieve PCI DSS compliance.

For further details on PCI DSS you can visit:
- http://www.pcisecuritystandards.org – this site holds the latest version of the PCI DSS specifications and guidance on how to become compliant
- http://www.mastercard.com/us/sdp/merchants/index.html
- http://www.visaeurope.com/receiving-payments/security.

WHAT YOU NEED TO DO

Under your Card Processing Agreement with us, you're required to achieve and maintain PCI DSS compliance. We require **proof of your compliance with PCI DSS within 2 months of processing your first transaction.**

All merchants will fall into one of four merchant levels based on transaction volume over a 12-month period. The following guide indicates the volume of transactions at each level and the validation method you must employ.

Level	Criteria	Validation Action	Validation By
1	Over 6,000,000 MasterCard or Visa transactions a year	• Annual on-site security audit (including a Report on Compliance (ROC) • Quarterly network scans	Qualified Security Assessor (QSA)
2	Between 1,000,000 and 6,000,000 MasterCard or Visa transactions a year	• Annual on-site security audit (including a ROC) • Quarterly network scans	QSA or Internal Security Assessor (ISA)

3	Between 20,000 and 1,000,000 ecommerce transactions per year	• Annual PCI Self Assessment Questionnaire (SAQ) • Quarterly network scans	QSA or Self Assessment
4	Below 20,000 ecommerce transactions and below 1,000,000 transactions per year	• Annual PCI SAQ • Quarterly network scans	QSA or Self Assessment

A full list of accredited QSAs can be found on the PCI Security Standards Council website:

https://www.pcisecuritystandards.org/approved_companies_providers/qualified_security_assessors.php

The following website provides details on how to become an ISA:

https://www.pcisecuritystandards.org/approved_companies_providers/internal_security_assessors.php

INTRODUCING GLOBAL FORTRESS – LEVEL 4 MERCHANTS

To help you achieve and maintain PCI DSS compliance, we've developed **Global Fortress**. The key benefits of **Global Fortress** include:

- this service gives you access to the resources and guidance you need to help you safeguard your customer data
- a simple one stop shop to compliance for a small monthly fee
- access to SecurityMetrics, our Qualified Security Assessor (QSA) partner for this product, who'll support you in taking the necessary steps to achieving compliance.

If you're not already compliant, it's important that you act now to start your compliance journey so please call SecurityMetrics on 0330 808 1003. SecurityMetrics is open for enquiries between 9am and 5pm Monday to Friday (excluding public holidays). Calls may be monitored and/or recorded.

Alternatively, you can visit www.globalfortress.co.uk for further information, including charges and you can also start your compliance journey by signing up at the same time.

What Is The Alternative To Global Fortress?

You may prefer to achieve compliance through an alternative QSA or complete a SAQ. SecurityMetrics will be able to provide you with the appropriate SAQ, so call them on 0330 808 0831. Or you can download them from the PCI Security Standards Council website at www.pcisecuritystandards.org.

Should you wish to do this, please inform us and provide proof of your compliance. This alternative will incur an administrative fee. This will be in addition to any fees charged to you by your alternative QSA.

It's our responsibility to verify your compliance status and register you with MasterCard and Visa. Therefore, please ensure you provide us with a copy of: your certificate of compliance (annually), and your scan results (quarterly) if applicable. If you use a third party (other than Global Iris) and/or

a Payment Service Provider (PSP), a copy of their certificate of compliance is also required.

Please send copies of your completed documentation to us at:

PCI DSS Compliance Programme
Global Payments
51 De Montfort Street
Leicester
LE1 7BB

Or email them to saq@securitymetrics.com.

If you enrol for **Global Fortress**, your compliance with PCI DSS will automatically be reported to us, so you won't have to provide us with your completed documentation.

LEVEL 1, 2 AND 3 MERCHANTS

You will need to provide us with evidence of your ongoing PCI DSS compliance. Therefore, please send us the following:

- your Attestation of Compliance (AOC)/ROC (annually) for level 1 or 2 merchants
- a copy of your signed and dated SAQ for level 3 merchants
- your network scans (quarterly), if required
- if you use a third party (other than Global Iris), a copy of their AOC.

