

COMMERCIAL BANKING



CARDNET

Card payments made easy for you and your customers



LLOYDS BANK

Contents

Welcome	1
1.Key points	3
2.Acceptable Cards	5
Visa	7
Visa Credit	9
Visa Debit	9
V PAY	11
Visa Electron	13
Visa Prepay	15
Visa and Visa Electron mini cards	15
Visa SimplyOne card	15
Mastercard®	17
Debit Mastercard	18
Maestro®	19
Mastercard® Digital First Card Programme (DFCP)	21
UnionPay	22
JCB	23
American Express	24
Discover® Global Network	26
Diners Club International®	27
Discover®	29
BC Global Card	30
Troy Global Card	31
RuPay	32
Elo Global Card	33
Contactless	37
Commercial Cards	38

Contents

3. Checking the Card	40
Security features	41
Additional checks	45
4. Accepting Transactions	46
Point of Sale Transactions	47
Card Not Present (CNP) Transactions	50
Address Verification Service	53
E-commerce	57
Strong Customer Authentication	59
Using your web browser as a virtual Point of Sale machine	62
Card Schemes	94
Pay by URL	96
Biometric Checkout	98
Digital Wallets	98
Additional Visa acceptance entities	100
5. Authorisation and referral	105
When to obtain Authorisation	106
Manual Authorisation	106
Authorisation adjustments/reversals	106
Pre-Authorisation and Final Authorisation	107
Update to Visa T&E Transaction Rules	108
Referrals	110
Split sales with cash, cheque or second credit Card	110
Cancelling a Transaction	111
Refunds	111

Contents

Visa Digital Authentication	112
6. Banking and reconciliation	114
Electronic data	115
Paper vouchers	115
Record keeping	117
Your Cardnet statement	118
Online reporting tools	118
7. Security	120
Data security	121
Payment Card Industry – Data Security Standards (PCI DSS)	122
Protecting your point of sale and Card processing equipment	125
Suspicious Transactions	128
How to guard against fraud	130
Mastercard PSD2 optimisation program	131
Disputes	136
8. Additional facilities for you and your customers	142
Purchase with Cashback	143
Mobile phone top-up	143
Recurring Transactions	144
Gratuities	145
Dynamic Currency Conversion (DCC)	146

Contents

Accepting currency Transactions	146
Cash Advance	146
Additional Cards	146
9. Exceptions	147
Failed chip Card read	149
Failed magnetic stripe Transactions – key entry (excluding internationally issued Maestro, Visa Electron and UnionPay cards)	149
Using the paper Fallback system to process Point of Sale Transactions when your Terminal is not working	151
10. Additional information	157
Notifying us of changes to your business	158
How to complain	159
What to do if you experience financial difficulties	161
Agencies offering financial assistance	163
Authorisation telephone numbers	164
Merchant services	164
Cardnet stationery	164
Point of sale and display material	164
Recommended tally roll supplier	165
Cards left on your premises	165
Emergencies and disruptions	166

Taking Card payments
should be simple
and convenient for my
business and customers

Security, flexibility and convenience – welcome to Cardnet®

Thank you for choosing Cardnet®. At Lloyds Bank Commercial Banking, we serve around 1 million UK businesses and understand what you need from your Card processing system. Cardnet is one of the UK's largest payment processors and offers you rapid Transaction handling and payment reconciliation. You'll be able to accept payments from one of the widest ranges of Card Schemes available.

This Manual will help your business make the best use of Cardnet features and services. In it you will find all the information and procedures needed to be sure of using Cardnet easily and securely.

The Manual forms part of your Agreement with Cardnet, so please read it and make sure it is retained in a safe place and available for all relevant staff to refer to.

Please contact us if you'd like this information in an alternative format such as Braille, large print or audio.

CARDNET HELPLINE



Call 01268 567 100

8am to 9pm Monday to Saturday

Call our knowledgeable UK-based team with any questions about your Cardnet service or this Manual.

1.06

Billion transactions a year

£66.3 Billion

Card sales every year

SOURCE

Cardnet billing data (Omnipay and MSIP)

1: Key points

To get the most out of the Cardnet service, it is important to follow some basic procedures that are strictly enforced by Visa, Mastercard, Maestro, UnionPay International, JCB and Discover® Global Network.

You must

- Display Visa, V Pay, Mastercard, Maestro, Discover® Global Network (Diners Club International®, Discover®) UnionPay International (UnionPay), JCB and, where applicable other scheme logos on promotional materials showing clearly which Cards you do or don't accept.
- Prominently display any surcharge you impose at point of sale (POS). Any surcharge must be included in the Transaction amount and not processed separately. Any surcharge should be representative of the actual processing cost involved.
- Include any taxes in the amount charged on Card Transactions. They may not be collected by you in cash.
- Provide the Cardholder with the option of receiving confirmation of the Transaction for their records. This need not be a separate receipt. The Card payment data can be included at the bottom of your POS itemised receipt. With chip and PIN-capable POS, the information displayed should include an indication that it is PIN verified. Only the last four digits of the Card number are to be shown on the Cardholder's copy.
- Only make cash disbursements to a Cardholder as part of a Card Transaction up to the limit authorised in your Agreement with us.
- Have prior written agreement from Cardnet before accepting mail/telephone order or E-commerce Card Transactions.

- You can choose which cards to accept but if you choose to accept a card issued in the UK that is not a commercial card, you need to accept all cards of this type regardless of who has issued the card.
- Inform us if you want to accept Transactions on behalf of third parties and apply for the relevant regulatory permissions from the Financial Conduct Authority.

You must not

- Indicate that Cardnet, Visa, Mastercard, UnionPay, JCB, Discover® Global Network, its partners or any other association endorses your goods and services.
- Submit a Transaction or sale that has previously been charged back. See Section 7, 'Security, Disputes'.
- Impose a surcharge on any card issued in the UK that is not identified as a commercial card. You must not charge an amount higher than the actual cost to you of accepting the transaction.
- Accept any direct payments from Cardholders, for example, cash/cheques for the credit of the Card account (only the Card Issuer is authorised to receive such payments).
- Process paper Transactions except in the case of Fallback. See Section 9, 'Exceptions', p147.
- Accept Transactions on behalf of third parties.
- Store magnetic stripe data that facilitates Card processing or Card Security Code (CSC) details. Special Card Scheme regulations apply if you (or your Agent) store this data electronically and failure to comply with these requirements may result in a fine.

2 : Acceptable Cards

This section details the features to
look for when accepting Cards.

You will have agreed separately with us the Card types you are able to accept

It is important to check the Cards thoroughly to help prevent Card fraud. The following descriptions will help you and your staff to check a Card's validity and to follow the correct Card acceptance procedures.

If a Card does not fit these descriptions, it must not be accepted. If you have any doubts or if you are suspicious, contact the Authorisation Centre on **01268 822 822** and ask for a Code 10 Authorisation. See Section 7, 'Security, Suspicious Transactions' (p128).

AUTHORISATION CENTRE



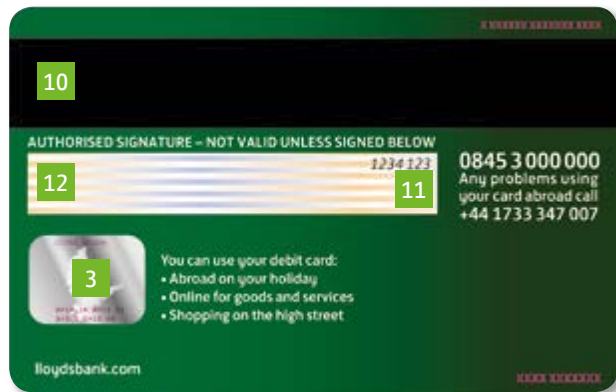
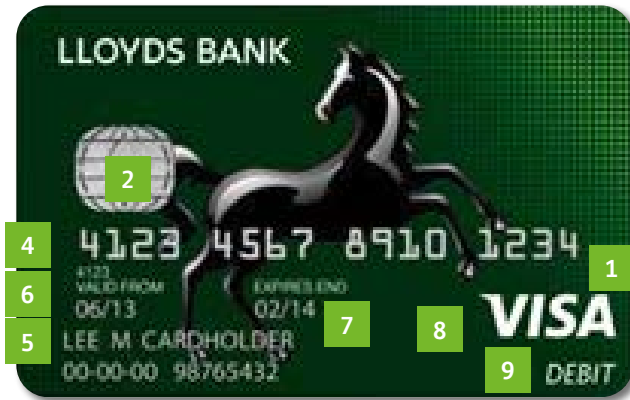
Call **01268 822 822**

State "This is a Code 10 call" and follow the operator's instructions.

If you have multi-currency or dynamic currency conversion facilities please call **01268 662 520**

Acceptable Cards

VISA



Visa cards are produced in many different designs and each Card identifies the issuer. All Visa cards have the Visa logo on the front of the Card. The position of the logo depends on the Card type.

The Card has the following features:

- 1 Visa logo – The blue logo on a white background will be displayed on the front of all Visa cards.
- 2 Chip – Most Cards carry an embedded chip which works together with the Cardholder's PIN or signature.
- 3 Visa 3D Secure logo – A dove in flight which moves and changes colour when tilted. The silhouetted, or silo, dove hologram is the latest version. This can be located on the front or on the reverse of the Card.
- 4 Embossed or printed account number – The embossed or printed account number, which can be up to 19 digits.

Some unembossed Visa cards may only be printed with a partial account number.

Part of the account number must match the printed account number on the sales receipt.

- 5 Cardholder name – Most Visa cards will carry an embossed or printed Cardholder name, which may also include their title.
- 6 Printed Bank Identification Number (BIN) – The four-digit printed BIN number must appear below the account number and must match the first four digits of the embossed or printed account number.

These Card images are for visual purposes only.

Acceptable Cards

- 7 Expiry date – Every Visa card must have an expiry date. Some may also include an optional ‘Valid From’ date.
- 8 Ultraviolet mark – When placed under an ultraviolet light newer Visa cards will have a ‘V’ visible over the Visa logo. On older Cards a dove will appear in the centre of the Card.
- 9 The category identifier displayed on the Card must match the product encoded on the magnetic stripe and (where applicable) the EMV chip.
- 10 Magnetic stripe – The magnetic stripe holds information about the Card and appears on the back of all Cards.
- 11 Card Security Code (CSC) – The three-digit security code may appear:
 - On the signature strip next to the full Card number or Card number showing only the last four digits.
 - Alternatively it may appear in a white box beside the signature strip.
- 12 Signature strip – The signature strip may be customised and may vary in length from Card to Card. On some older Cards it may still extend the entire width of the Card. The last four digits of the Card number, together with a three-digit Card Security Code, will appear on the right-hand side. Some older Cards in circulation may show the whole account number followed by the three-digit Card Security Code.

It is now optional on current Visa cards for the ‘flying V’ (the letter V tilted to the right) to appear next to the expiry date on the front of the Card.

Acceptable Cards

Visa Credit



Visa Debit



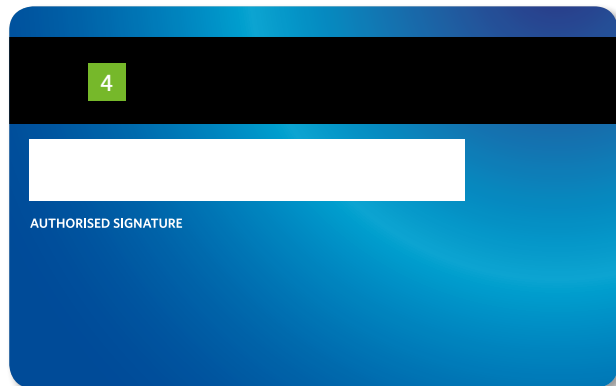
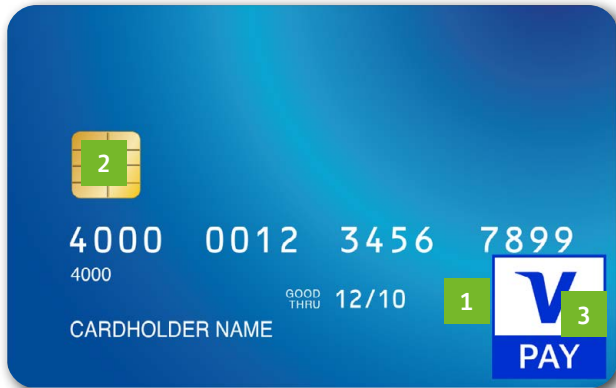
These Card images are for visual purposes only.



Speed and convenience

Cardnet makes payment faster and easier for you and your customers.

V PAY



V PAY is a Visa debit card issued by banks from around Europe to their customers. The big difference with V PAY is that it is a chip and PIN only Card, so it is very easy to accept and the risks of fraud and associated disputes are greatly reduced.

V PAY cards mandatory features:

- 1 V PAY logo – The V PAY logo is the blue Visa logo on a white background and can be displayed in three locations on the front of the Card (upper left, upper right or lower right).
- 2 Chip – Is located on the front of the Card. Cardholders are required to enter a PIN to make a purchase.
- 3 Ultraviolet mark – When placed under an ultraviolet light, a 'V' printed in ultraviolet ink is visible over the V PAY logo.
- 4 Magnetic stripe – Holds information about the Card and appears on the back of all Cards.

Optional features:

Features that can appear on the front or back of the Card:

- The Cardholder's name.
- The expiry date.
- Cardholder number – The unembossed number can be between 16 and 19 digits.
- Issuer identification (bank name) – May appear on the front or the back of the Card.

These Card images are for visual purposes only.

Acceptable Cards

- Contactless indicator – Can be displayed in Visa blue, black or white.
- Cardholder photograph.
- Domestic debit scheme mark.

Features that only appear on the front of the Card:

- Printed BIN (Bank Identification Number) – The four-digit printed BIN number must appear below the account number and must match the first four digits of the printed account number.

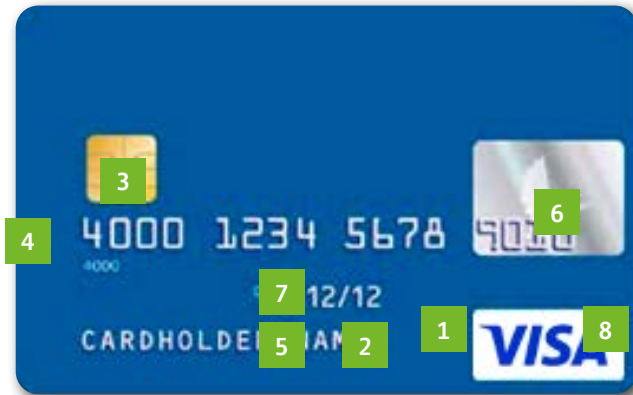
Features that only appear on the back of the Card:

- Signature strip – Can be customised and can vary in length from Card to Card.
- Plus symbol – Allows ATM services.
- Card Security Code (CSC) – Three-digit security number.

Important

- Authorisation – All V PAY Transactions must be authorised – either online or offline – at the time of the Transaction.
- Internet (E-commerce) V PAY cards can be used to make purchases over the Internet if permitted by the issuer. However, you must be registered for Visa Secure to be allowed to display the V PAY logo on your website.
- Mail order/telephone order and Recurring Transactions – V PAY cannot be accepted for mail order/telephone order or Recurring Transactions.

Visa Electron



- 1 Visa Electron logo – Always appears on the front of the Card, usually on the right-hand side.
- 2 'Electronic Use Only' legend – Visa Electron cards are printed with the wording 'Electronic Use Only' and this may appear on either the front or the back of the Card.
- 3 Chip – Most Cards carry an embedded chip which works together with the Cardholder's PIN or signature.
- 4 Account number – 16-digit account number with first four digits printed below. Not all Cards show the full account number, however, in the UK the full account number is required.
- 5 Cardholder name – This is always unembossed and appears on the front of the Card. The Cardholder's title may also be present.
- 6 Hologram – The hologram is optional for Visa Electron cards and features a dove in flight which moves and changes colour when tilted. This may be located on the front or on the reverse of the Card.
- 7 Expiry date – Every Visa card must have an expiry date. Some may also include an optional 'Valid From' date.
- 8 Ultraviolet mark – When placed under an ultraviolet light newer Visa Electron cards will have a 'V' visible over the Visa logo. On older Cards a dove will appear in the centre of the Card.
- 9 Card Security Code (CSC) – The Card Security Code will only be present if the full account number appears on the front of the Card. If present, the Card Security Code may appear on or to the side of the signature strip.

These Card images are for visual purposes only.

- 10 Signature strip – This may appear in the traditional position or lower and may vary in length. Visa Electron is a globally accepted payment Card and all Transactions must be authorised regardless of the amount. In the UK, the Visa Electron will be primarily issued as a debit Card and will have the full account number printed on the front.
- 11 Magnetic stripe – The magnetic stripe holds information about the Card and appears on the back of all Cards.

Important

- Point of Sale Transactions – As the Visa Electron card can only be accepted electronically, it must be inserted into the Terminal or swiped through the Terminal in a Card present environment. It cannot be key entered or accepted on paper vouchers even for Fallback if your Terminal is not working.
- Card Not Present Transactions – In a Card Not Present environment, key entry is permitted.
- E-commerce Transactions – Visa Electron can be accepted over the Internet.

The above procedures must be adopted for all Visa Electron payments. If these procedures are not followed we reserve the right to Dispute any Transaction.

Electron Card means a Visa Card which must always be submitted for Authorisation to the Bank.

Visa Prepay

Visa issues prepay Cards where funds have been preloaded onto the Card. These Cards carry the Visa logo and should be treated the same as a Visa debit card. These Cards will display a category identifier of “Prepaid”.

Visa and Visa Electron mini cards

Visa has produced miniaturised Visa and Visa Electron cards. These Cards carry the Visa and Visa Electron logos in reduced sizes positioned in either the bottom or top right of the Card.