Please send these to your Relationship Manager (RM) or the address above. Please speak to your RM or call our helpdesk (see page 86 for our contact details) if you need any further information.

THIRD PARTY COMPANIES

If you're using a third party company and give them access to card and financial data for any purpose (for example, processing transactions, storing data or call centre functions), you'll need to ensure that they also adhere to all rules and regulations governing card data security. In particular, all third parties storing or processing this data on your behalf are required to be PCI DSS compliant. Any violations of these requirements by your third party are your responsibility and may result in you having unnecessary financial exposure.

A copy of their AOC is required. Please send it to the address detailed above.

WHAT HAPPENS IF YOU DON'T BECOME COMPLIANT?

If you don't validate your compliance, you'll be subject to monthly non-compliance charges that are charged in arrears and are non-refundable. These non-compliance charges will continue until you achieve PCI DSS compliance.

Details of the non-compliance charges can be found on www.globalfortress.co.uk.

Whichever route to compliance you choose, you won't be considered compliant with the PCI DSS requirements until we've received and registered your compliance status with the Card Schemes.

IF YOU SUSPECT A SECURITY BREACH

If you've followed the best practices listed above and become fully compliant with PCI DSS, you'll have minimised your chances of suffering a security breach. However, security can never be perfect - it's therefore necessary to put an instant response plan in place, tailored to your own business environment, so that you know what steps to take.

If you experience, or even suspect, a security breach at your business which might involve card financial data, it's vital that you take the following precautions:

- contact us immediately (see page 86 for contact details)
- don't access or alter compromised systems - don't log on or change any passwords
- don't turn the compromised systems off; isolate them from your network and unplug any network cables
- preserve all logs and similar electronic evidence
- perform a back-up of your systems to preserve their current state; this will facilitate any subsequent investigations
- log all actions taken.

Additionally, you should obtain professional advice from a PCI DSS approved Qualified Forensic Investigator, details of which can be obtained at:
www.pcisecuritystandards.org/approved_companies_providers/pfi_companies.php

HOW TO REDUCE FRAUD

Fraud has become a global epidemic that threatens everyone. It's tempting to think that once a payment is authorised you're assured of receiving your money. Unfortunately, that's not the case.

Authorisation doesn't guarantee payment!

When an authorisation is provided, all this confirms is that funds are available and that the card hasn't been reported lost or stolen – yet. The rightful owner might not know that the card is missing so the transaction could still turn out to be fraudulent.

The vast majority of card payments are completed without problem. However, just one rogue transaction can have a significant impact to you, taking up your time, potentially costing you money and it may damage your reputation.

Fraudsters are ingenious, creative and adaptable. To help you be more aware of how fraudsters can attack you we have compiled a list of the most common frauds we have encountered through our time working with our customers.

TYPES OF FRAUD TO LOOK OUT FOR

Pick Up Fraud Scam

This is one of the most common fraud scams we see. A new customer rings up and places an order for goods over the phone and says they, or a courier/taxi will come and pick up the goods. The fraudster may have the correct name and address details for the genuine cardholder so things like the Address Verification Service (AVS) (see page 80) check may pass. As the goods are being picked up there is no way to confirm where they are actually going so be wary, and ask the customer to bring in the card and do the transaction as chip and PIN on collection.

Third Party Delivery Addresses

Take care when you are given an alternative delivery address, particularly where the delivery address is in a completely different location to the billing address. Some merchants send out a letter to the billing address asking their customers to confirm that the order is genuine before the order is dispatched. This has proven successful in preventing fraud and could be something you might wish to consider.

Multiple Cards Used And Decline Attempts

Fraudsters often buy batches of compromised card details and will try to place orders over the phone, by fax or online. They will continue to try each set of card details until they can get one to work. If you're seeing multiple declines, then you need to careful of the order.