The Visa mini dove hologram will always appear on the Visa card but is optional on the Visa Electron mini card.

The mini dove hologram can appear on either the front or the back of the Card.

Other features include:

Signature strip

A signature strip can be found on the back of the Card.

Magnetic stripe

The magnetic stripe can be found on the back of the Card.

Card Security Code

The three-digit security code may appear on the signature strip next to the full Card number (or alternatively the last four digits from the Card number) or it may appear in a white box beside the signature strip.

Cardholder photograph and signature

A photograph of the Cardholder may appear on either the front or back of the Card.

Visa SimplyOne card

The Visa SimplyOne card is a multiple payment chip Card that will provide Cardholders with two (or more) payment applications (for example, debit and credit) on a single chip Card.

The Card design has two Card numbers and two Card Security Codes. The Card number for the main functionality is embossed on the front of the Card with a corresponding Card Security Code positioned beside the signature strip on the reverse of the Card. The secondary Card number and Card Security Code are printed on the reverse of the Card.

Both Card functions share the same validity dates.

A Card that is both a debit and a credit Card will have ‘Debit/ Credit’ printed below the Visa logo on the front of the Card. This Card will allow the Cardholder to choose at the point of sale whether to use the Card as a debit or a credit Card.



For further information about
Visa and its interchange rates
visit www.visaeurope.com

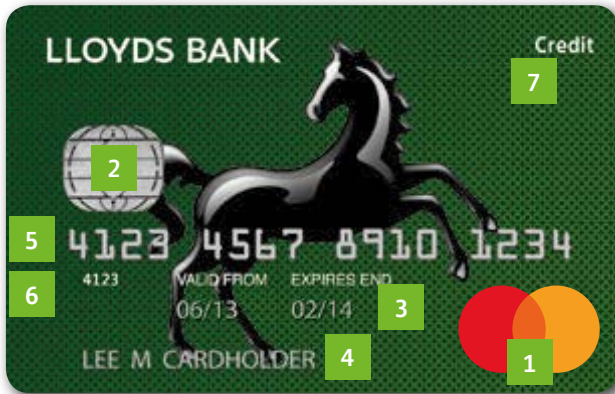


The efficient way to trade

Rapid, secure Transactions and easier
payment reconciliation.

Acceptable Cards

Mastercard®



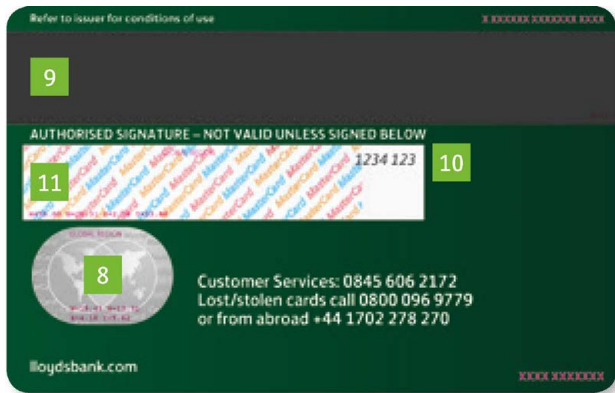
Mastercard® cards are produced in many different designs and each Card identifies the issuer. All Mastercard cards have the Mastercard logo on the front of the Card.

All Mastercard cards carry the following features:

- 1 Mastercard logo – The Mastercard symbol of two interlocking globes and the Mastercard hologram will appear together surrounded by a retaining line on the front of the Card. Alternatively the two interlocking globes will appear on the front of the Card and the hologram will appear on the back.
- 2 Chip – Most Cards carry an embedded chip which works together with the Cardholder's PIN or signature.
- 3 Expiry date – Every Mastercard card must have an expiry date. Some may also include an optional 'Valid From' date.
- 4 Cardholder name – Most Cards carry an embossed or printed Cardholder name and may also include their title.
- 5 Embossed or printed account number – The embossed or printed account number, which can be up to 19 digits.

Part of the account number must match the printed account number on the Sales Receipt.

- 6 Printed Bank Identification Number (BIN) – The four-digit printed BIN number must appear below the account number and must match the first four digits of the embossed or printed account number.
- 7 The category identifier displayed on the Card must match the product encoded on the magnetic stripe and (where applicable) the EMV chip.



These Card images are for visual purposes only.

Acceptable Cards

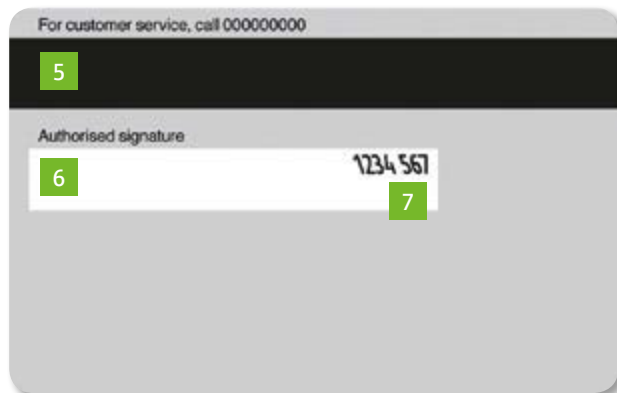
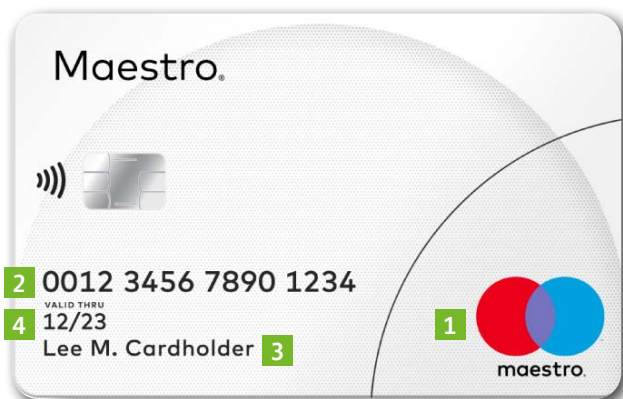
- 8 Mastercard 3D interlocking globe hologram – The hologram can appear on the front or the back of the Card and shows two interlocking globes which move and change colour when tilted.
- 9 Magnetic stripe – The magnetic stripe holds information about the Card and appears on the back of all Cards.
- 10 Card Security Code (CSC) – The three-digit security code may appear on the signature strip next to the full Card number (or alternatively the last four digits from the Card) or it may appear in a white box beside the signature strip.
- 11 Signature strip – Many Cards will carry a shortened signature strip; however, on some older Cards it may still extend the entire width of the Card. The signature strip is tamper-evident and will always be printed with a Mastercard repeat pattern.

It is now optional on current Mastercard cards for the letters 'MC' tilted to the right to appear next to the expiry date on the front of the Card.

Debit Mastercard



Maestro®



Maestro® is the debit Card brand owned by Mastercard and is issued by many different banks, both in the UK and overseas.

All Maestro cards identify the issuer and feature the standard blue and red Maestro logo on the front of the Card.

Usually Cards will carry the following details:

- 1 Maestro logo – The blue and red interlocking circles with the word 'Maestro' printed across the centre in white.
- 2 Cardholder number – This can be between 12 and 19 digits.
- 3 The Cardholder's name – Most Cards carry an embossed or printed Cardholder name and may also include their title.
- 4 The expiry date – Every Mastercard card must have an expiry date. Some may also include an optional 'Valid From' date.
- 5 The magnetic stripe.
- 6 Signature strip – This may be printed with the word 'Maestro' in repeat pattern and may also contain the last four digits of the Cardholder number followed by the three digit Card Security Code.
- 7 Card Security Code (CSC) – The three-digit security code may appear on the signature strip next to the full Card number (or alternatively the last four digits from the Card) or it may appear in a white box beside the signature strip.

Please note, there are some fundamental differences in the appearance of UK Maestro cards and internationally issued Maestro cards.

These Card images are for visual purposes only.

Acceptable Cards

Some may also contain the following:

- The chip.
- The hologram.
- The Cardholder's title (for example, Mr, Mrs, Miss).
- The start date.
- The Card issue number – This is the sequential number used to identify Cards issued on the same account. It will be one or two digits only.
- ATM functionality.

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

Please ensure that your staff are trained to accept Maestro cards, and are familiar with these procedures.

Maestro

Maestro Transactions must always be processed through your Terminal. Some Maestro cards have additional functionalities such as ATM.

International Maestro

All internationally issued Maestro Transactions must be authorised and your Terminal will recognise this. (In the event of failed Card read or swipe, please refer to the Terminal Fallback procedures set out in Section 9, 'Exceptions'.)

If you accept E-commerce Transactions you must be registered for Mastercard Identity Check before you can accept any Maestro or International Maestro cards.



For further information about Mastercard and its Interchange rates visit www.mastercard.us/merchants/support

Mastercard® Digital First Card Programme (DFCP)

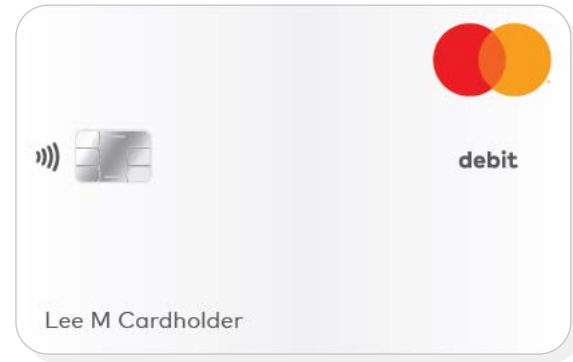
The Mastercard DFCP enables consumers to pay for goods and services without a physical card or with a physical card that excludes card account information. It enables consumers to pay at POS digitally using wallets such as Apple Pay or Google Pay.

Mastercard Secure Symbol

Mastercard Secure Symbol can now be used on most Mastercard card types replacing the traditionally printed Mastercard Symbol.

The Mastercard Secure Symbol must be stamped on the card front.

When used, the Mastercard Global Hologram or Debit Mastercard Hologram – Silver is optional.



This card is issued by Lloyds Bank pursuant to license by Mastercard International Incorporated.

Acceptable Cards

UnionPay®



These Card images are for visual purposes only.

The Cards have the following features:

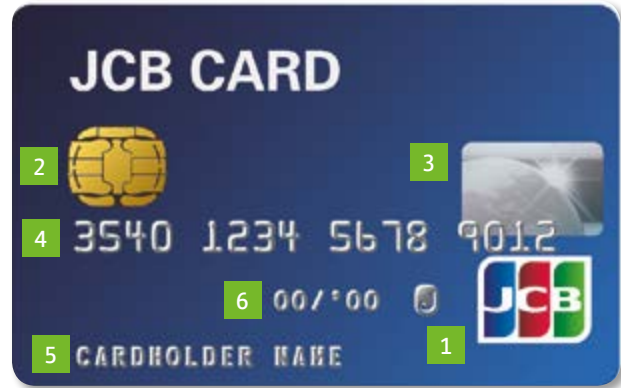
- 1 UnionPay logo – The three-colour logo of the UnionPay brand will be displayed on the front of all UnionPay cards.
- 2 Chip – Most Cards carry an embedded chip which works together with the Cardholder's PIN or signature.
- 3 UnionPay "Pagoda" hologram – A hologram of the Temple of Heaven this can be located on the front or on the reverse of the card. All UnionPay Credit cards have the hologram while most UnionPay debit cards do not have the hologram.
- 4 Embossed or printed account number – The embossed or printed account number can be up to 19 digits. Card Number on valid cards begins with "62" or "81".
- 5 Cardholder name – Most UnionPay cards will carry an embossed or printed Cardholder name, which may also include their title.
- 6 Expiry date – All UnionPay Credit cards have an expiry date on the card. Some UnionPay Debit cards do not have an expiry date shown on the card.
- 7 QuickPass (Contactless) Mark – QuickPass is a UnionPay contactless payment innovative product. Cardholder could pay with waving the QuickPass card in front of contactless payment terminal.
- 8 Magnetic stripe – The magnetic stripe holds information about the card and appears on the back of all UnionPay cards. Most magnetic stripe cards always require PIN, but some UnionPay Credit cards will require signature only which is selected by Cardholders when this is offered by the Terminal.
- 9 Card Verification Number 2 (CVN) – The three-digit security code will usually appear on the signature strip next to the last four digits of the account number on a UnionPay credit card.
- 10 The product name of Platinum, Diamond cards must be printed on the card face.
- 11 Prepaid, Debit, Credit, Corporate card must be printed on the card face.

Acceptable Cards

The Cards have the following features:

- 1 JCB logo – The JCB logo will be displayed on the front of all JCB cards.
- 2 Chip – Most Cards carry an embedded chip which works together with the Cardholder's PIN or signature.
- 3 JCB hologram – The JCB hologram appears on the front of the Card comprising of part of a globe with a rising sun in the background.
- 4 Embossed or printed account number – The embossed or printed account number is a 16 digit account number.
- 5 Cardholder name – Most JCB cards will carry an embossed or printed Cardholder name, which may also include their title.
- 6 Expiry date – Every JCB credit card must have an expiry date.
- 7 Magnetic stripe – The magnetic stripe holds information about the Card and appears on the back of all Cards.
- 8 Card Authentication Value 2 (JCB-CAV2). The three-digit security code appears on the signature strip next to the last four digits of the account number.

JCB®



These Card images are for visual purposes only.

Acceptable Cards

American Express



The Cards have the following features:

- 1 American Express logotype; “Business” or “Corporate” locked up with American Express logotype as applicable
- 2 Gingerbread Border
- 3 World Service Filigree Pattern
- 4 Member Since Ribbon
- 5 Centurion Portrait
- 6 Four-Digit Batch Code (4CSC or 4DBC)
- 7 Contactless Indicator: Size is fixed, Must be locked-up with 4DBC, black in colour
- 8 © AMEX
- 9 Personalised Embossing: Card member Name, Account Number, Valid Thru date (“Valid Thru” may appear in English and/or the local language)
- 10 Member Since year
- 11 Chip: Size and design varies per vendor
- 12 American Express Blue Box with registration mark
- 13 Silver Magnetic Strip will include “Cardmember Signature”
- 14 Signature Panel
- 15 Contactless Indicator: Size is fixed, required to be black or white in colour only

- 16 Property Legal Information
- 17 “Not transferable”
- 18 Issuer URL and/or Email Address
- 19 Customer Service Information
- 20 Issuer Legal Information
- 21 Printing Country & Date: May include country, month and year of print
- 22 Printer Code

CARDNET HELPLINE



Call 01268 567 100

8am to 9pm Monday to Saturday

Call our knowledgeable UK-based team with any questions about your Cardnet service or this Manual.

Discover® Global Network :

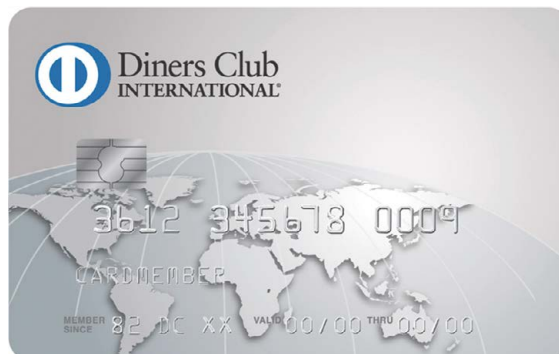
Discover® Global Network is the fastest growing global payments network¹ with over 270M cardholders around the globe and acceptance in over 200 countries and territories.

Discover® Global Network offers more than \$415 billion in spend opportunity from all of the cards that leverage its network, including Discover® from the United States, Diners Club International® issued in more than 55 countries, and 20+ Network Alliance Partners globally.

Activate Discover Global Network and you'll automatically have the ability to accept all these card types.

BC Global Card (South Korea), RuPay Global Card (India), Elo Global Card (Brazil), Troy Global Card (Turkey) are Discover® Global Network Alliance Partner Cards.

58% of Discover cardholders* look for signage before deciding on a merchant. To show you accept Discover and Diners cards you can order signage at no cost from [DiscoverGlobalSignage.com](https://www.discoverglobalsignage.com).



¹ Based on signed network alliance agreements over the past ten years with major payment networks within respective countries – Panoramic Research study, conducted 2018.

* Discover cardholders who have travelled internationally in the past 18 months.

C+R Research Study of 3,000 Discover Cardholders, April, 2018, commissioned by DFS Services LLC.

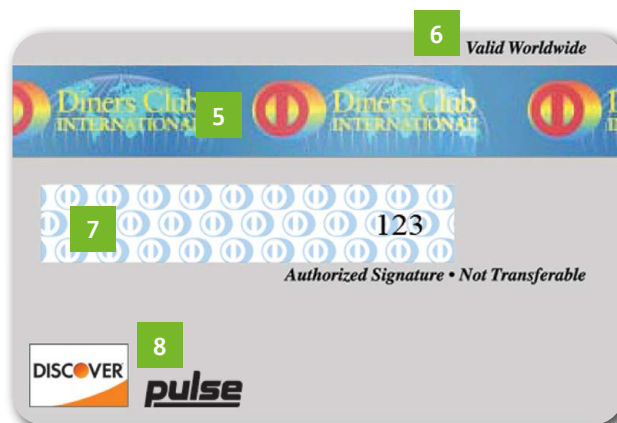
Acceptable Cards

Diners Club International® is a product of Discover Financial Services and is a globally recognised brand serving the needs of consumers, corporations and small business owners worldwide. The Cards come in many different designs (including some with the Cardholder's photo on the front or back of the Card), all have the Diners Club International logo on the front of the Card and co-branded Cards may also display the co-branded logo in the upper right-hand corner.

Some corporate Cards may also have the words 'Corporate Card' or 'Business Card' and the company or corporate name displayed on the front of the Card.