Non-UK Issued Cards Being Used For Orders To Be Delivered To A UK Address

A lot of Cardholder Not Present (CNP) fraud is committed using non-UK issued cards for goods that are to be delivered to an address in this country. For online orders, or if a virtual terminal is being used, many Payment Service Providers (PSP) can flag up orders such as these. On other

terminal types, one sign that a card was not issued in the UK is that the AVS check doesn't pass. The first six digits of a card number are called the Bank Identification Number (BIN number) and these can be checked online on various sites, which can be found by searching for 'BIN list look up'.

Requests To Refer An Authorisation To The Authorisation Centre

If a message such as 'CALL AUTH CENTRE' appears on your terminal screen when carrying out a transaction, you should call our authorisation centre (see page 87 for contact details) so that further checks can be made to ensure that your customer is the actual cardholder. **Never** accept an authorisation code provided to you by your customer, or from a person who rings your business and claims to be from our authorisation centre. The codes are not genuine and the card issuer will be able to claim the funds back from your business if you use them.

Customer Distraction

A fraudster may attempt to distract you when they are entering their PIN on your terminal so that they can enter a dummy authorisation code. Be wary if a customer who holds onto the terminal for longer than is strictly necessary.

Split Sales

If a transaction declines for the full amount of an order, don't attempt to split the total down into smaller amounts or spread it over several cards. Fraudsters are frequently unaware of the available balance on the card(s) they get hold of and will ask you to try various amounts until they can get a transaction to go through.

Magnetic Stripe Transactions And Counterfeit Cards

The UK has led the world in the introduction of chip and PIN technology. Chip and PIN is rolling out gradually around the rest of the world, but until such time as chip and PIN is universal, there'll still be a need to retain the magnetic stripe and signature panel on all cards.

However, if a chip is present on the card, be careful if a customer says that the chip doesn't work, or that they have forgotten their PIN.

Also beware of counterfeit cards, a forged card that has been printed, embossed or encoded with the details of a genuine card. Most counterfeit cards are the product of 'skimming', where the data from the card is copied without the genuine cardholder's knowledge. 'Skimming' can occur at retail outlets or cash machines, where the card is put through a device that electronically copies the cardholder data.

It is therefore important that, if you swipe the card through your terminal, ensure you follow the instructions in this documents for checking the card (see page 10).

Also consider other warning signs listed below:

- watch out for seemingly random and careless purchases, for example, is the customer buying a large number of the same item?
- has the customer not bothered to try on the clothes?
- is the customer nervous or trying to distract you?

- is the transaction for a low amount with a big cashback?
- is the transaction amount just below your floor limit?

Phishing

Phishing is a way that fraudsters can obtain card details, which they then use to commit CNP fraud.

Phishing can be done by sending emails that claim to come from a genuine company operating on the internet. They're sent in an attempt to trick customers into disclosing information at a bogus website operated by fraudsters. These emails usually claim that it's necessary to 'update' or 'verify' customer account information and they urge people to click on a link from the email which takes them to the bogus website. Any information entered on the bogus website will be captured by the criminals for their own fraudulent purposes.

Fraudsters can also call your business saying that they're a terminal engineer, or calling from MasterCard, Visa, or Global Payments and then ask for details of the last few transactions you processed. Do **not** given them any information.

Email Addresses

There are two types of email addresses. Email access is generally available as part of a customer's subscription to a package from their Internet Service Provider (ISP). Alternatively 'free' email accounts can be used, for example from Yahoo, Hotmail and Google 'G Mail'.

Many genuine customers utilise 'free' email accounts due to the ability to be able to use email wherever there's an internet connection. However, fraudsters favour 'free' email accounts due to the anonymity it provides them, and the vast majority of ecommerce fraud is committed where 'free' email accounts have been quoted. Be suspicious if the customer's name isn't reflected in the email address.

The email address alone should not be used to make a decision as to whether a transaction may be fraudulent. Additional validation should be undertaken if a 'free' email address is used.

We recommend that you send the customer an email once an order has been placed. It's highly advisable not to process transactions where the email messenger states it has been unable to deliver the email.

Requests To Pay Third Parties Via Wire Transfer

Be suspicious if a customer places an order for goods and/or services and also asks you to take payment for additional services to be provided by another company. You are then asked to forward the additional money you have taken by wire transfer to the other company. The customer may also offer you an additional sum as a thank you for helping them. This is a scam, and we most often see this happening to hotels and B&Bs.

Also, be very careful if you're exporting goods and your customer asks you to forward funds to their shipping agent via a wire transfer. The shipping agent may well not exist and the order is quite likely to be fraudulent.

Decline any requests you might receive to forward overpayments by wire transfer to third parties such as intermediaries or facilitators.

Fraudulent Refunds

If a sale is done on one card, any refund should be done onto the same card. Be suspicious if a customer asks you to refund the sale onto a different card, or to return it to them via wire transfer.

Unfortunately we do see cases where a member of staff processes refunds onto their own card so make sure that you control who has access to the supervisor PIN for your terminal. Ensure that you have procedures in place that may help you spot an unusual refund activity.

Additionally, there has been an increase in criminals using social engineering techniques, such as phishing, to obtain information about a merchant's account with the aim of processing fraudulent refunds. Using these details, criminals are able to hack into the merchant's payment gateway or third party software and can then submit credit refunds to card accounts which have previously been set up using false details or have been subject to account takeover. Once the refund has been credited the funds are quickly withdrawn. These transactions may appear as though cardholders' accounts have been legitimately credited for the return of goods, but in reality, no goods or services have ever been purchased.

To reduce the risk of your business being subject to this type of fraud, you must always:

- ensure that your account IDs and passwords are stored in encrypted form
- ensure that passwords for internet payment gateways are changed regularly – at least every 90 days
- when processing a refund ensure you have the details of the original sale and that the refund is processed on the same card account
- inform us of any suspicious emails or telephone calls you may receive requesting user account IDs or passwords
- if you have a mobile terminal, ensure it is kept secure at all times to prevent criminals simply walking off with them
- if you receive a new Point of Sale (PoS) terminal, change the supervisor password immediately from the factory set generic code and change it regularly
- inform us straight away if your PoS terminal is either lost or stolen. This will ensure that these devices are blocked from further processing.

HOW CAN I PROTECT MY BUSINESS?

We have a dedicated team with fraud investigators who use risk monitoring tools to assess and monitor the risk of fraud. The team review merchant trading patterns to determine if any fraudulent activity has or is about to occur.

However, this won't prevent fraud from happening. You'll need to implement business practices to minimise the risk and cost of fraud to you.

If you process CNP transactions, you need to be even more vigilant. There's a greater inherent risk in accepting CNP transactions because you're unable to guarantee that it's the genuine cardholder providing the information. Therefore, accepting CNP payments considerably increases your vulnerability to fraud, chargebacks and ultimately financial loss. This is because you cannot physically verify the transaction by performing card validation checks and checking the

cardholder's signature or PIN.

If you accept CNP transactions, then you won't have the same protection as a customer undertaking face-to-face transactions and you **will** be liable for chargebacks in the future in the event of any dispute. It's good practice to conduct further investigations when there are any anomalies with a CNP transaction. These can take the form of standard industry fraud prevention tools and 'common sense' checks to validate a transaction.

Don't be afraid to decline suspicious orders. You're under no obligation to fulfil a transaction you consider fraudulent.

Fraud Prevention Tools

Fraud prevention tools such as the Address Verification Service (AVS) and the Card Security Code (CSC) are in place to help with authentication of the transaction. Unlike PIN or signature, AVS and CSC don't confirm the cardholder's identity, but when used together they offer further information to help you decide whether to proceed with the transaction.

Address Verification Service (AVS): AVS allows you to confirm that the numeric characters in the billing address provided by the cardholder match the address details held by the card issuer. This check is available for all **UK issued** cards. A fraudster may be in possession of a card including the CSC, but may not be able to provide the genuine cardholder's address.

Note: British Forces Postal Office (BFPO) addresses are likely to result in a 'no match' AVS response.

Card Security Code (CSC): The CSC provides additional security information designed to confirm that the customer is physically in possession of the card. If present, the CSC may appear as the last three digits printed on the reverse of the card on the signature strip itself or in a white box to the right hand side of the signature strip. For American Express cards this number has four digits and is printed on the front of the card.