- 1 Chip – The Card may have a chip. Cards with chips also have a magnetic stripe. They have a shorter signature panel to accommodate the chip.
- 2 Embossed account number – All Diners Club account numbers start with 30, 36, 38 or 39. Embossed Card numbers should be uniform in size and spacing.
- 3 Expiry dates – 'Valid' and 'Thru' dates indicate the first and last month in which the Card is valid.
- 4 Some Diners Club® cards have a vertical design. The embossing, magnetic stripe and signature panel are still aligned across the long edge of the card.
- 5 Magnetic stripe – The holographic magnetic stripe contains a repeating image of the Diners Club International® logo, name and world map, which shift colour and appearance when the card is tilted. It should be smooth, with no signs of tampering. Three-digit CVV2 appears on the signature panel in independent printing (debossed). A full or partial account number may also appear in the same printing style.
- 6 The words "Valid Worldwide" must appear in the upper

Diners Club International®



These cards are for visual purposes only.

right corner of the card back, in a bold italic typeface.

- 7 The Diners Club International® split circle graphic may appear on a tamper-evident signature panel. The words “Authorized Signature – Not Transferable” are printed under the signature panel.
- 8 The Discover® and PULSE® acceptance marks must appear in the lower left corner of the card back.
- 9 The Diners Club® split-circle graphic with slash marks will appear on the card front under an ultraviolet light (not shown).

CARDNET HELPLINE



Call 01268 567 100

8am to 9pm Monday to Saturday

Call our knowledgeable UK-based team with any questions about your Cardnet service or this Manual.

Acceptable Cards

Discover® Global Network is the global payments brand of Discover Financial Services. Discover® Global Network includes Discover Network, which generates billions in annual volume and has alliances with more than 18 network alliances in the world.

- 1 The card may be a chip-enabled card, which will also have a magnetic strip on the back.
- 2 Card numbers will appear on either the front or back of the card. Card numbers begin with the number “6” and are composed of 16 digits that should be clear and uniform in size and spacing.
- 3 The “Valid Through” date may appear on either the front or back of the card in an mm/yy format that indicates the last month in which the card is valid.
- 4 The Discover Acceptance Mark will appear on the back of most cards, and may also appear on the front of the card, along with other affiliated logos.
- 5 The cardholder name and, if applicable, business name, will appear on either the front or back of the card.
- 6 A 3-digit Security Code (CID) will appear to the right of the signature panel.
- 7 An underprint of “VOID” on the signature panel becomes visible if erasure of the signature is attempted

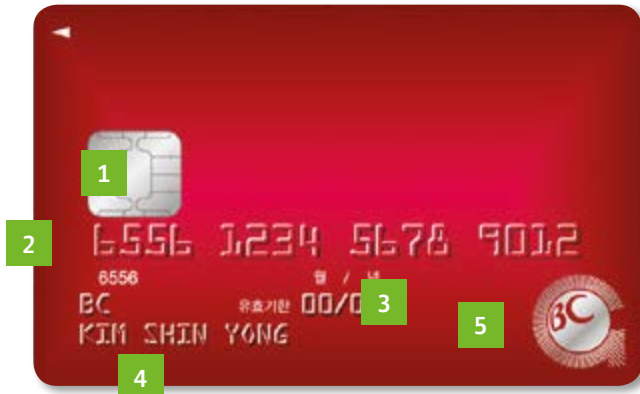
Discover®



These Card images are for visual purposes only.

Acceptable Cards

BC Global card



These Card images are for visual purposes only.

BC Global card is a partner brand of Discover® Global Network and is the largest domestic network in South Korea. As Korea's biggest credit Card company, BC Global card currently have 11 financial institution partners and have issued approximately 55 million Cards in Korea.

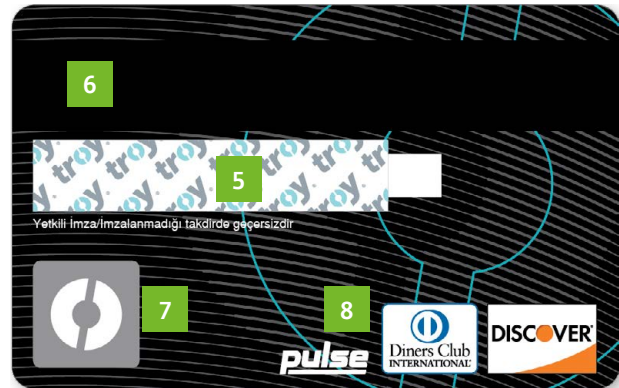
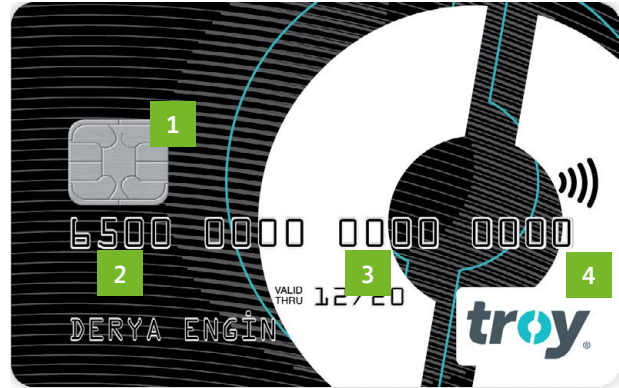
- 1 Contact module with an embedded D-PAS chip appears on the front card.
- 2 Embossed account number – BC Global Card account numbers start with 65. The account number appears on the front of the card.
- 3 Expiry date – 'Valid Thru' indicates the last month in which the Card is valid.
- 4 Cardholder name – The Cardholder name is embossed on the front of the Card.
- 5 BC Global card logo – The logo appears on the front of the Card.
- 6 Magnetic stripe – The magnetic stripe should appear smooth and straight, with no signs of tampering.
- 7 BCCard hologram.
- 8 Signature strip – The signature panel is shortened on chipenabled Cards. The signature on the Card should match the customer's signature on the charge record.
- 9 Acceptance marks – The back of the Card should display the acceptance marks of Discover®, Diners Club International® and PULSE®, in addition to the BC Global card Logo.
- 10 Some cards have a vertical format.

Acceptable Cards

The Cards have the following features:

- 1 An embedded D-PAS chip appears on the card front.
- 2 6-digit Troy Card number starts with 65. The card number appears on the front panel of the card.
- 3 "Valid Through" indicates the last month in which the card is valid.
- 4 Troy logo appears on the front of the card.
- 5 Signature on the back of the card should match the customer's signature on the charge slip. "troy" is printed repeatedly on a tamper-evident signature panel.
- 6 Magnetic stripe should appear smooth and straight, with no signs of tampering.
- 7 "O" from Troy appears on the back of the card.
- 8 The back of the card should display the Acceptance Marks of Discover®, Diners Club International® and PULSE®.

Troy Card Global (Turkey)



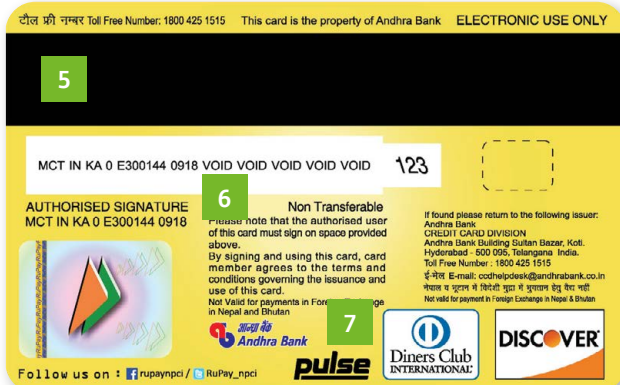
Acceptable Cards

RuPay



The Cards have the following features:

- 1 An embedded D-PAS chip appears on the card front.
- 2 6-digit RuPay Card number starts with 65. The card number appears on the front panel of the card.
- 3 “Valid Through” indicates the last month in which the card is valid.
- 4 RuPay logo appears on the front of the card.
- 5 Magnetic stripe should appear smooth and straight, with no signs of tampering.
- 6 Signature on the back of the card should match the customer’s signature on the charge slip.
- 7 The back of the card should display the Acceptance Marks of Discover®, Diners Club International® and PULSE®.



Acceptable Cards

The Cards have the following features:

- 1 An embedded D-PAS chip appears on the card front.
- 2 6-digit Elo Card number starts with 65. The card number appears on the front panel of the card.
- 3 "Valid Through" indicates the last month in which the card is valid.
- 4 Elo logo appears on the front of the card.
- 5 Magnetic stripe should appear smooth and straight, with no signs of tampering.
- 6 Signature on the back of the card should match the customer's signature on the charge slip. "elo" is printed repeatedly on a tamper-evident signature panel.
- 7 The back of the card should display the Acceptance Marks of Discover®, Diners Club International® and PULSE®.

Elo Global Card (Brazil)







More choice for your customers

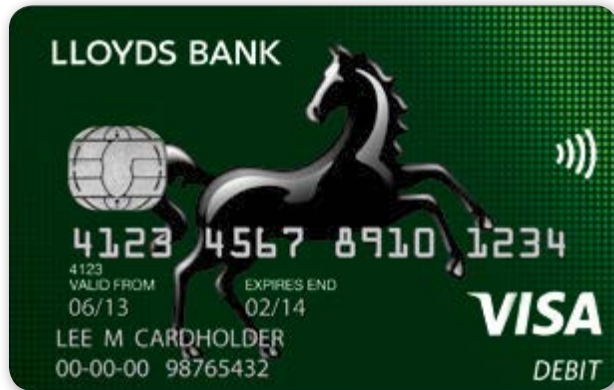
Accept payment from one of
the widest ranges of Card
Schemes available.



Contactless technology offers swifter Transactions

Call our helpline to find out more.

Contactless



These Card images are for visual purposes only.

Contactless enabled Cards are now a significant proportion of the UK Card population. These Cards enable purchases for low value Transactions (£100 as of October 2021) to be undertaken by waving the Card over a Contactless enabled payment acceptance device. This improves the customer payment experience, speeds up Transactions and helps retailers to remove cash and cheques from their business.

As part of the security systems for this type of Transaction and to protect both consumers and retailers, on occasion, the Contactless Transaction will be disallowed and a prompt for a chip and pin Transaction will be made. This is a normal action which has been built into the system by the Card Schemes. You will recognise a Contactless enabled Card as it will carry the Contactless logo (see left).

Payments using mobile phones and FOBs

Contactless technology is constantly evolving and there are now an increasing number of prepaid Contactless devices available such as mobile phones and FOBs. These work in the same way as a Card by waving the phone or FOB over a contactless enabled payment acceptance device.

-))) All terminals must be enabled and switched on to accept Contactless transactions and you must promote acceptance by displaying the correct acceptance marks. **These are available by contacting the Cardnet Helpline on 01268 567 100**

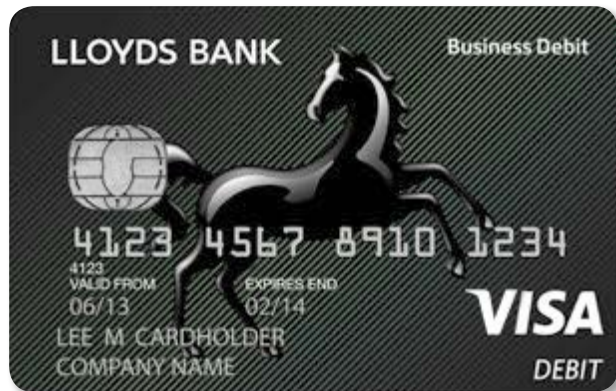
Commercial Cards

Commercial Cards bring specific benefits to a business-to-business sales Transaction. They look like any other Visa or Mastercard card although many have the description of the Card's function on the front of the Card. For example, 'Purchasing Card'.

There are three main types of Commercial Cards:

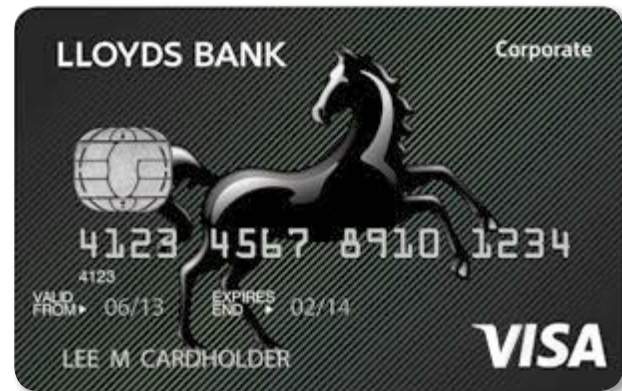
Business Card

- Suitable for paying everything a small business needs (e.g. stationery, office supplies, travel and entertainment etc.).
- Provides small businesses with a business payment method, an expense control mechanism and a cash management tool.
- Available as charge and credit Cards.



Corporate Card

- For travel and entertainment for mid-sized to large companies.
- Provides management information which makes it easier to control expenditure and to manage business expenses.
- Allows streamlined administration of expenses, saving time and money by reducing cash handling and paper-based payment methods.



These Card images are for visual purposes only.

Acceptable Cards

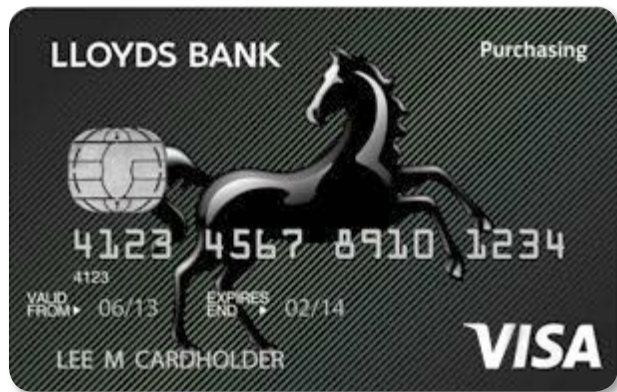
Purchasing Card

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

- Used by Government departments, public sector bodies and large businesses.
- Enables control and monitoring of expenditure and the provision of data and information to help improve cost management.
- Allows VAT reclamation.
- Removes paper-based processes, through electronic invoicing with detailed breakdowns of expenditure.

BENEFITS

In order to capture the full benefits of purchasing Cards you will need to upgrade your point of sale equipment. For more detailed information or operating instructions contact the Cardnet Helpline on **01268 567 100**



These Card images are for visual purposes only.

3 : Checking the Card

The following details need to be checked carefully on all Cards, even if the holder is well known to you or is a regular customer.

Checking the Card

The name of the Card (e.g. Visa/Mastercard/Maestro, UnionPay, JCB, Amex, Diners Club International, Discover and BC Global card) and Card Issuer (for example, Lloyds Bank) should appear in bold letters on the Card. You should also check the following:

Security features

Front of Card

- 1 Microchip.
- 2 Card number.
- 3 Bank Identification Number (BIN).
- 4 Validity date.
- 5 Cardholder's name/title.
- 6 Contactless function.

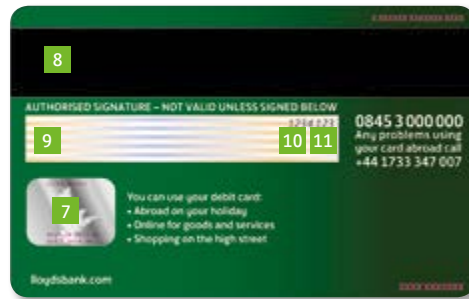


These Card images are for visual purposes only.

Back of Card

- 7 The hologram – the hologram may appear on the front or the back of the Card depending on the Card type. On this example the hologram appears on the back.

- 8 Magnetic stripe.
- 9 Tamper evident signature strip which must be signed.
- 10 Last four digits of the Card number (some older Cards in circulation may show the whole account number).
- 11 Card Security Code.



These Card images are for visual purposes only.

The number embossed on the front of the Card may be 12 to 19 digits in length dependent on the type of Card presented.

This number is tied to the information encoded in the chip, on the magnetic stripe and the number indent-printed on the signature strip. This enables Card Issuers and sales staff to immediately recognise a counterfeit Card when these codes do not match. This makes it more difficult to alter encoded information.

The easiest way to check for inconsistencies in this information is to make sure that the last four digits of the Card number embossed on the front of the Card match the last four digits electronically printed on the Terminal receipt.

Checking the Card

Card Security Codes (CSC)

The three-digit CSC may appear on the signature strip next to the full Card number (or alternatively the last four digits from the Card number, or it may appear in a white box beside the signature strip. These additional digits are a further security feature for use in 'Card Not Present' (CNP) Transactions. (See Section 4, 'Accepting Transactions' p46.)

Tamper-evident signature strip

The signature strip on most Cards has a feature whereby the strip will change colour if the signature is tampered with.

Indent printing

The last four digits of the Card number, together with the three-digit CSC, are printed using a unique reverse italic font on the signature strip on the back of the Card which makes alteration extremely difficult. The four digits should match the last four digits of the Card number on the front of the Card. Some older Cards in circulation may show the whole account number followed by the three-digit CSC.

UV (ultraviolet) lamp test

You may already use a UV lamp to check for fake bank notes. Cards can also be checked in the same way. If you place a genuine Card under a UV lamp you should see a special mark. If these features do not show, the Card is probably a counterfeit. In these circumstances you should make a Code 10 call to the Authorisation Centre, see Section 7, 'Security, Suspicious Transactions'.

Visa UV image

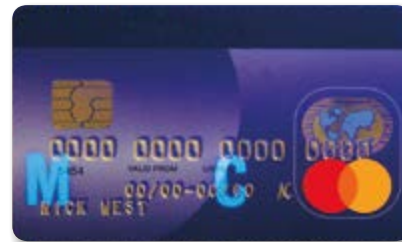
Older Cards will still show the dove image in the centre of the Card. Please be aware that some Electron cards do not have a UV image.

Newer Visa cards will show an ultraviolet 'V' over the Visa brand mark.



Mastercard UV image

Mastercards will show the letters 'MC'.



These Card images are for visual purposes only.

Checking the Card

Maestro UV image

The word Maestro will show on the front of the Card in the bottom left-hand corner.



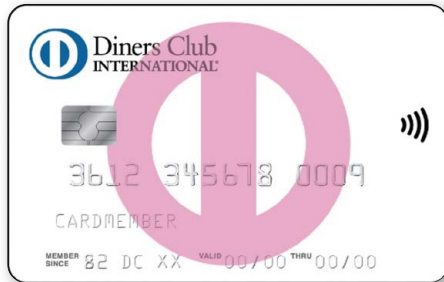
Discover card UV image

'DISCOVER' or 'DISCOVER NETWORK' will appear across the middle of the Card under an ultraviolet light.



Diners card International UV image

The Diners Club split circle graphic in an invisible line pattern will appear in the middle of the card in red cast fluorescent ink.



These Card images are for visual purposes only.

Hologram

Check the hologram which appears on the face or reverse of all Visa, Mastercard®, Maestro®, Diners Club International®, and Discover® cards.

The holograms to look for are:

- Visa and Visa Electron – A flying dove which moves and changes colour when tilted.
- Mastercard – Two interlocking globes which change colour when tilted.
- UK Maestro – Maestro logo.
- UnionPay – UnionPay “Pagoda” hologram – A hologram of the Temple of Heaven which can be located on the front or on the reverse of the Card.
- Diners Club International – Most Cards carry a holographic magnetic stripe containing a repeating image of the logo, Diners Club International name and world map which shift colour and appearance when the Card is tilted. It should appear smooth, with no signs of tampering. Some Cards may have a standard black magnetic stripe.
- Discover – All Cards display a hologram on the front of the Card with a globe pierced by an arrow, unless the back of the Card displays a holographic magnetic stripe.

CARDNET HELPLINE



Call 01268 567 100

8am to 9pm Monday to Saturday

Call our knowledgeable UK-based team with any questions about your Cardnet service or this Manual.

Additional checks

The following additional checks will help you validate the Cards handed to you when carrying out Point of Sale Transactions.

- 1 Validity dates: The majority of Cards will have effective (valid from) and expiry (valid to) dates which are located on the face of the Card. The Transaction date must fall on or between these dates. Do not accept a Card prior to the effective date (the first day of the month) or after the expiry date (up to and including the last day of the month) or you may be subject to a Dispute. Some Cards may just have an expiry date. In these cases you'll need to make sure that Transactions are not accepted after the last day of the month of expiry.

Please note that some V PAY cards may not have either a valid from or expiry date.

- 2 Cardholder's title: If the Cardholder's title is embossed on the front of the Card (for example, Mr, Mrs) check that it is appropriate to the person presenting the Card. Check that there is no obvious discrepancy between the Cardholder and the Card.
- 3 Cardholder's signature: The signature strip should not be disfigured or tampered with in any way and should have only one signature. If you are presented with an unsigned Card, please contact the Authorisation Centre immediately for advice, stating "This is a Code 10 Authorisation" – see Section 7, 'Security, Suspicious Transactions'. Do not allow the Cardholder to sign the Card until you have received

instructions from the Authorisation Centre. If the Card is a chip and PIN Card and the Cardholder has successfully entered the PIN, they should be advised to sign the Card.

- 4 Bank Identification Number (BIN): On Visa and Mastercard cards check that the first four digits of the Card number are printed in small characters below the first four digits of the Card number. If the four digits are missing or do not match, the Card is probably counterfeit.
- 5 Damaged Cards: Ensure that the chip or magnetic stripe on the Card you are presented with has not been mutilated or damaged in any way.

Code 10

If after making these checks you think the Card may be invalid, keep the Card and do not release the goods or provide the services. Telephone the Authorisation Centre immediately, stating "This is a Code 10 Authorisation" – see Section 7, 'Security, Suspicious Transactions'.

Reward

If the Card Scheme participates in the reward scheme, a reward may be payable to any Cardnet Merchant who recovers a Card, when requested to do so by the Authorisation centre. The amount of the reward is dependent on the Card Scheme.

Please note: Discover® Global Network do not participate in the Reward scheme. This means we are unable to pay a reward for the recovery of Diners Club International®, Discover®, BC Global Card, Troy Global Card, RuPay Global Card, and Elo Global Card.

4 : Accepting Transactions

This section explains how to conduct the various types of Transaction smoothly and securely.

Accepting Transactions

Cardnet allows your business to accept Point of Sale Transactions and, with our written agreement, Mail/Telephone Transactions using certain types of Card. You can also accept Internet payments by applying to Cardnet for an E-commerce facility.

Point of Sale Transactions

All Transactions must be processed through an electronic Terminal.

Always follow the instructions shown in the user Manual supplied with your Terminal.

Below is a brief summary of the procedures you need to follow when processing Card Transactions.

Chip and PIN Card Transactions

- 1 Ensure the Card is inserted into the Card reader.
- 2 Follow your Terminal operating instructions.
- 3 The Cardholder will be prompted to enter their PIN.

What if the Cardholder enters an incorrect PIN?

Dependent on the Card Issuer rules, ordinarily the Cardholder has three chances to enter their PIN. After this if the PIN is entered incorrectly the PIN will lock. At this stage you should tell the Cardholder that their PIN has locked and ask for an alternative method of payment.

Contactless receipt.



Verified by PIN receipt.



Chip Card Transactions

- 1 Insert the Card into the Card reader.
- 2 Follow your Terminal operating instructions.
- 3 Ask the Cardholder to sign the receipt.

Please be aware that some chip Cardholders may still have chosen to identify themselves with a signature rather than a PIN. In these circumstances please check the Card following the instructions in Section 3, 'Checking the Card' (p40).

Accepting Contactless Card payments

- 1 The Cardholder simply waves their Card, FOB, mobile phone or other device over the Contactless reader.
- 2 Transaction complete.

Sales – a single Contactless Transaction is permitted only for an amount under a predefined limit set by the Card Schemes. We will notify you of the current limit and let you know if there is any change to this limit. Transactions above the 'Contactless' limit must be processed following your Terminal prompts.

Refunds – all Refunds should be processed following your Terminal prompts.

Any Transaction that is not able to be processed as a Contactless Transaction should be processed following your Terminal prompts.

There will be occasions where it will be necessary for additional security checks to be carried out on Contactless Cards which will require the sale to be a full chip and PIN Transaction. Cardholders will be aware of this.

Receipts – The Cardholder should be offered a receipt, but it is optional for the Cardholder to accept.

Important

If a chip and PIN Card is presented and for any reason you process the Transaction without a PIN being entered, you may be liable for any Disputes.

Magnetic stripe only Card Transactions

Most UK Cards are issued with chip and PIN; however, some Cards will continue to be issued without a chip and will be read by the magnetic stripe. This also tends to be the case for some Cards issued outside Europe. Please examine these Cards carefully.

- 1 Check the Card: Follow the step-by-step instructions in Section 3, 'Checking the Card' (p40). Only when you are satisfied with all checks, should you proceed.
- 2 Swipe the Card: Refer to the procedures in your Terminal operating instructions. As an extra security measure you may be prompted to key enter the last four digits of the number embossed on the front of the Card. The Terminal will then check these numbers against those held in the Card's magnetic stripe.
- 3 Authorisation: All Transactions must be authorised. Refer to Section 5, 'Authorisation and referrals' (p105).
- 4 Check the receipt: Compare the Card number printed on the receipt with the number embossed on the front of the Card-see Section 3, 'Checking the Card'. If the numbers do not match, telephone the Authorisation Centre immediately for advice, stating "This is a Code 10 Authorisation" – see Section 7, 'Security, Suspicious Transactions' (p128).

You must retain copies of all Sales and Refund Receipts for a minimum of 13 months. This will assist you in checking your statements and resolving any possible Disputes. Please see Section 7, 'Security' (p120) for details on how this information must be stored. If you are unable to produce a copy, the Transaction may be charged back to you.

- 5 Return the Card: Once you have completed all the above steps, return the Card to the Cardholder together with any goods purchased and a signed copy of the receipt.

Mag-stripe receipt.



Note: Not all Card Schemes support Code 10 Authorisation calls. In this scenario please request an alternative method of payment from the Cardholder. Also, subject to local law, a signature is no longer a requirement.

Card Not Present (CNP) Transactions

Provided you have received written agreement from Cardnet you may accept a Mail/Telephone Transaction from a Card holder who wishes to pay using a Visa, Mastercard, Maestro, Diners Club International, Discover, BC Global, Troy Global, RuPay Global, Elo Global or American Express card.

You must not accept internationally issued Maestro cards and V PAY for CNP Transactions. Visa Electron cards can be accepted for CNP, as long as Transactions are always authorised. You cannot accept CNP payments for JCB or UPI cards.

When accepting a CNP order, please take extra care to ensure you have permission to debit the Card account and it is the genuine Card holder who placed the order as you are responsible for any Transactions where the Card and the Card holder are not present.

The following examples are all acceptable as CNP orders.

Mail Transactions – written authority from the Cardholder, bearing the Cardholder's signature in any form including:

- Completed order forms.
- Facsimile transmissions.

If you conduct CNP Transactions by mail, the Card holder's signature must appear on your order form. You must also keep the instruction for 13 months in case the Transaction is disputed at a later date.

Telephone Transactions – authority from the Cardholder by telephone.

When taking an order by telephone always record in writing all details of the Transaction along with time and date of the conversation as you may be asked to produce this or the Cardholder's authority for a CNP sale if the Transaction is disputed at a later date.

For all orders received by mail, telephone or fax, goods must be delivered and it is advisable to keep documentary evidence of the delivery address for 13 months.

If you are unable to deliver the goods immediately, your Authorisation is only valid for seven calendar days.

All Mail/Telephone Transaction records must be kept securely. Full details about how to store Cardholder information can be found in Section 7, 'Security'.

Collecting Cardholder information for CNP Transactions

When a Cardholder is not present for the sale, you must obtain the following information in order to verify their identity and help validate the Transaction:

- Card number.
- Card expiry date.
- Card issue number, if present on the Card.
- Cardholder name and initials as shown on the Card.
- The Card Security Code (CSC) (the three-digit number on or near to the signature strip on the back of the Card, or on American Express cards the four-digit number on the front of the Card).
- The address known to the Cardholder's bank (for example, where their Card statements are sent to).
- Contact telephone number (it is a higher risk to accept a mobile telephone number).

This information will enable you to carry out the usual status check so that you can confirm whether the Cardholder has sufficient funds to pay you. It also allows you to find out whether or not the Card has been reported lost or stolen.

You will be asked to produce this information, except for the CSC, if the Transaction is disputed at a later date.

Important

Under no circumstances can goods paid by mail or telephone be handed Point of Sale to, or collected by, the Cardholder. See Section 7, 'Security, How to guard against fraud' (p130).

If a Cardholder wishes to collect the goods, then they must attend your premises in person and produce their Card. Any Sales Voucher already prepared must be destroyed and a Point of Sale Transaction processed. If you have already completed a CNP order you must either cancel the Transaction or perform a Refund. If you perform a Refund, please let the Cardholder know that the original Transaction, a Refund and the Point of Sale Transaction will all appear on their Card statement.

If Authorisation was obtained for the original Transaction, or your Terminal indicates that Manual Authorisation is required, you must telephone the Authorisation Centre.

The Address Verification Service (AVS) and Card Security Code (CSC)

Since the introduction of chip and PIN fraudsters have increased their activity in Card Not Present Transactions.

As you are responsible for any Transactions where the Card and the Cardholder are not present, as well as collecting the Card Security Code (CSC), we recommend you complete these Transactions using the Address Verification Service.

Accepting Transactions

What are the Address Verification Service and Card Security Code?

The Address Verification Service (AVS) is available on all UK issued Cards, with the exception of Discover® Global Network and partner Cards, and allows you to check the numerical part of the Cardholder's postcode and statement address with the Card Issuer.

- 1 Card Security Code (CSC) – The three-digit security code may appear on the signature strip next to the full Card number (or alternatively the last four digits from the Card) or the four digits on the front of an Amex or it may appear in a white box beside the signature strip.

Please remember you remain ultimately responsible should a Transaction be confirmed as invalid or fraudulent, even if the AVS and CSC data matches and an Authorisation code is given.

Collecting the Card Security Code and Address Verification information

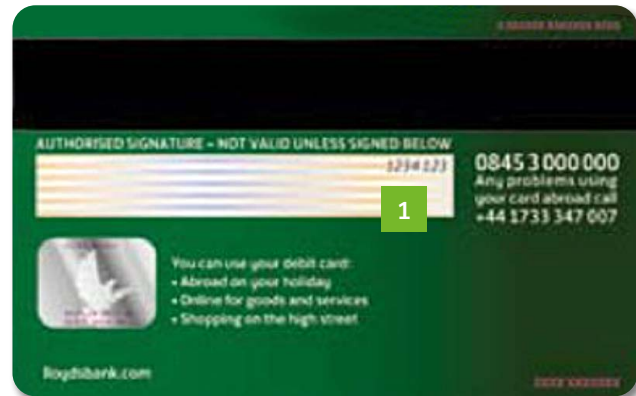
You must always ask the Cardholder for their Card Security Code as this is a good indication that they have the Card in their possession when they are ordering from you.

On the majority of Cards, only the last four digits of the Card number are repeated in the signature strip, followed by the three-digit CSC.

- 2 For American Express cards the CSC is a four-digit number and it appears on the front of the Card.

Please remember that you must not retain the CSC after the Transaction has been authorised.

Please note you can verify the CSC on Discover and Diners Club International cards. However, the AVS is not supported on these Cards.



These Card images are for visual purposes only.

Accepting Transactions

Address Verification Service

Because criminals can use lost or stolen Cards to order goods in CNP situations, it is possible that they might be able to give you the CSC. However, it is less likely that a fraudster would also have the Cardholder's address, so the AVS will act as an additional check.

The AVS is available on all UK issued Cards, with the exception of Discover® Global Network and partner Cards, and allows you to check the numerical part of the Cardholder's postcode and statement address with the Card Issuer.

You will need to ask the Cardholder for their address as recorded by their Card Issuer and input the relevant numbers as shown in the examples below.

Cardholder's details to be entered:

Cardholder's address	Card Security Code	Post Code Numeric	Address numerics*	Details to be entered when prompted by your Terminal
20 High Street Any Town Any County TN26 2BN	123 or 7594	262	20	12326220 or 759426220
Flat 1A 25 London Road Any Town Any County BN4 6RJ	123 or 7594	46	125	12346125 or 759446125
Rose Cottage Mill Lane Any Town Any County SS21 3HP	123 or 7594	213		123213 or 7594213
Flat 12A 1067 Main Road Any Town Any County RG12 4UB	123 or 7594	124	12106	12312412106 or 759412412106

*Maximum five digits
(if over five, take first five digits).

When using an electronic Terminal enabled with the AVS functionality to process CNP Transactions, your Terminal will automatically prompt for the AVS information and call the Authorisation Centre as normal. Transactions should take the same time to authorise, even though you have given us more information to check.

The CSC and AVS are designed to eliminate the need for CNP Code 10 calls, this means the Authorisation Centre cannot be used for any additional checking. This is because the Authorisation Centre will only be able to perform the same checks as your Terminal and you will also run the risk of receiving two Authorisation numbers for the same Transaction.

Please note: You can verify the CSC on Discover and Diners Club International cards. However, the AVS is not supported on these Cards.

Your customers should now be used to giving the additional information for CNP Transactions. The protection against Card fraud is a benefit to them as well as to you and should be used. These extra security measures shouldn't make any difference to the speed it takes to authorise a Transaction electronically. In fact, Authorisation could be quicker because you will no longer need to make CNP Code 10 phone calls. Plus, the final decision on whether or not to accept a payment is still up to you.

Address Verification Service means the service enabling Retailers (for UK issued Cards) to verify a Cardholder's postcode and the statement address recorded by their Card Issuer.

Accepting Transactions

Authorisation responses

If there are available funds and the Card hasn't been reported lost or stolen, you will receive one of the standard responses shown in the table below.

It is your decision whether or not you wish to progress a CNP Transaction, and this additional information will help you decide. However, as with all CNP Transactions, payment is not guaranteed and you bear the risk if the Transaction is disputed at a later date.

Response	Definition	Preferred actions
Data Matches	This means that both the AVS and CSC match the Card Issuer's records.	As long as you have been given an Authorisation code, and you are satisfied that the Transaction is genuine, then unless there are other suspicious circumstances that concern you, you may decide to go ahead with this sale. However, as with all CNP Transactions, payment is not guaranteed and you bear the risk if the Transaction is disputed at a later date.
Data Non Match	The CSC and/or the address details don't match with the Card Issuer's records.	Your Terminal may decline your Transaction. There is the possibility that this is a fraudulent Transaction. Further enquiries with the Cardholder should be made. It could also be that the member of staff has noted the details incorrectly, so you may want to check your records.
CSC Match Only	Only the CSC matches and either one or both of the address details don't match with the Card Issuer's records.	The address given must match the address recorded by the Card Issuer, so in this case there is a possibility that the Transaction is fraudulent. However, it could also mean that the Cardholder has changed address without notifying the Card Issuer or the Card Issuer doesn't support AVS. Another possibility is that a member of staff may have noted the details incorrectly. In these circumstances it would be advisable to verify the address again with the Cardholder and for you to check your records.
AVS Match Only	Both address and postcode match, or just the postcode in cases where the home address has a house name rather than a number. However, the CSC doesn't match.	Your Terminal may decline your Transaction. There is the possibility that this is a fraudulent Transaction. However, it could be that the Cardholder has given you an incorrect CSC number by mistake. It could also be that a member of staff has noted the number down incorrectly. Therefore, before taking any further action, you may want to verify the CSC again with the Cardholder. You may also want to check your records.
Not Checked	This means that neither the CSC nor the AVS has been checked.	This could be because the Card Issuer doesn't support either of the services, or their system is down. If this happens then you will have to make a decision based on the information you have, as you do now. We would recommend that you make further checks before going ahead with the sale.