The CSC can also be referred to as CVV, CVV2 or CVC2.

Note: You must not store CSC data. This is strictly prohibited by the Card Schemes (see page 71 regarding 'Data Security').

MasterCard SecureCode (SecureCode)/Verified By Visa (VbV): For ecommerce transactions, an additional layer of security can be incorporated into websites. SecureCode and VbV, both of which use the umbrella name of 3D Secure, have been developed to allow customers to authenticate themselves as the genuine cardholder.

SecureCode and VbV are global ecommerce solutions that enable cardholders to authenticate themselves to their issuer through the use of a unique personal code or password.

The cardholder must enter their password in a separate browser window before their online transaction can be authorised. The card issuer confirms it's the true cardholder performing the transaction in moments. Cardholders enjoy peace of mind knowing that no one else has access to their password, and you obtain explicit evidence of an authorised purchase.

In the event of the need for a chargeback following fraud, in a standard online transaction, the merchant is liable to pay back the disputed transaction amount. Use of 3D Secure may result in a shift in liability from the merchant to the card issuer. The liability shifts under the following conditions:

- merchant and card processor have installed the service, but the card isn't registered for the service
- merchant and cardholder are registered for the service and the cardholder authenticates themselves
- merchant and card processor have installed the service but the card issuer isn't enabled to operate the service.

To gain the benefits of 3D Secure you'll need to deploy the required technology on your website. This can be accomplished by loading a registered Merchant Plug-In (MPI) application on your server. Alternatively, you can enter into a contract with a hosted service to perform the authentication process for you. Our Global Iris service provides both this additional authentication and the transaction processing (see page 48).

Note: Undertaking internet transactions will be solely at your own risk, regardless of whether any requests for authorisation or other enquiries have been made to us.

The use of the 3D Secure authentication process for internet transactions reduces this risk. This is only available for use with MasterCard and Visa cards. If the cardholder's identity is successfully authenticated through SecureCode and/or VbV, then a chargeback won't occur solely because the cardholder denies undertaking a transaction. This also applies if authentication is attempted but cannot be completed because the cardholder for whatever reason doesn't participate in a SecureCode or VbV transaction.

If the cardholder's identity cannot be authenticated for any other reason, including failure of your own equipment for any reason, or any inputting error or omission by you or the cardholder, you won't have the above protection from a chargeback. Authentication and its effect on liability for relevant transactions is governed by and subject to MasterCard and Visa rules (as applicable), which change from time to time. Amongst other things, these rules exclude certain cards and transactions from the authentication service. This means that even if you've opted to use 3D Secure, the service and the protection it offers won't apply to all transactions. For further information please refer to MasterCard and Visa websites. Please note that in any event, a transaction may be charged back for other reasons.

Note: To accept Maestro cards over the internet, you must support MasterCard SecureCode.

If you don't support SecureCode for Maestro internet transactions, then you may be liable to significant financial penalties.

Fraud Screening

If you accept CNP transactions, then we strongly recommend that you introduce fraud screening, to check the validity and history of cards tendered.

As a minimum these checks should include:

- statement address
- statement address country

- number of previous declined transactions on same card or same order
- delivery address
- phone numbers
- same value transactions
- number of times a card has been used in a given time.

In addition to the checks above, we also strongly recommend that you undertake the following additional fraud screening checks for internet transactions:

- location of IP (Internet Protocol) addresses in relation to country of card issue/delivery address
- review frequency of use and whether the addresses are linked to orders from more than one delivery address
- email addresses, as detailed in the section on page 78.

Other Helpful Tools

Fraud Management Systems: We strongly recommend that you implement a suitable fraud management system, either directly or via a Payment Service Provider (PSP). Should you do so, the system is your responsibility and you must correctly implement and maintain it.

Verifying Your Customers: Websites such as 192.com, yell.com and Google Streetview can be used to verify your customers and the address you are sending the goods to. For example, be careful where an order that has apparently been placed by a company is being delivered to a residential address.

Financial Fraud Action UK: Financial Fraud Action UK raises awareness about all types of plastic card fraud in the UK and provides information to prevent fraudulent use of credit cards, debit cards and charge cards.