Next steps

- If a Transaction has been authorised, but you are not happy to continue, you should process a reversal or refund immediately to reinstate available credit to the Cardholder.
- If the Transaction is referred, the CSC and AVS information may be returned by your Terminal so that you can verify the Transaction with the Authorisation Centre by telephone: CNP Authorisation **01268 278 278**. For more information on referred transactions, please see page 105 (Section 5: Authorisation and referrals).
- If you have multi-currency or dynamic currency conversion facilities please call **01268 662 520**.

Important information

Please read the points detailed below. These points explain a few key things that you should be aware of when processing CNP Transactions.

This information should answer some of the questions you may have about the processes, but if you have further queries, please call the Cardnet Helpline on **01268 567 100**.

1 Guidance only

Please remember the use of CSC checks and AVS is not a guarantee of payment. They are there to help you establish if the Card is present at the time of the Transaction and that you are more likely to be dealing with the genuine Cardholder.

2 Transaction approval criteria

The CSC and AVS checks are in addition to the overall Card status check. The overriding criteria are still the availability of funds and Card status.

3 Declined Transactions

Even if the CSC and AVS data matches, never process a declined Transaction.

4 Delivery address

If you deliver goods to a different address, other than the one checked using the AVS service, you are taking an additional risk.

5 Destroying records

If you keep records of your Transactions in any format other than the Cardnet Mail Order Transaction schedule, you must ensure that you do not keep any records of Cardholders' Card Security Codes. This information must be destroyed once the Transaction has been authorised.

6 Overall responsibility

It is your decision whether or not you wish to progress a CNP Transaction, and this additional information will help you decide. However, please remember that you remain ultimately responsible should a Transaction be confirmed as invalid.

E-commerce

A new application must be made for an E-commerce facility with Cardnet even if you have an existing Cardnet facility for Point of Sale or Mail/Telephone Transactions. When your E-commerce account is approved, you will be issued with a new Cardnet Merchant number. This number must be used for E-commerce Transactions only. This is because E-commerce Transactions must be identified separately from your Point of Sale Transactions.

Your website must contain all of the following information:

- Your full legal entity details that your customers will be transacting with.
- Card Scheme logos in full colour to indicate Card acceptance.
- Complete description of the goods or services offered for sale by you on your website and any return/Refund policy.
- Customer service contact, including electronic mail address or telephone number and international dialling code.
- Your business address and country.
- Transaction currency.
- Export restrictions (if known).
- Delivery policy.
- Consumer data privacy policy.
- Security capabilities and policy for transmission of payment Card details.
- Cookie policy and data protection policy.
- Your purchase terms and conditions made available to the Cardholder during the order process, either:

- on the same screen used as the checkout screen indicating the total Transaction amount; or
- within the sequence of web pages accessed by the Cardholder prior to the final checkout.

Cardholder receipts

Your customers must be supplied with a Transaction receipt (this must be part of an order confirmation notice) at the time of the purchase. Please remember, the receipt must not include the full Card number or the merchant terminal and card acceptor IDs for POS acceptance devices or payment gateways deployed on or after 15 October 2022.

Processing E-commerce Transactions

To process E-commerce Transactions along with your website (with a checkout cart) you will need a Payment Service Provider (PSP) to process your payments. Lloyds Bank Cardnet has its own PSP, Lloyds Bank Online Payments. Cardnet will be able to advise you of relevant costs, set-up times and systems integration requirements with your website.

Should you already use an alternative PSP, please contact us to ensure Cardnet can support this.

Lloyds Bank Online Payments has a fully 'hosted' solution, in simple terms this means having the payment application (Card holder payment page) hosted on the PSP's secure server. If you choose the secure hosted option, responsibility for PCI DSS compliance requirements regarding customer Card data security will be undertaken by Cardnet.

PCI DSS is a set of requirements, endorsed by the Card Schemes (Visa, Mastercard and Discover® Global Network) governing the safekeeping of account information and applies to anyone that stores, processes or transmits Card holder data. To see how PCI DSS affects you as an E-commerce Merchant and what you need to do to validate your compliance with these standards – see Section 7, 'Security, Data security' (p121).

Fraud Screening

As a part of Lloyds Bank Online Payments functionality, we offer E-commerce fraud screening using our dynamic fraud screening tool. With E-commerce, fraudsters look to take advantage of the customer not being present at the moment of Transaction and will use various methods to try and defraud the Merchant. With the Lloyds Bank Online Payments fraud screening tool, a variety of fraud rules are in place to try and ensure that the Card holder is kept safe from these methods and that checks are made so that validation of Card/payment method ownership can be verified. Depending on the sector there are a variety of bespoke checks that can be put in place to ensure we can combat fraud together.

All E-commerce Transactions must be authenticated according to current Card Scheme regulations.

All Maestro E-commerce Transactions must be authenticated with Mastercard Identity Check according to current Card Scheme regulations.

Strong Customer Authentication

How does Strong Customer Authentication work?

From 14th March 2022 cardholders will be required to authenticate themselves for certain electronic transactions using two independent authentication elements (known as two factor authentication). This is known as Strong Customer Authentication (SCA).

This means that a customer will need to authenticate using two of three authentication categories to access their accounts, make payments or complete other high-risk journeys, such as changing their contact details.

The three authentication categories customers could be asked to provide are:

1. something they know (e.g. a password)
2. something they have (e.g. confirming an authorisation code sent to their mobile phone)
3. something they are (e.g. using facial biometric technology).

Certain low-risk transactions can be authorised without requiring SCA. Generally, we will try to process transactions without SCA wherever this is possible. The main exemptions apply to Transactions that are:

1. Subscriptions or recurring transactions (although initial setup will require SCA)
2. Contactless payments for €50 or below
3. Online transactions for €30 or below
4. To a 'trusted beneficiary' nominated by the cardholder and whitelisted by the card issuer

There are also circumstances where we do not have to apply SCA if the transaction poses a low risk of fraud. This relies on analysis of a number of factors, and we will ask you to provide additional fraud-related information on a regular basis in order to help perform this analysis. The final decision as to whether SCA should be applied will be down to the card issuer, but we will introduce an option for you to request this exemption where you believe the fraud risk is low (e.g. because it fits with location information and spending patterns that are typical of your customer).

You will be liable for any transactions processed under an SCA exemption requested by you. This means that these transactions can be charged back to you if disputed by the card issuer or a cardholder.

For more information on SCA contact the Cardnet Helpline on **01268 567 100**. Lines are open 8am-9pm, Monday to Saturday.

How do Visa Secure, Mastercard Identity Check and Diners Club International® and Discover® ProtectBuy work?

Visa Secure, Mastercard Identity Check and Diners Club International® and Discover® ProtectBuy operate on your website and interact with both the Cardholder and their Card Issuer.

The Cardholder signs up for these extra security features with their Card Issuer.

When shopping online:

- 1 The Card holder selects their chosen goods and proceeds to the payment page.
- 2 The Card holder enters their Card number. If they are registered for Visa Secure, Mastercard Identity Check or Diners Club International ProtectBuy, a pop-up or in line screen from their Card Issuer appears asking for their password (or random characters as set out by their Card Issuer's authentication requirements).
- 3 The Card Issuer verifies the password.
- 4 The Transaction is completed giving both the Merchant and the Card holder the confidence that the identity of each has been verified.

Please note: Some UK Card Issuers will assess each Transaction and verify them automatically. Instead of being asked to input a password or random set of characters, Cardholders will receive a message in a pop-up or in line screen to confirm that the Transaction is being processed.

These services also benefit Merchants. By deploying Visa Secure, Mastercard Identity Check and Diners Club International® and Discover® ProtectBuy you will be protected from most Disputes where the Card holder subsequently denies engaging in or authorising the original Transaction.



For more information on Visa Secure, Mastercard Identity Check and Diners Club International® and Discover® ProtectBuy, contact the Cardnet Helpline on **01268 567 100**. Lines are open 8am-9pm, Monday to Saturday.

American Express have their own security scheme.

For further details, please check their website:

www.americanexpress.com/uk/security/safekey/

Alternatively, for Merchant and consumer advice, frequently asked questions (FAQs) and online demonstrations on how these solutions work, visit:

www.visaeurope.com (Businesses and Retailers)

www.mastercard.com/global/merchants/identity-check.html

www.dinersclubinternationalprotectbuy.com

www.discovernetwork.com/en-intl/business-resources/fraud-security/products-tools/protect-buy

www.financialfraudaction.org.uk

Transaction terminology

It is important to understand the terminology for processing Transactions so that you use the appropriate Transaction type for your orders and returns.

- **Sale** – this is the most common Transaction type which immediately charges a customer’s Card or bank account.
- **Authorise Only** – reserves funds on a customer’s credit Card. Authorise only does not charge the Card until you perform a Completion (Ticket Only) Transaction and/or confirm shipment of the order (using an option available in Reports). Note that Authorisation reserves funds for varying periods, depending on the issuing Card company’s policy. We strongly suggest that you confirm shipment as soon as possible after Authorisation.
- **Completion (Ticket Only)** – a Post-Authorisation Transaction. Captures the funds from an Authorise Only Transaction, reserving funds on the customer’s Card for the amount specified. Funds are transferred when your batch of Transactions is settled. If you enter a larger total in the Post-Authorisation Transaction than was specified for the Authorise Only Transaction, the Post-Authorisation Transaction may be declined. If you enter a smaller amount than was authorised, an adjustment is made to the Authorisation to reserve only the smaller amount of funds on the customer’s Card for the Transaction.
- **Forced Ticket** – a forced Post-Authorisation. This Transaction type is used in a similar way to a Completion Transaction, except it is specifically for Authorisations you obtained over the phone. It requires a reference number (or approval code) that you should have received when you carried out the phone Authorisation.
- **Return** – returns funds to a customer’s Card against an existing order on Lloyds Bank Online Payments. To perform a return, you need the order number (which you can find in your Reports). If you perform a Return of the full order amount, the order will appear in your Reports with a Transaction amount of 0.00. To perform a Return Transaction, use the Return page.
- **Credit** – returns funds to a customer’s Card for orders from outside Lloyds Bank Online Payments. Use the Credit page to perform a Credit Transaction. Credit Transactions are marked as Returns in your Reports.
- **Void** – Transactions can be voided before the batch of Transactions is settled.

No funds are transferred during any of these Transactions. Funds are transferred only after your batch of Transactions is settled (this is set up to occur automatically once a day).

Using your web browser as a virtual Point of Sale machine

The Virtual Terminal is the main page you will use for all your Sale and Authorise Only as well as Forced Ticket Transactions.

Since some of the other types of Card Transactions (Completion and Return) need to look in the database to get order information, they have their own pages. Credit is a special Transaction that not all users have access to, so it also has its own page.

A hide/reveal function is available for all sections of the page, which can expand to provide additional options or fields -such items are identified by a right-arrow graphic. When clicked upon, the arrow changes to point downward and the expanded choices are revealed. Clicking again reverses the process.

Processing Sale Transactions

To do a Sale Transaction, you will need to complete all the required fields from the following sections. Then, fill in additional fields as appropriate for your Transaction.

- 1 Follow these steps to perform a Sale Transaction.
- 2 If using the product catalogue feature, select items from the Product Catalogue.
- 3 Enter Order Information.
- 4 Select Credit Card as the Payment Method.
- 5 Enter Credit Card Information, select Transaction Type Sale.

- 6 If needed, enter further optional fields.
- 7 Click on the Continue button.
- 8 If there are data entry errors or any required fields are missing, the same page will reappear with an error message at the top, and all incorrect/missing fields flagged with a warning graphic. Make any necessary corrections, then click the Continue button again. Once your page is error free, a Please Confirm page will appear.
- 9 Review the data, make corrections if needed by clicking on the Back button, then click the Submit button. A Transaction Result page will appear.
- 10 Review the Results.

Selecting products from your product catalogue

The Cardnet Virtual Terminal offers you the timesaving ability to choose items from your product catalogue every time you process an order. To enable this feature, you first need to enter your product catalogue using the 'Manage your Product Catalogue' function in the Customisation section. For every product you have entered, you can click on 'Edit' to add options (e.g. colour, size etc.). Once you've done that, simply go to the Virtual Terminal page and click on the Select Products button to select products for this order. The Product Catalogue page will appear.

Adding products to the order

The top half of the page is the Product Summary table, which lists all the products in your product catalogue. To add products to the order in progress, simply enter the desired quantity of a particular product in the Qty (quantity) column. If there are any options for this product, they will appear in the Options column of this table. Select the appropriate choices by choosing one of the choices available in the dropdown box (e.g. colour: red, size: 5), then click on the 'Add Item(s)' button below the table.

The correct quantity, choices, product description, price, and total should appear in the Selected Products table on the bottom half of the page.

Removing products from the order

If you have made an error in entering any of the product quantities or options, you can delete the product(s) from the order very easily by checking the checkbox for that line item in the Selected Products table, then clicking on the 'Delete Item(s)' button located just below the table. To delete all the products in the order, click on the checkbox at the top left corner of the Selected Products table (this selects all the items in the order), then click on the 'Delete Item(s)' button.

Completing the order process

Once you've completed your product selections, click on the 'POS Main' button to return to the Virtual Terminal page, where you can enter payment and contact information for this order. A table should appear at the top of the page showing all the products selected for this order along with the subtotal of the order.

Product Catalogue

Products Summary

Qty	Item Id	Description	Options	Unit Cost
0	glasses	sun glasses		79.99 GBP
0	hat	hat		5.70 GBP
0	shirt	shirt		9.50 GBP
0	shoes	shoes		10.00 GBP

Add Item(s)

Selected Products

<input type="checkbox"/>	#	Qty	Item Id	Description	Options	Unit Cost	Extended Cost
							Subtotal:
							Delete Item(s)
							POS Main

Virtual Terminal: Products selected from Product Catalogue

If any of the product selections should change before you've submitted the order, you can return to change your product selections by clicking on the 'Select Products' button again.

Order information

The Order Information section has only one required field: the total amount of the order (including all taxes and shipping). Other fields in the section are optional and can be used at your discretion.

You must fill out all required fields. To enter Order Information, follow the steps below.

Order number (optional)

For regular credit Card Transactions, this field is optional. If you wish to assign an order number to this order, enter one in the text box provided.

Each order number must be unique, so if you are going to use this field on a regular basis, you should adopt an order number generation procedure. If you choose not to assign an order number, Lloyds Bank Online Payments system will automatically generate one for you.

Purchase order number (optional)

If there is a purchase order number associated with this order, enter it here. Because you may have several Transactions against the same purchase order, you may use the same purchase order number for several Transactions, if needed. For regular credit Card Transactions, this field is optional.

Shipping amount (optional)

If there are shipping charges associated with this order and if you wish to track your shipping charges, enter a real or integer number equalling the charge for shipping this order.

VAT (if applicable)

There may be cases where you are doing international business where you need to charge a Value Added Tax (VAT), either in addition to or in lieu of the regular sales tax. If the VAT applies to your order and if you need to charge the customer the VAT now, enter the amount of the VAT in the VAT field. In some cases, you may not need to charge the VAT; it will be taken care of when the goods are imported.

Total amount (required)

As you enter Subtotal, Tax, and VAT, the Virtual Terminal will automatically calculate the total amount for you. If you need to, you can replace this value with any real or integer number representing the total amount of the Transaction. The total amount should include tax, VAT (if applicable), and shipping charges, and should reflect the sum of all charges for this Transaction. The total amount should always equal the sum of the product subtotal, tax, shipping, and VAT. This is a required field for ALL Transactions.

Currency (required)

If you want to use another currency for this Transaction then the displayed default currency, you can change it using the drop-down box.

Enter payment data for Card Transactions

The Payment Details section shows fields required for a Card Sale, Authorise Only, or Forced Ticket Transaction.

A graphic for each Card type that has been setup for your store is shown.

The screenshot shows a form titled "Card" with a sub-label "Credit/Debit Card". The form contains the following fields:

- Select card type: A dropdown menu.
- Supported Card Types: A row of logos for VISA, Mastercard, American Express, and Discover.
- Transaction Origin: A dropdown menu with "Mail Order/Telephone Order" selected.
- Transaction Type: A dropdown menu with "Sale" selected.
- Card number: A text input field.
- Expiry date: Two dropdown menus for the month and year, with "01" and "2020" selected respectively.
- Card Security Code: A text input field.

Virtual Terminal: Card data input fields

To enter Card information, follow the steps below:

Step 1: select the Card type

First, select the Card type from the 'Select Card type' dropdown box or click on one of the brand logos.

Step 2: enter the Transaction Origin

Select the Transaction origin from the 'Transaction Origin' dropdown box.

- Select Retail (face to face) if the customer and the Card are in your presence.
- Select Electronic Commerce (internet) if the order came to you over the Internet or via email.
- If you received the order over the phone or through the mail, select Mail/Telephone Transactions.

Transaction Origin is always a required field; you must make a selection.

Step 3: enter the Transaction type

Once you've selected the Transaction origin, select the appropriate Transaction type for your credit Card Transaction in the Transaction Type dropdown box.

- Select Sale to charge the customer's Card immediately (upon batch settlement).
- Authorise Only to reserve funds on the customer's Card, but not complete the Transaction yet.
- Forced Ticket to complete a voice Authorisation Transaction.

If you need to do any other type of Transaction, you'll need to visit another page. To complete an Authorise Only Transaction,

go to the Completion page. To do a return, go to the Return or the Credits page.

Transaction Type is always a required field, but if you do not make a selection, it defaults to Sale.

Step 4: enter the Card number or swipe the Card

Enter the Card number in the Card Number field. You may include spaces or dashes if you wish.

If the Card is present and you have the appropriate reader (configured correctly), place your cursor in the Card Number field, and then swipe the Card through the reader. The Card Number field should be automatically filled in for you. If it is, there is no need to enter any other data.

All other required fields (except Transaction origin and Transaction type) become optional because the entire customer's data is passed to us from this one entry.

If something should go wrong and this field does not fill in when you swipe the Card, check your reader to make sure it's configured correctly. If the reader is configured correctly and you are still unable to swipe the Card, the Card may be unreadable. Go to the previous field (Are you swiping the Card?), uncheck the Yes checkbox, and enter the Card data manually.

Step 5: enter the expiry date

Select the Card's Expiry Date from the dropdown boxes. Select the month first, then the year that the Card expires.

Step 6: enter the Card Security Code

The Card Security Code is a 3 or 4-digit number usually found on the back of the customer's credit Card or the four digits on the front of an Amex card, on the same line as the customer's signature, following the last four digits of the credit Card number. There are many different names for this code: Visa calls this code CVV2, Mastercard calls it CVC2, American Express 4DBC.

Step 7: enter the reference number (required only for forced ticket Transactions)

If you are performing a Forced Ticket Transaction, enter the reference number associated with this Transaction (typically given to you over the phone with the Authorisation) in the Reference Number box. The Reference Number field will not appear unless you have chosen Forced Ticket as the Transaction type.

Step 8: continue to the customer contact information section

Click on Customer Contact Information to expand the text, and then enter the appropriate fields. The Customer ID is a unique identification number you can choose for the customer.

Shipping

The entire Shipping section is optional by default. You do not have to enter any shipping information to perform a Transaction.

If the shipping address is the same as the billing address, checking the Yes checkbox will cause the corresponding fields from the billing information to be copied into the shipping section, saving you time and reducing the risk of error. If the addresses are different, then enter the shipping address in the fields below.

If desired, enter the type of shipping you will use for this order. Up to 36 alphanumeric characters are allowed in this field. Examples are Federal Express, UPS, etc.

Recurring payments

This section allows you to make a credit Card (Sale) Transaction recurring. To make a Transaction recurring, click on the Make recurring? Yes checkbox.

Next enter how often you wish to charge the customer. In the Bill the customer fields, enter a number from 1 to 999 with no decimal point and select day, week, month, or year in the dropdown box. For example, if you wish to charge the customer once a year, enter the number 1 and select "year" in the dropdown box. To charge the customer twice a year (once every 6 months), you would enter the number 6 and select "month" in the dropdown box.

Select the month / day / year to start charging the customer in the Start on dropdown boxes.

Enter the number of times to charge the customer in the End After textbox.

► Make Recurring (For Credit Card Sale Transactions ONLY)

Make Recurring?:	<input type="checkbox"/> Yes
Bill The Customer:	every <input type="text"/> Select one... ▾
Start On (DD/MM/YYYY):	17/01/2022 <input type="text"/>
End After:	<input type="text"/> payments

Virtual Terminal: Recurring Payments input fields

Please see Reports section of this document for details about how to modify or cancel Recurring Payments.

Comments

The expandable Comments section is not required by default. There is only one field in the Comments section: Comments. It is intended to let you enter optional notes about the Transaction.

Comments are visible in your Reports, so they can help you with your Transaction management if you use them effectively.

Complete the Transaction

Two final options remain: Clear Form, which is self-explanatory, and Continue, which when clicked, takes you to the next screen. When you click the Continue button, all your entries are validated. If pieces of information are missing or incorrect, the Cardnet Virtual Terminal page will reappear with an error message at the top and the incorrect or missing fields flagged with an error graphic. If this should occur, make the appropriate corrections to the fields, then click the Continue button again.

If there are no apparent invalid entries, a review of all the information you entered with a request for confirmation will appear. Review the information and, if necessary, click on Back and make any corrections. Otherwise, click on Submit.

The Transaction Result screen will appear. The result screen will contain all the information you entered, plus an extra section at the top called Transaction Information.

For retail Merchants who need a receipt for the customer to sign, there is a print receipt function. Simply click on the Show Receipt button at the bottom of the Transaction Result page. A new browser window will open with a Transaction receipt. Click on the Print Receipt button at the bottom of the Receipt page to print the receipt. Once you have printed all the receipts you need, close the receipt window by clicking on the Close button at the bottom or on the X in the top right hand corner of the Receipt window.

The Transaction Information section is where you will see whether the Transaction was approved or declined. If the Transaction was approved, the Transaction Status line will say Approved. The Date and time of Transaction, a Transaction reference number, an Approval Code, and a Reference number will follow.

A typical Approval Code for a successful Transaction contains four alphabetic characters in the middle of the code, e.g. PPXM. The first three letters indicate Address Verification Service results:

Value	Meaning
PPX	No address data provided or not checked by the Card Issuer
YYY	Card Issuer confirmed that street and postcode match with their records
YNA	Card Issuer confirmed that street matches with their records but postcode does not match
NYZ	Card Issuer confirmed that postcode matches with their records but street does not match
NNN	Both street and postcode do not match with the Card Issuer's records
YPX	Card Issuer confirmed that street matches with their records. The Issuer did not check the postcode.
PYX	Card Issuer confirmed that postcode matches with their records. The Issuer did not check the street.

The last alphabetic character in the middle is a code indicating whether the Card Security Code matched the Card Issuer's code. An "M" indicates that the code matched. See further details in the Card Security Code section.

If the Transaction was declined, a reason for the decline will show on the Approval Code line.

Processing subsequent Transactions

Ticket only (post auth)

After you run an Authorise Only Transaction, you need to complete it. Running an Authorise Only Transaction tells you whether the customer has sufficient funds on the Card for your order, but it may or may not reserve any funds for you. To reserve the funds, you must either mark the order as "shipped" (via your Reports) or perform a Ticket Only Transaction. A Ticket Only Transaction is sometimes referred to as a Post-Authorisation.

- 1 To perform a Ticket Only Transaction, go to the Completion page.
- 2 The first Completion page simply asks for the order number. This is the order number associated with your Authorise Only Transaction. (If you don't know your order number, you can find it in your Reports.) Enter the order number then click on the Retrieve Order button.
- 3 A new page will appear with several pre-filled input fields related to the order. Review these fields to ensure you have selected the correct order. (You may have to expand some of the sections at the bottom of the page to see all the fields you need to see.) If this isn't the right order, click on the Back button on your browser and enter the correct order number to retrieve. If it is the right order, make any changes you need to make to the input fields, then click on the Continue button.

- 4 Once you click the Continue button, if all entries in the form were valid, another page will appear asking you to confirm the information. If everything is okay, click on the Submit button; otherwise, click on the Back button to make the appropriate changes. (If any fields are missing or incorrect, the Completion page will reappear with an error message at the top and the incorrect/missing fields flagged with a warning graphic. Make the appropriate changes then click the Continue button again. A Please Confirm page should appear.
- 5 Review the information, then click the Submit button. A final Transaction Results page will appear, indicating whether the Transaction was approved or declined and reiterating all the Transaction information.

Forced ticket Transactions

Use a Forced Ticket Transaction to complete the Sale for an Authorisation you received over the phone.

To process a Forced Ticket Transaction, go to the Cardnet Virtual Terminal page. This is the same page you use to process credit Card Sale, or Authorise Only Transactions.

To do a Forced Ticket Transaction, complete all the required fields from the following sections. Then fill in additional fields as appropriate for your Transaction. Follow these steps to perform the Transaction:

- 1 If using the product catalogue feature, select items from the Product Catalogue.
- 2 Enter Order Information.
- 3 Select Credit Card as the Payment Method.
- 4 Enter Credit Card Information, select Transaction Type Forced Ticket: a Reference number field will appear. Enter the reference number (the Authorisation code you received over the phone).
- 5 Fill out Customer Contact Information.
- 6 Enter the Shipping Address (optional).
- 7 If in test mode, select the Desired Response.
- 8 Enter Comments (optional).
- 9 Click on the Continue button.
- 10 If there are data entry errors or any required fields are missing, the same page will reappear with an error message at the top, and all incorrect/missing fields flagged with a warning graphic. Make any necessary corrections, then click the Continue button again. Once your page is error free, a Please Confirm page will appear.
- 11 Review the data, make corrections if needed by clicking the Back button, then click the Submit button. A Transaction Result page will appear.
- 12 Review the Results.

Processing returns

Should a customer return something associated with an order, you can credit their account for the amount of the return using a Return Transaction.

- 1 To do a Return, first go to the Return page. A page will appear, with a field for the order number. If you don't know your order number, you can find it in your Reports.
- 2 Once you've located the order number, enter it in the input box, then click on the Retrieve Order button. A page will appear showing all the existing information from that order.
- 3 Review these fields to ensure you have selected the correct order. (You may have to expand some of the sections at the bottom of the page to see all the fields you need to see.) If this isn't the right order, click on your browser's Back button to return to the previous page and retrieve an alternate order.
- 4 If this is the correct order, enter the amount to return in the appropriate fields. By default, the fields will be pre-filled with the total amount available to be returned. If your return amount is less than the order total, make corrections as appropriate.
- 5 Once you've finished with the Order fields, change any other fields related to Customer Contact Information, Payment Information, or Comments, then click the Continue button.
- 6 Once you click the Continue button, if all entries in the form were valid, another page will appear asking you to confirm the information.
- 7 If everything is okay, click on the Submit button; otherwise, click on the Back button to make the appropriate changes. (If any fields are missing or incorrect, the Return page will reappear with an error message at the top and the incorrect/missing fields flagged with an error graphic. Make the appropriate changes then click the Continue button again. A confirmation page should appear. Review the information, then click the Submit button.
- 8 A final Transaction Results page will appear, indicating whether the Transaction was approved or declined and reiterating all the Transaction information. As you enter values in the Return subtotal, Return Tax or VAT, and Return Shipping Amount fields, the Total amount to Return field will automatically change to the sum of the three fields. You are allowed to change the total, but the sum of the subtotal, tax and shipping amount must equal the Total amount; if it doesn't, you will get an error when you click the Continue button.

Crediting a customer's account

Sometimes you need to credit a customer's account for an order that occurred outside Lloyds Bank Online Payments. Because there is some inherent risk of fraud with a credit, not every Merchant has permission to perform credit Transactions. If you do not see the credit function listed in the Side Menu Box of your Virtual Terminal section, you do not currently have permission to perform a credit. Contact your processor's Merchant services department to enable the function if you need it and do not have it.

Processing Transactions

If you indeed need to do a credit against an order received elsewhere, click on Credit to bring up the Credit page with several entry fields. Fill the appropriate and required fields for your credit, then click on the Continue button.

Once you click the Continue button, if all entries in the form were valid, another page will appear asking you to confirm the information. If everything is okay, click on the Submit button; otherwise, click on the Back button to make the appropriate changes. If any fields are missing or incorrect, the Credit page will reappear with an error message at the top and the incorrect/missing fields flagged with a warning graphic. Make the appropriate changes then click the Continue button again. A confirmation page should appear. Review the information, then click the Submit button. A final Transaction Results page will appear, indicating whether the Transaction was approved or declined and reiterating all the Transaction information.

Voiding orders

If an order has not yet been settled, you have the capability to void the order. The process for voiding orders is as follows:

- 1 Click on the Reports button on the Main Menu Bar.
- 2 If you wish to void credit Card orders, click on the View Credit Card Batches link in the Side Menu Box.
- 3 Specify Time Period – Select any of the named time periods or enter a specific range of dates.
- 4 Click on the Submit Query button. The batch report will appear.
- 5 Click on the words Current Batch to bring up the Current Batch report.

- 6 Select the orders you wish to void by clicking on the corresponding checkboxes in the left-most column.
- 7 Click on the Void Selected Orders button at the bottom of the page.
- 8 A page showing the results will appear. Each order you chose to void should show on the list.

You can only void orders which have not yet settled. If you should notice any orders in the Current Batch list with a Transaction approval code of YTEST, we recommend you void them before your batch is submitted for processing.

Use Reports to view your store's Transactions from several different perspectives and to perform some administrative tasks.

To view the reports, click on the Reports button on the Main Menu Bar. The Reports Main Menu for your store is displayed in the Side Menu Box and in the main content portion of the screen. The reports available are listed below.

- Dashboard – shows information on Card sales made including a table with the last 6 months Transactions.
- Transaction Charts – shows Transactions in bar, pie, or line charts.
- Orders – shows all successful orders by specific time period, by credit Card number and time, by order number, or by user ID and time. You also have the option to show only unshipped orders.
- Transactions – shows all Transactions by time period, by credit Card number and time, order number, User ID and time or by Transaction type and time.
- Transactions Summary – shows a summary of approved and declined Auth and Sale Transactions and a summary of approved Auth and Sale Transactions by Card type.
- Credit Card Batches Report – lets you view credit Card batches processed during a specified time period.
- Active Periodic Bills – shows information about Recurring Transactions and allows you to modify them.

Credit Card numbers

As a security feature, only the first four and last four digits of credit Card numbers are displayed in the reports. These Credit Card Identification (CCID) numbers are often active links that can be selected to display information about all Transactions involving the selected Card number.

Downloading report data

To download the data from any of the reports for use with your own accounting tool, follow the steps below:

- 1 Bring up the report which contains the data you wish to download.
- 2 Locate the Export All Data button located at the bottom of the page.
- 3 Select your desired format from the dropdown list. Choose either CSV (Comma delimited) or XML format. CSV lists are suitable for importing into most common spreadsheets or databases. XML format is helpful for applications that allow you to import XML.
- 4 Click on the Export All Data button to download the data. Depending on your browser, a File Download dialogue box will most likely appear, asking what you would like to do to the file (Open, Save, or Cancel). If you choose Open, the file will open in the application that is assigned to that type of file. Choosing Save will ask you to choose a location where you wish to save the file.

Regardless of the number of pages in the report, all report data will be included in the downloaded file.

Viewing the dashboard

To view the Dashboard click on the Reports button in the Main Menu Bar then click on Dashboard.

The Dashboard offers a graph showing the past weeks Processed Sales Volumes, a chart showing the past 3 months of Transactions by status (approved versus declined) and a Transaction overview table offering details of the last 6 months Transactions.

The Transaction overview table can be sorted by clicking on any of the headers and there is a search option to search for a specific Transaction if required.

The details of each Transaction can be viewed by clicking on the Transaction's Order reference. A new window will then provide you with the Order Detail Report. Please see the Order Detail Report for what can be viewed and managed from this report.

There is also an option to select to 'Make the Dashboard your VT start page'.

Viewing Transaction charts

Lloyds Bank Online Payments offers four graphical chart types, which are helpful for visualising orders and sales, and for when you need charts for a presentation. To view your orders in chart format, follow the steps below.

- 1 Click on the Reports button in the Main Menu Bar.
- 2 Click on the Transaction Charts link in the Side Menu Box or the main content area. The View Transaction Charts screen appears.

- 3 Select Chart Type: select an option. You can view your Transactions in a bar chart, a pie chart, a line chart, or you can view a bar chart summary report.
- 4 Select Transaction Types: select any of the listed Transaction types or click on the All checkbox in the separator bar if you would like to view all the Transaction types.
- 5 Specify Time Period: select any of the named time periods or enter a specific range of dates you wish to view.
- 6 Select Hierarchy: choose whether you wish to view all stores below you in the hierarchy or a subset by choosing an option in the dropdown menu. (This option only appears if you are logged in as a multi-store administrator.)
- 7 Click on the Submit button to view the report. If you want to re-enter the information, click on the Reset button to clear the information.

Chart types

Depending on which type of chart you chose, the chart which appears will look different.

The chart types available are listed below:

- Detailed bar chart
The Detailed Bar Chart report shows the Transaction totals by type in a bar chart format. Each Transaction type is shown in a different colour. For each month in the specified timeframe, there is a row of coloured bars showing Transaction totals for that month. At the bottom of the chart, a table shows summary statistics for each type of Transaction. Hold your mouse over any coloured bar to see the total exact amount

of Transactions of that type. Clicking on the bar will bring up a detailed Transactions Processed report for that Transaction type. (For more information on viewing detailed Transaction reports, see [Viewing Transactions](#).) Click on the coloured boxes in the legend on the right to see individual bar chart reports for the selected Transaction type. Right click on any of the charts to save that chart as a graphic in jpeg format. You can then import the graphic into your presentations or documents as needed.

- **Summary bar chart**

The Summary Bar Chart report shows the Transaction totals by type in a bar chart format. Each Transaction type is shown in a different colour. Each coloured bar represents the total amount of all Transactions of that type over the entire timeframe specified. At the bottom of the chart, a table shows summary statistics for each type of Transaction. Hold your mouse over any coloured bar to see the total exact amount of Transactions of that type. Clicking on a coloured bar will bring up a detailed Transactions Processed report for that Transaction type. (For more information on viewing detailed Transaction reports, see [Viewing Transactions](#).) Right click on any of the charts to save that chart as a graphic in jpeg format. You can then import the graphic into your presentations or documents as needed.

- **Pie chart**

The Pie Chart report shows the Transaction totals by type in a pie chart format. Each Transaction type is shown in a different colour. At the bottom of the chart, a table shows summary statistics for each type of Transaction. Hold your

mouse over any coloured pie piece to see the total exact currency amount of Transactions of that type. Clicking on a pie piece will bring up a detailed Transactions Processed report for that Transaction type. Right click on any of the charts to save that chart as a graphic in jpeg format. You can then import the graphic into your presentations or documents as needed.

- **Line chart**

The Line Chart report shows the Transaction totals by type in a line chart format. Each Transaction type is shown in a different colour. Each coloured line represents the total amount of all Transactions of that type. At the bottom of the chart, a table shows summary statistics for each type of Transaction. Click on any of the legend boxes to see a line chart for that Transaction type alone. Right click on any of the charts to save that chart as a graphic in jpeg format. You can then import the graphic into your presentations or documents as needed.