Financial Fraud Action UK
Working together to prevent fraud

www.financialfraudaction.org.uk

In addition, Financial Fraud Action UK provides on-line training for retailers, retail staff and law enforcement agencies and contributes to the fight against plastic card fraud.

The website featured above offers comprehensive information about plastic card fraud, free publications and training materials, as well as useful tips and answers to frequently asked questions. We ask you to play your part in combating plastic card crime and would encourage you to visit this website to learn how to protect yourself against fraud.

Ten Tips To Help Prevent CNP Fraud

Extra vigilance can help prevent CNP fraud. If sales staff can answer ‘yes’ to one or more of the questions below, it doesn’t mean that the transaction is fraudulent - but it does mean that your staff should consider further checks before proceeding with the transaction.

1. Is the sale too easy? Is the customer disinterested in the price or details of the goods? Are they a new customer? Is the customer’s address in your normal catchment area? If not, why

are they ordering from you?
2. Are the goods of a high value or easily re-sold?
3. Is the amount of the sale excessively high in comparison with your usual orders? Is the customer ordering many different items or several units of the same item? Do they seem unlike your usual customer?
4. Is the customer providing details of someone else's card, for example that of a client or a family member?
5. Is the customer reluctant to give a landline contact phone number? Are they only prepared to give a mobile number?
6. Does the address provided seem suspicious? Has the delivery address been used before with different customer details? Is the delivery or contact address overseas?
7. Is the customer being prompted by a third party whilst on the phone or do they seem hesitant when answering certain questions?
8. Is the customer using more than one card to split the value of the sale?
9. Does the customer seem to lack knowledge of their account?
10. Does the customer seem to have a problem remembering their home address or phone number? Does the customer sound as if they're referring to notes?

GLOBAL IRIS INTEGRATED FRAUD PREVENTON TOOLS

To reduce your fraud risks, you can accept mail order and telephone order (MOTO) and internet transactions, by using our Global Iris service to accept transactions. Global Iris is a browser-based solution, which means you can set up with no need for software installation and you benefit from automatic updates, including the latest in security and PCI DSS compliance requirements.

Global Iris comes complete with the tools to manage and greatly reduce the exposure to fraud faced in a CNP environment, including:

- 3D Secure Payer Authentication
- fraud scoring/transaction screening
- Card Security Code (CSC) checking
- Address Verification Service (AVS) checking.

If you would like to know more about Global Iris, please contact us (see page 86 for contact details).

For further information on how to utilise the Global Iris service, refer to the customer guides located online at: https://resourcecentre.globaliris.com/.

ADDITIONAL IMPORTANT INFORMATION

KEEPING YOU INFORMED

We'll send you regular updates on issues that affect the way in which you accept and process credit and debit card transactions.

It's essential that you read these updates and follow our recommendations, especially regarding mandatory Card Scheme changes. Please contact us if you need further help or support (see page 86 for contact details) or if you're concerned that you're not receiving such information.

STATIONERY

If you use a terminal to process card transactions, we'll provide you with a starter pack that contains:

- Fallback Voucher Pack - sales Fallback vouchers, refund Fallback vouchers and summary Fallback vouchers
- Merchant Card and Imprinter Plate
- MasterCard/Visa/Visa Electron/Maestro/V PAY/Discover Global Network/UnionPay point of sale stickers, depending on the card types you've been set up to accept. Please display these so that cardholders are aware your business accepts these card
- Authorisation and helpdesk telephone number stickers
- Manual Card Imprinter* (optional item, a charge may apply).

*In case of terminal failure, telephone line fault or disruption to your power supply, you'll need to have access to a manual imprinter. Without access, you'll be unable to accept card payments in the event of any of the above circumstances occurring. Full details of your obligations to maintain an imprinter are set out in our *Terms of Service*.

To order further supplies of stationery please call us on the number provided on page 86. Allow five business days for delivery. Please ensure you hold sufficient stocks for your business.

TALLY ROLLS FOR ELECTRONIC TERMINALS

If you operate an electronic terminal, make sure you have enough tally rolls to cope with the demands of your business.

To order tally rolls for our terminals, please call us (see page 86 for contact details). You'll find our prices very competitive. We can supply rolls within 24 hours on a business day (Monday to Friday, excluding public holidays) to most areas of the UK.

We strongly recommend that you hold at least one month's supply of tally rolls. For busy periods you may wish to order additional supplies.

Note: Please be careful of unsolicited calls from third parties selling tally rolls that might not meet the quality required for your terminal.

PRODUCING YOUR OWN ADVERTISING

If you want to produce your own materials to tell your customers that you accept cards as a means of payment, please ask us for an artwork pack.

The artwork pack gives full details about reproducing the Card Scheme logos.
Please note that the following rules apply:

- the card logos have been registered as trademarks and must be used in accordance with the instructions contained in the artwork pack
- the card logos must not be featured in advertising in a way that suggests that the Card Schemes are endorsing your goods or services
- you must submit all promotional or sales material that refers to us, or any card type, for our approval
- your internet payment page(s) must feature the appropriate Card Scheme logos.

If you're using a Mobile POS Solution, to produce materials to tell your customers that you accept cards as a means of payment, please visit the GLOBAL MPOS website at www.globalmpos.co.uk. The information on the website gives full details about reproducing the Card Scheme logos.

In addition, if you want to use the Global Payments logo or the Global Iris logo on your website or advertising material, you must enter into a Trade Mark Licence Agreement. Please contact us for more information (see page 86 for contact details).

Each of your outlets and their points of sale must be clearly identified in the appropriate promotional material.

HOW TO END THE CARD PROCESSING AGREEMENT

We've every confidence that you'll be satisfied with our service. However, if you want to end the Agreement for any reason (other than breach of the Agreement by us) you must give us at least **30 days**' written notice.

If you wish to end the Agreement within the first 12 months, we're entitled to charge £150 in respect of our reasonable administrative costs.

Full details on how to end the Agreement are set out in our *Terms of Service*.

globalpayments

HOW TO CONTACT US

Have your merchant number ready whenever you call us. We assign you a merchant number to help us identify you. It appears on your monthly invoice and on receipts from your electronic terminals.

Calls are monitored or recorded from time to time to improve our service to you. Any recording remains our sole property.

GLOBAL PAYMENTS HELPDESK: 0345 702 3344

We're here to help, so please call us but please don't use this number for authorisations (see next page).

Listen to the options available when you call and select carefully as the order may change from time to time. The options include:

- **Stationery** - select if you require more tally rolls or any other item of Global Payments stationery. Lines are open every day (except Christmas Day) between 8.00am and 11.00pm Monday to Saturday, 10.00am and 5.00pm on Sunday and between 10.00am and 4.00pm on public holidays.
- **Card Terminal, Global Iris or GLOBAL MPOS Support** - select if you're experiencing technical difficulties with your Global Payments provided terminal or have a query regarding Global Iris or your Mobile POS Solution (GLOBAL MPOS).
  - For Card Terminal Support, ensure you know the terminal type you're calling about. Lines are open every day (except Christmas Day) between 8.00am and 11.00pm Monday to Saturday, 10.00am and 5.00pm on Sunday and between 10.00am and 4.00pm on public holidays. Ensure you know the terminal type you're calling about.
  - For Global Iris, lines are open 8.30am to 6.15pm Monday to Friday, except Christmas Day, Boxing Day, New Year's Day, Easter Monday and May Day. All other public holidays, lines are open 10.00am to 6.00pm.
  - For GLOBAL MPOS Support, lines are open 24 hours, 7 days a week, except Christmas Day. You can also email this team (support@globalmpos.co.uk) or you can visit the GLOBAL MPOS website (www.globalmpos.co.uk).
- **Other Enquiries** - select if you have any queries that aren't covered by the options above. Lines are open 9.00am to 6.00pm Monday to Friday (except public holidays).

We also provide a textphone service on 0345 602 4818.