View orders report

To view your orders, you need to use the Orders Received report. Generate an orders report by following the steps below.

- 1 Click on the Reports button in the Main Menu Bar.
- 2 Click on the Orders link in the Side Menu Box or the main content area. The View Orders screen appears.

Reports

- 3 Display Orders: select an option. You can view orders sorted by time period, by credit Card number and time, by User ID and time, or by order number.
 - 4 Specify Time Period: select any of the named time periods or enter a specific range of dates you wish to view.
 - 5 Options: click on a box if you want the report to show only unshipped orders or to show only approved orders. By default, the Only Show Unshipped Orders box is unchecked and the Only Show Approved Orders box is checked, so the report will show approved orders only (both shipped and unshipped). If the Only Show Unshipped Orders box is checked, the report will show all unshipped orders. If both boxes are unchecked, the report will display all orders (both shipped and unshipped), including declined and Recurring Transactions with future start dates. If both boxes are checked, the report will show only all approved, unshipped orders.
 - 6 Display Preference: this option allows you to choose how many orders will appear on each page of the report. Choose a number from the dropdown list.
 - 7 Select Hierarchy: choose whether you wish to view all stores below you in the hierarchy or a subset by choosing an option in the dropdown menu. (This option only appears if you are logged in as a multi-store administrator.)
 - 8 Click on the Submit Query button to view the report. If you want to re-enter the information, click on the Reset button to clear the information.
- The **Orders Received** report shows the following information about each order.
- Select – click on the associated Select checkbox to select one or more orders.
 - Shipped – shows Y if the order has been shipped, or N if the order has not yet been marked as shipped.
 - Retail – shows Y if the order was a retail order, or N if the order was not retail.
 - Order # – the number associated with this order. Click on the order number to view order details.
 - User ID – if there is a user ID number associated with the order, it will be listed in this column. The number is also a link to view all the orders placed by a particular customer.
 - Date – the date that the order was placed. Shows the most recent order first. The time period you selected for the report will be shown under the report title.
 - Name – the name of the person who placed the order. Click on the name to send email to this customer.
 - Amount – shows the amount and currency of the order. The total amount of the orders listed on the page and the total amount of all orders in this report is also shown at the bottom of the page, along with the total tax and shipping charges collected.

Confirming shipment, crediting orders, or rejecting orders

You can confirm shipment, credit the entire amount of the order(s), or reject order(s) by IP address or credit Card number. To perform any of these three tasks, follow the steps below:

- 1 First select order(s) by clicking on the associated checkbox(es) in the left-most column.
- 2 Click on the Work with Selected Orders button. The Selected Order Menu screen appears.
- 3 Select an action by clicking on the appropriate radio button. If you select Reject Order, you must also check on a checkbox to choose whether you wish to reject this order by IP address or by credit Card number. When you reject an order by IP address, all future orders from this IP address will be declined. When you reject an order by credit Card number, all future orders using this credit Card number will be declined.
- 4 Click on the Submit Query button to complete the task. A screen listing the results will appear.

If you choose to reject an order by IP address or credit Card number, you will find yourself at the Fraud Settings page, which will show you all the IP addresses and credit Card numbers you have currently blocked from purchasing at your store. The IP addresses or credit Card numbers from the order(s) you just blocked should appear on this list. To block more Transactions or to unblock any IP address or credit Card number, click on one of the links located towards the top of this screen, just under the title Your Fraud Settings. For more information on changing your fraud protection settings, see Preventing Fraud.

Viewing details

View the details of any order by clicking on the associated Order #. Details will be shown in the Order Detail Report.

View all orders placed by a specific customer by clicking on the User ID link. This column will only be filled in if you have entered a unique Customer ID Number for each customer when entering orders.

If there are more orders in the report than will fit on the current page (according to the number of orders you've chosen to show on each page), a set of numbers will appear at the bottom of the page, reflecting page numbers for the report. The current page number will be larger than the others and will not be underlined. To view any page, click on the associated underlined page number.

Order detail report

To view this report, click on the Reports button on the Main Menu Bar, then click on the Orders link in the Left Menu Box.

Select the appropriate parameters for your query, then click the Submit Query button.

Once the Orders Report appears, you can view an order's detailed report by clicking on the associated Order # link.

The Order Detail Report allows you to:

- View the details associated with that order.
- Email the customer by clicking on the Name or Email link.
- Do a return against this order.

- View all the orders associated with the credit Card number by clicking on the Card Number link.

The Order Detail report has several sections which show the following information:

- The Order ID Number and Order Date/Time are shown at the top of the report.
 - Billing Address section – gives the User ID, shipping status, and the customer’s company, name and address. If the customer’s name and email address were supplied, you can click on the customer’s name to send an email to the customer.
 - Shipping Address section – shows the name, address to which the order was shipped.
 - Contact Information section – shows the customer’s telephone number, email address, fax number and IP address. If an email address was supplied, you can click on the customer’s email address to send an email to the customer.
 - The next part of the report includes subtotal, shipping, tax, return (if applicable) and total amounts.
 - The last portion of the report is a Transaction history which shows all Transactions related to this order (including authorisations, sales, returns, tickets, etc.) The summary information shown here includes date, user ID, type of Transaction, the Card number, the expiration date, approval code, the amount of the Transaction, and comments.
- The Return Order button at the bottom of the report allows you to do a return against this order. Enter the amount to refund to the customer in the box next to the Return Order button at the bottom of the page. The amount you enter must be equal to the total amount of the order. To process the return, click on the Return Order button. To return to the Reports Main Menu, click on the Reports Main button on the bottom of this report.

Viewing Transactions

To view all your Transactions, use the Transactions Processed report. Follow the steps outlined below to see this report.

- 1 Click on the Reports button on the Main Menu Bar.
- 2 Click on View Transactions in the Side Menu Box or the main content area.
- 3 Display Transactions – select an option. You can view Transactions sorted by time period, by credit Card number and time, by User ID and time, by Transaction type and time, or by order number.
- 4 Specify Time Period – select any of the named time periods or enter a specific range of dates you wish to view.
- 5 Select Hierarchy: choose whether you wish to view all stores below you in the hierarchy or a subset by choosing an option in the dropdown menu. (This option only appears if you are logged in as a multi-store administrator.)
- 6 Submit Query – click to view the report.

To re-enter the information, click on the Reset button to clear the information.

The Transactions Processed report shows the following information about each Transaction. The time period you selected for the report will be shown just under the report title.

- Order number – shows the number associated with each order.
- Date – shows the date and time of each Transaction, from the most recent order to the oldest order.
- User ID – if there is a user ID number associated with the order, it will be listed in this column. The number is also a link to view all the orders placed by a particular customer.
- Type – shows the type of Transaction.
- PayerAuth – shows details about authentication (3D Secure/ giropay).
- Invoice Number # – shows the Invoice ID that has been assigned when entering the Transaction.
- Card/Account Number – shows a link to view all Transactions processed with that Card or account number.
- Exp. Date – lists the expiry date of the Card.
- Approval – shows the approval code of the Transaction. If a specific Transaction was declined, the reason it was declined is shown here.
- Amount – shows the amount and currency of the Transaction.

Viewing details

View the details of any order by clicking on the associated Order #.

View a list of all the numbers associated with any credit Card number or routing number by clicking on the associated Card/Route Number.

View all orders placed by a specific customer by clicking on the User ID link. This column will only be filled in if you have entered a unique Customer ID Number for each customer when entering orders.

Viewing the Rest of the Data

If there are more Transactions than will fit on the current page (according to the number of Transactions you've chosen to show on each page), a set of numbers will appear at the bottom of the page, reflecting page numbers for the report. The current page number will be larger than the others and will not be underlined. To view any page, click on the associated underlined page number.

Transactions summary report

To view this report, click on the Reports button on the Main Menu Bar, then click on Transactions Summary in the Side Menu Box.

Choose from the following options to view your report:

- 1 Display Transactions Summary – select options. You can enter a specific User ID or select specific Transaction types and/or Card types to include in the report.
- 2 Specify Time Period – select any of the named time periods or enter a specific range of dates you wish to view.
- 3 Display Preference – choose the number of things you wish to display on one page by clicking on the dropdown box and selecting the number desired. The default is 25.
- 4 Select Hierarchy: choose whether you wish to view all stores below you in the hierarchy or a subset by choosing an option in the dropdown menu. (This option only appears if you are logged in as a multi-store administrator.)
- 5 Submit Query – click to view the report.

If you want to re-enter the information, click on the Reset button to clear the information.

Authorisation Summary Table

The first table that appears in the Transactions Summary report shows the following summary information for each selected Transaction type over the time period specified.

- Approved – shows the total number of approved Transactions of that type and the total amount for all approved Transactions of that type.

- Declined – shows the total number of declined Transactions of that type and the total amount for all declined Transactions of that type.
- Total – shows the total number of Transactions of that type and the total amount for all Transactions of that type.

The totals for each column are listed at the bottom of the table.

Approved Summary Table

The second table that appears in the Transactions Summary report shows the following summary information for each selected payment type over the time period specified.

- # – shows the total number of approved Transactions for that payment type.
- Amount – shows the total amount for approved Transactions of that payment type.
- Total – shows the total number of Transactions of that type and the total amount for all Transactions of that type.

The totals for each column are listed at the bottom of the table.

Transaction notifications by email

Lloyds Bank Online Payments can automatically send out confirmations for each payment Transaction by email. These notifications can be sent to you as well as to your customer.

- 1 To activate this feature, click on the **Administration** link on the Main Menu, then click on **Set options for Transaction notifications via email** and select **Enable Notifications**.
- 2 **Address settings** – enter your email address that shall receive notifications and the one that shall be used as sender address for notifications to your customer. You also need to state a Merchant name that will be used in the email to your customers. Click on the **Save Changes** button at the bottom of the page.
- 3 If you wish to insert additional text for the notifications to your customer, click on **View/modify individual text to be displayed in the email to your customer**. To save your changes, click on the **Save Changes** button at the bottom of the page.
- 4 Click on **View/configure the events where you want to send/receive a notification** to select Transaction types and Transaction results. To save your changes, click on the **Save Changes button** at the bottom of the page.

Customising Virtual Terminal content

Your Cardnet Virtual Terminal has many possible input fields that you can use, but very few of them are really required. Most of the fields available are there to help you gather information about your Transactions. Since we don't know which ones are helpful for you, we let you choose which ones you want to use.

To simplify your ordering process, you can take the ones you don't use off your entry pages. You make these choices by clicking on **Customisation** in the Main Menu Bar, then on 'Customise your Virtual Terminal page content'. A page will appear which contains a table, listing all the fields you may choose from. Some of the fields cannot be removed from the page; if this is the case, they either do not appear in the listing, or they may appear in the listing with a checked graphic in front of them, rather than a checkbox which you can check or uncheck.

You might notice that not all the input fields appear on this page. Some fields are always required to process a Transaction (for example, the credit Card number is always required for a credit Card purchase). Since these fields must always appear on your entry pages and they are always required, they are not customisable.

Once you've finished your selections, click on the 'Submit' button on the bottom of the page. To put back any of the fields you removed, simply recheck the box preceding the field names (to select them) and click the 'Submit' button again.

You should see a confirmation message at the top of the page if the change was successful.

If you wish to restore the default settings, click on the 'Get Defaults' button at the bottom of the page, then click on the 'Submit' button to submit these settings to our server. Again, a confirmation message should appear.

If you uncheck all the boxes within a particular section, the entire section will disappear from your POS pages.

This same page also allows you to change which fields are required. If, for example, you require an email address for all your customers, you can make email address a required field by checking the appropriate box in the Required column. Make your selections, then click on the 'Submit' button at the bottom of the page. There are a few fields which cannot be made required: all fields related to Items and Recurring Payments. The Total Amount of the order is always required, so you are not allowed to change this either.

Another timesaving feature you might want to use is setting a default value for your fields. For example, if you consistently have sales of the same amount, you might want to set the default value of Total Amount to that specific amount. When you process an order with Lloyds Bank Online Payments, then, the Total Amount will already be pre-filled with your usual total.

If you commonly have the same Transaction origin (for example, all mail orders), it's handy to enter a default for Transaction Origin as well.

To set a default value for one of the fields, simply enter the value you would like it to be in the appropriate textbox in the Default column, then click the 'Submit' button. A confirmation message should appear.

Customising your receipts

When you enter orders into the Cardnet Virtual Terminal, you have the option to show and print a receipt from the final Transaction screen. You can print this receipt and give it to your customers as a sales receipt.

To customise your receipt, follow the steps outlined below:

- 1 Click on Customisation on the Main Menu Bar.
- 2 Click on 'Customise your Receipts'.
- 3 Enter up to 24 characters in the Receipt Header textbox. This text will appear towards the top of your receipt.
- 4 Enter up to 24 characters in the Receipt Footer textbox. This text will appear at the bottom of your receipt.
- 5 Click on the 'Submit' button.

Whenever you return to this screen, your current customised text should appear in the Receipt Header and Receipt Footer text boxes.

Settings for your online store integration

The information contained in this section is applicable only if you are using the Connect solution.

To view this form:

- 1 Logon to Cardnet Virtual Terminal.
- 2 Click on Customisation in the Main Menu.
- 3 Click on 'Define the UR Ls for the integration with your online store'.

Below is an explanation of each of the form fields for the Settings form.

Confirmation Page URL

This is where you tell us the page on your website where to send your customers after a successful Transaction.

Alternatively, you can submit this URL with every Transaction request (see Integration Guide for the Connect solution).

If you want us to display this URL automatically after the receipt page, check the box that says automatically display specified URL after the payment process.

Failure Page URL

You may want to link non-approved customers (customers whose payment Transactions were declined) to a specific page on your website where they will find information on how to get in contact with you by email or by phone. In this section of the screen, you may want to supply the URL for a "Sorry" page where you can invite the customer to contact you to make other payment arrangements.

Alternatively, you can submit this URL with every Transaction request (see Integration Guide for the Connect solution).

If you want us to display this URL automatically after the receipt page, check the box that says automatically display specified URL after the payment process.

Transaction Notification URL

One of the notification options for the results of your payment Transactions is that we send the results to a URL that you can define here.

Alternatively, you can submit this URL with every Transaction request (see Integration Guide for the Connect solution).

Ability to overwrite the stored URLs

If you want to be able to overwrite these URLs with different URLs that you submit with the Transaction request, check the box that says Allow URLs to be overwritten by those in the Transaction request.

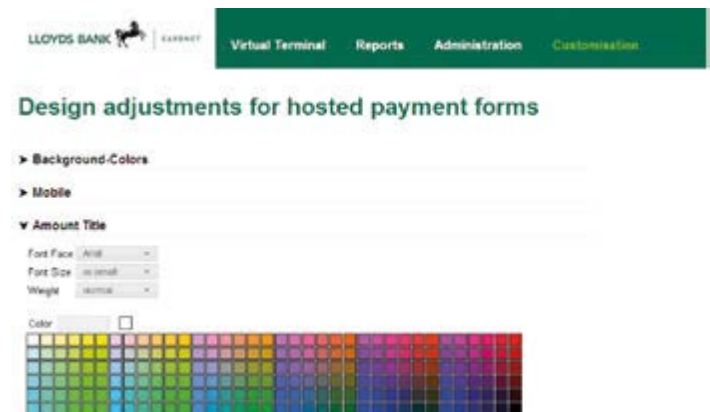
Customising the payment page design

If you use the hosted payment forms of the Connect solution, you can customise the design of these pages to align it with your shop or corporate design.

Choose the Connect Pages link from the Customisation section to individually define the following elements:

- Background colours of different page areas.
- Font type, size, colour and weight for headlines.
- Font type, size, colour and weight for field tags.
- Font type, size, colour and weight for normal text.

- Colour and background colour for buttons.
- Font type, size, colour and weight for button text.
- Font type, size, colour and weight for hyperlinks.
- Font type, size, colour and weight for system messages.



Customising the payment page design

The 'Preview Style' button at the bottom of the page allows you to check the design changes you made before saving (preview is in English language).

Furthermore, the link 'Add static text to your hosted payment forms' allows you to enter a text that will then be shown to the Cardholder on the right side of the payment pages.

Also, it is possible to display your individual company logo on these pages. If required, please contact our technical support team.

There are several ways that Lloyds Bank Online Payments helps you prevent fraud from interfering with your business success. If certain individuals are continuously hurting your business with costly charge-backs, you can block them from purchasing at your store.

We can provide you with the capability to block credit Card numbers, names, domain names, and IP or Class C addresses from purchasing at your store. In addition, two further capabilities are available, and these are the power to set a limit on the maximum purchase that can be made at your store, and the ability to set auto lockout and duplicate lockout times.

To change your fraud settings, select **Administration** in the Main Menu Bar and then click on one of the links in the Fraud Settings section.

Fraud settings are sequentially ordered, so once you've finished with one, you can proceed to the next fraud setting. There is also a quick navigation bar at the right of each Fraud Setting page, which allows you to jump immediately to any Fraud Setting.

Here is a list of all the fraud settings that the Cardnet Virtual Terminal gives you control over:

- Blocking Credit Card Numbers.
- Blocking Names.
- Blocking Domain Names.
- Blocking Class C and IP Addresses.
- Setting a Maximum Purchase Limit.
- Setting Auto lockout times.

- Setting Duplicate Lockout Times.
- Setting a Country Profile.

Another way to prevent fraud is by paying close attention to the address verification response. If the address and/or post-code do not match the Card Issuer's address on record, there is a higher probability of fraud.

Furthermore, for your protection, we urge you to regularly use the Card code field.

Blocking credit Card numbers

The first setting you will encounter when you bring up Fraud Settings is Block Card. Here you can enter the credit Card numbers that you do not wish to allow to purchase at your store.