You can also contact us via:

Our website: www.globalpaymentsinc.co.uk

And email: customerservices@globalpay.com

Or write to us at: Global Payments
51 De Montfort Street
Leicester
LE1 7BB

OUR AUTHORISATION SERVICE: 0345 770 0600

Open 24 hours, 7 days a week, 365 days a year.

Please ensure you have your merchant number and the card details before you call.

There are several options on this number:

- **A Code 10** - if you're undertaking a face-to-face sale and are suspicious of the transaction.
- **An authorisation** - if this is a new authorisation request, in other words, you haven't previously sought authorisation. Don't use this option if your electronic point of sale equipment has requested that you call the authorisation centre or refer a transaction. Select the option below
- **You've received a request to call the authorisation centre or the item is a referral** - if your electronic point of sale equipment has requested that you call the authorisation centre or refer a transaction
- **Cancel a previous authorisation*** - when a decision has been made not to proceed with a transaction for which authorisation has already been granted, for example, the cardholder decides not to proceed with the purchase before it's completed but after an authorisation has been granted. However, please note that this will only cancel the authorisation code and not the transaction. If the sale has been completed and you wish to cancel the transaction, you should contact our helpdesk detailed on the previous page
- **Address Verification** - this service allows you to confirm that the numeric characters in the billing address provided by the cardholder match the address details held by the card issuer.

*Should you wish to cancel a high value pending authorisation we'll need to call you back to validate your request. This contact will be made from the details that we hold on our records and not made on any contact details provided at the time of the call. In order for us to expediently action your cancellation requests, please ensure that you notify us of any change to your contact details. Please note that not all card issuers will accept authorisation cancellation requests irrespective of the value. You may wish to notify your customers accordingly of the potential need for them to contact their card issuer directly to undertake an authorisation cancellation.

IF YOU WANT TO COMPLAIN

If for any reason you're not entirely satisfied with any aspect of our service, we want to hear from you as soon as possible. We'll then make the relevant enquiries and aim to put matters right as soon as we can.

Please begin by calling our helpdesk on **0345 702 3344** and telling us where the problem has arisen. We'll try to answer your concerns straight away, and if we cannot do so there and then, we'll investigate and call you back as soon as we can.

If you subsequently feel we haven't resolved the problem to your satisfaction, you can escalate your complaint via our helpdesk or you can write to our head office at:

Customer Relations Department
Global Payments
51 De Montfort Street
Leicester
LE1 7BB

We'll send you written acknowledgment of your complaint within three business days of us receiving your letter. This will confirm that we've received and recorded your complaint.

We always want to be able to resolve any concerns you raise with us. However, you may have the right to refer the matter to the Financial Ombudsman Service.

A copy of *Our Complaints Procedure* is available on request.

The Financial Ombudsman Service

The Financial Ombudsman Service deals with some types of complaints from private individuals, together with businesses and charities with an annual turnover of less than two million euros and has fewer than ten employees.

Call: 0800 023 4567 – calls to this number are free when calling from a fixed line or a mobile phone in the UK,
or
0300 123 9123 – calls to this number are charged at the same rate as 01 or 02 numbers on mobile phone tariffs

Please note calls to both these numbers are recorded.

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

Write to: The Financial Ombudsman Service
South Quay Plaza
183 Marsh Wall
London
E14 9SR

Or visit at: www.financial-ombudsman.org.uk

Global Payments
51 De Montfort Street
Leicester
LE1 7BB
Tel 0345 702 3344
Textphone 0345 602 4818
www.globalpaymentsinc.co.uk
www.globalpaymentsinc.com

Global Payments is HSBC Bank Plc's preferred supplier for card processing in the UK.

Global Payments is a trading name of GPUK LLP. GPUK LLP is authorised by the Financial Conduct Authority under the Payment Services Regulations 2009 (504290) for the provision of payment services.

GPUK LLP is a limited liability partnership registered in England number OC337146. Registered Office: 51, De Montfort Street, Leicester, LE1 7BB. The members are Global Payments U.K. Limited and Global Payments U.K. 2 Limited. Service of any documents relating to the business will be effective if served at the Registered Office.

© GPUK LLP. All rights reserved.

MOI 08/2015 | GP083