Fraud Settings

Block Card Numbers

You can choose to block certain card numbers from purchasing at your store. Those card numbers will be prohibited from buying at your online store. You can block a credit card number by directly entering it in the box below or by entering the order number associated with the credit card. When you click the "Add" button, you are submitting your change to our server.

Card #	<input type="text"/>	(numbers only)	<input type="button" value="Add"/>	<input type="text" value="340201 0781"/>
Order Number	<input type="text"/>		<input type="button" value="Delete"/>	
				<input type="button" value="View All Fraud settings"/>
				<input type="button" value="Next"/>

Fraud prevention: Blocking Card numbers

If you have any credit Card numbers already on your blocked credit Cards list, they will automatically appear in the select box on the right side of the screen when you enter this page.

Adding a Card number

To add a Card number to your blocked Card number list:

- 1 Enter the Card number you wish to block in the Card # input box on the left-hand side of the screen. If you do not know the credit Card number you can use the Order Number of the Transaction where the Card has been used instead.
- 2 Then click the Add >> button. When you click the Add >> button, the change is submitted to Lloyds Bank Online Payments, we add the Card number to your list of blocked Card numbers, then we regenerate the page with the new Card number in the select box at the right side of the page.

If this blocked Card should be used to attempt to purchase anything at your store, the Transaction will be declined because of fraud.

Add as many Card numbers as you like by repeating the same process.

Removing a blocked Card number

To remove a blocked Card from your list, select the Card number in the select box on the right side of the screen, then click the << Delete button.

Upon removal from your blocked Card list, the Card number will again be allowed to be used to purchase at your store. Delete as many Card numbers as you need by repeating the same process.

Once you have finished adding and deleting Card numbers, click on the Next button if you wish to go to the next fraud

setting page – this will take you to the Block Names page. If you wish to see all your fraud settings, click on the 'View All Fraud Settings' button.

Blocking names

Take care when blocking names from purchasing at your store. For the name to be blocked, it must match exactly, character for character, space for space. So, for example, if you block the name “John Redenbacher” from your store, “Johnny Redenbacher”, “John Samuel Redenbacher” or “John S. Redenbacher” would not be blocked.

Lloyds Bank Online Payments fraud system cannot distinguish between one “John Smith” and another, consequently blocking all persons with the same name.

You may still wish to block particular names from purchasing at your store. To do so, navigate to the Block Names page (select Administration on the Main Menu Bar, then on 'Add/change names to block').

If you have any names already on your blocked names list, they will automatically appear in the select box on the right side of the screen when you enter this page.

Adding a name

To add a name to your blocked name list, follow these steps:

- 1 Enter the name in the Name input box on the left-hand side of the screen. You can also use the Order Number of the Transaction with the customer to be blocked instead.
- 2 Click the Add >> button.
- 3 When you click the Add >> button, the change is submitted to Lloyds Bank Online Payments, we add the name to your list of blocked names, then we regenerate the page with the new name in the select box at the right side of the page.

If any person with this blocked name should attempt to purchase anything at your store, the Transaction will be declined because of fraud.

Add as many names as you like by repeating the same process. You may want to enter several different versions of the particular name you wish to block.

Removing a blocked name

To remove a blocked name from your list, select the name in the select box on the right side of the screen, then click the << Delete button.

Upon removal from your blocked name list, anyone with that name will again be allowed to purchase at your store. Delete as many names as you need by repeating the same process.

Once you have finished adding and deleting names, click on the Next button if you wish to go to the next fraud setting page – this will take you to the Block Domain Names page. If you wish to see all your fraud settings, click on the View All Fraud Settings button.

Blocking domain names

Once you've finished blocking names and clicked on the Next button, you will find yourself at the Block Domain Names page. (Alternatively you can reach this page by selecting **Administration** on the Main Menu Bar, then clicking on 'Add/change domain names to block'.)

Here you can enter the domain names for individuals from domains that you do not wish to allow to purchase at your store.

If you have any domain names already on your blocked domains list, they will automatically appear in the select box on the right side of the screen when you enter this page.

Adding a domain name

To add a domain name to your blocked domains list, follow the steps below:

- 1 Enter the domain name in the Domain name input box on the left-hand side of the screen, then click the Add >> button. You must enter a domain in valid domain name format (e.g. here.com, there.net, savetheworld.org, universityX.edu).
- 2 Click the Add >> button.

- 3 When you click the Add >> button, the change is submitted to Lloyds Bank Online Payments, we add the domain to your list of blocked domains, then we regenerate the page with the new domain name in the select box at the right side of the page.

If an individual from this domain attempts to purchase anything at your store, the Transaction will be declined because of fraud.

Add as many domain names as you like by repeating the same process.

Removing a blocked domain name

To remove a blocked domain from your list, select the domain name in the select box on the right side of the screen, then click the << Delete button.

Upon removal from your blocked domains list, individuals from that domain will again be allowed to purchase at your store.

Delete as many domains as you need by repeating the same process.

Once you have finished adding and deleting domain names, click on the Next button if you wish to go to the next fraud setting page – this will take you to the Block IP/Class C Address page. If you wish to see all your fraud settings, click on the View All Fraud Settings button.

Blocking IP and Class C addresses

Once you've finished blocking domain names and clicked on the Next button, you will find yourself at the Block IP/Class C page. (Alternatively you can reach this page by selecting Administration on the Main Menu Bar, then clicking on 'Add/change IP/Class C addresses to block'.)

Here you can enter the IP and Class C addresses for people or organisations that you do not wish to allow to e-purchase at your store.

If you have any IP or Class C addresses already on your blocked IP or Class C list, they will automatically appear in the select box on the right side of the screen when you enter this page.

Adding an IP or Class C address

To add an IP or Class C address to your blocked IP or Class C list, follow these steps:

- 1 Enter the address in the IP/Class C input box on the left-hand side of the screen. You must enter IP addresses in the standard format, which is four numbers separated by 3 decimal points (e.g. 123.123.123.123). To enter Class C addresses, enter the first 3 numbers separated by decimal points with a decimal point at the end (e.g. 123.123.123.)

If you do not know the address you can use the Order Number of the Transaction where the IP/Class C address has been used instead.

- 2 Click the Add >> button.

- When you click the Add >> button, the change is submitted to Lloyds Bank Online Payments, we add the name to your list of blocked IPs/Class Cs, then we regenerate the page with the new name in the select box at the right side of the page.

Removing an IP or Class C address

To remove a blocked IP or Class C address from your list, select the address in the select box on the right side of the screen, then click the << Delete button.

Upon removal from your blocked IP or Class C address list, persons visiting from that address will again be allowed to purchase at your store.

Delete as many addresses as you need by repeating the same process.

Once you have finished adding and deleting IP and Class C addresses, click on the Next button if you wish to go to the next fraud setting page – this will take you to the Set Maximum page. If you wish to see all your fraud settings, click on the View All Fraud Settings button.

Setting maximum purchase limit

Once you've finished blocking IP and Class C addresses and clicked on the Next button, you will find yourself at the Set Maximum page. (Alternatively you can reach this page by selecting Administration on the Main Menu Bar, then clicking on 'Set Maximum Purchase Amount'.)



Fraud prevention: Setting maximum purchase limit

Any Transactions for your store above this amount will be declined because of fraud. This field will be pre-filled with the current maximum purchase limit for your store, if you have one.

If you wish to change this limit, simply enter the number in the Maximum Purchase Limit input box with the limit you wish to enforce, then click on the 'Submit' button.

If you do not wish to change your maximum purchase limit, you can click on the Next button to go to the next Fraud Setting: Auto Lockout. If you wish to see all your fraud settings, click on the View All Fraud Settings button.

Setting auto lockout and duplicate

Once you've finished with the Maximum Purchase Limit and clicked on the Next button, you will find yourself at the Set Lockout Times page. (Alternatively you can reach this page by selecting **Administration** on the Main Menu Bar, then clicking on 'Set lock out times'.)

There are two things you can set on this page: the auto lockout time and the duplicate lockout time.

Auto Lockout time is the amount of time that automatically blocked Transactions are prohibited from trying Transactions at your store again.

Duplicate lockout time is the length of time that duplicate Transactions are restricted from your store. That is, if two Transactions are identical and they both occur within a length of time less than the specified duplicate lockout time, they will be automatically blocked as duplicate Transactions.

To change your auto lockout or duplicate lockout time, simply replace the value in the appropriate input box with the new value and then click on the 'Submit' button.

If you don't wish to change your lockout times, you can click on the Next button to go to the next Fraud Setting: Country Profile. If you wish to see all your fraud settings, click on the View All Fraud Settings button.

Setting a country profile

Once you've finished with the Lockout times and clicked on the Next button, you will find yourself at the Country Profile page. (Alternatively you can reach this page by selecting **Administration** on the Main Menu Bar, then clicking on 'Set country profile'.)

The Country Profile page allows you to constrain credit Card acceptance to Cards from specific countries. Simply chose one of the five profiles that vary from accepting Cards from all countries (default) to accepting only Cards from one specific country. Then click on the Submit button.

If you don't wish to change your country profile, you can click on the View All Fraud Settings button to see all your fraud settings.

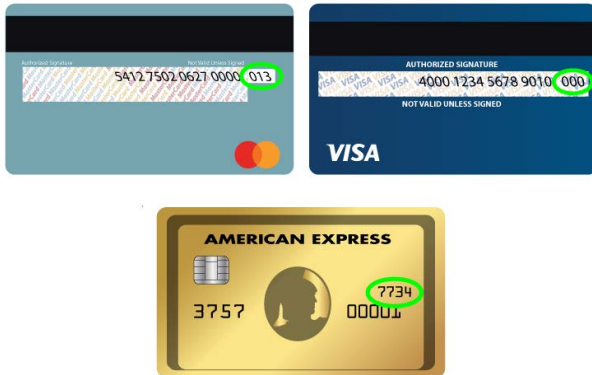
Card Security Code information

Mail order and telephone order (MO/TO) and other Card Not Present Transactions have higher fraud rates than face-to-face Transactions. To help reduce fraud in the Card Not Present environment, credit Card companies have introduced a Card code programme.

Visa® calls this code Card Verification Value (CVV); Mastercard® calls it Card Validation Code (CVC); American Express calls it 4DBC; Diners® calls it CID; Diners Club International® calls it CVV2.

Fraud Prevention Tools

The Card Security Code is a three or four digit security code that is printed on the back of Cards (American Express: front of the Card). The number typically appears at the end of the signature panel. This programme helps validate that a genuine Card is being used during a Transaction.




Card Security Code information

You enter the Card code on the Point-of-Sale screen when processing an order. Cardnet then compares the Card code against the code on file with the Card Issuer. Results of this comparison show in the Transaction approval code.

Card Credit/Debit Card

Select card type:

Supported Card Types: 

Transaction Origin:

Transaction Type:

Card number:

Expiry date: /

Card Security Code:

Virtual Terminal: Card Security Code field

To help combat fraud, Card Not Present Merchants (those who receive orders via mail order, telephone order, or the Internet) should always enter a Card Security Code (if on the Card) when processing an Authorisation. For retail Transactions, you may wish to enter the Card Security Code printed on the Card to ensure that the Card was not fraudulently reproduced.

A typical Transaction result code might look like this. The Card Security Code result is highlighted:

0097820000019564:YNAM:12345678901234567890123:

The last alphabetic character in the middle (M) is a code indicating whether the Card Security Code matched the Card Issuer's code. An "M" indicates that the code matched.

This code may or may not be present, depending on whether the Card Security Code was passed and the service was available for the type of Card used. Below is a table showing all the possible return codes and their meanings.

Value	Meaning
M	Card Security Code Match
N	Card Security Code does not match
P	Not processed
S	Merchant has indicated that the Card Security Code is not present on the Card
U	Issuer is not certified and/or has not provided encryption keys
X	No response from the credit Card association was received

A blank response should indicate that no code was sent and that there was no indication that the code was not present on the Card.

Inventory management

If you are using the Cardnet Online Payment's Web Service API to manage stock information for your products, you can view and manually modify the quantities in the Online Portal. Select Customisation on the Main Menu Bar, then click on 'Manage your Inventory' to access the Inventory Management page.

Please note that this feature does not automatically update the stock information for orders that have been processed via the Virtual Terminal.

Changing your own password

To change your password in the Cardnet Virtual Terminal, select Administration on the Main Menu Bar, then click on 'Change Password'. This will bring up the Change Password page.

When you first sign up for an account with the Cardnet Virtual Terminal, you are provided with a temporary password. The Change Password feature allows you to change that password and it is a necessary step that everyone must undertake.

The choice of new password is important too. Security specialists recommend that you avoid using common words or numbers as passwords-especially words or numbers that might be associated with you, like your name or your date of birth.

One simple approach is to choose a phrase -not a word -that you can remember or look up easily. Put together the first letter from each word in the phrase and that string of letters becomes your password. The phrase should consist of at least six words, to produce at least a six letter password. In addition, the password needs to have at least one numeric character.

To change your password, type your new password into the New password box. What you see in the box are asterisks instead of the letters and numbers that you type, for security reasons anyone looking over your shoulder cannot easily see what you have typed. Type the password again, this time into the second box entitled 'Enter password again'. This is a commonly employed precaution against accidentally mistyping it the first time.



Changing your password

Click on the 'Submit' button. If you did accidentally mistype your new password you will be advised that there is an error, and asked to re-enter the information. For added security, the error message will not specify which entry is at fault. If you successfully changed your password, you will receive feedback to that effect.

Managing users

You can have multiple users for one store, which allows multiple employees to process orders and/or view reports, each of them logging on with their own user ID, password, and permissions. All users of one store can share the same client certificate.

To add or delete users, you must be logged in on the store's original user account. The primary user for the store – the user ID and password that was provided when the store account was set up – is the only user who can add/delete users and assign permissions. No other users are allowed to add or remove users or assign user permissions. Users who do not have permissions to manage users will not see the Manage Users option on the Administration page.

Adding and Deleting Users

To manage users, you first need to get to the Account Manager:

- 1 Click on Administration on the Main Menu Bar.
- 2 Then click on 'Add/remove/modify user'.
- 3 The Current Users page will appear.

Now that you are on the current users page, you can add or delete users, reset password, and/or define permissions for each user.

To add a user:

- 1 Click on the Add link located at the bottom of the page.
- 2 The Add User screen will appear.
- 3 Enter a unique User ID for the new user in the Username text box, then enter a Password for your new user twice.
- 4 Click on the 'Continue' button to create the new user.
- 5 The Current Users list will reappear, showing the new user on the list.

The user can change their own password when they log in by using the Change Password utility.

To delete a user:

- 1 Click on the delete link located next to the user you wish to delete.
- 2 A dialogue box will appear, stating that this operation will delete the selected user.
- 3 Click the OK button to delete the user or Cancel if you do not wish to delete the user.

- 4 Once the user is deleted, the Current Users screen will refresh, with the deleted user omitted from the list.

Resetting User Passwords

If a user should forget their password and you need to reset it:

- 1 Click on the reset password link for the appropriate user.
- 2 Enter a new password for the user twice, then click the 'Submit' button.

The user can change their temporary password when they log in by using the Change Password function.

Setting User Permissions

To set permissions for a user:

- 1 Click on the permissions link associated with the desired user.
- 2 The Set User Permissions page will appear.
- 3 In the Permissions portion of the table, click on the appropriate checkboxes to turn on or off permissions for this user. You can control the user's access to View Reports, Process Transactions, and/or Issue Credits.
- 4 Click on the 'Continue' button at the bottom of the page.

You will be returned to the Current Users listing. The words "updated successfully" should appear at the top of the page if the change was successful.

Accepting Transactions

Card Schemes

Your Cardnet facility allows you to accept many different types of Cards. The guide below shows you the processing options possible for each of the different Card Schemes.

Card type	Electronic processing	Manual key entry	Mail and telephone order*	E-commerce*	Purchase with Cashback*
Mastercard	✓	✓	✓	✓	✗
Debit Mastercard	✓	✓	✓	✓	✓
Maestro	✓	✓	✓	✓#	✓
International Maestro	✓	✗	✗	✓#	✓
Visa Credit	✓	✓	✓	✓	✗
Visa Debit	✓	✓	✓	✓	✓
Electron	✓	✗	✓	✓	✓
V PAY	✓	✗	✗	✓**	✓†
Discover Global Network (includes Discover®, Diners Club International® and Partner cards)	✓	✓	✓	✓	✗
Corporate, Commercial and Purchasing Cards	✓	✓	✓	✓	✗
UPI (UnionPay International)	✓	✓	✗	✗	✗
JCB (Japan Credit Bureau)	✓	✓	✗	✗	✗

Accepting Transactions

* The acceptance of these facilities must also be agreed with Cardnet. For more information contact the Cardnet Helpline on **01268 567 100**. Lines are open 8am-9pm, Monday to Saturday.

Maestro cards can only be accepted over the Internet if you are registered for Mastercard Identity Check.

For more information about Mastercard Identity Check see, Section 4 'Accepting Transactions' page 46, or visit www.mastercard.com/global/merchants/identity-check.html

† If permitted by the issuer.

** V PAY can only be accepted over the Internet if:

- Permitted by the issuer.
- You are registered for Visa Secure.

For more information about Visa Secure see page 46, Section 4 'Accepting Transactions', or visit the Business and Retailers Section of www.visaeurope.com

For more information about Diners Club International ProtectBuy see page p46, Section 4 'Accepting Transactions', or visit www.discovernetwork.com/en-intl/business-resources/fraud-security/products-tools/protect-buy

If you would like further information on accepting American Express, please contact Cardnet the Cardnet Helpline on **01268 567 100**.

Please note that zero floor limits will apply to all of the following Transaction types below and you must always obtain an Authorisation for such Transactions.

Where the customer is present:

- All magnetic stripe read Transactions.
- All key entered Transactions.
- All paper or manually processed Transactions (Authorisation by telephone).
- All Purchase with Cashback Transactions.

Where the customer is not present:

- All Card Not Present Transactions which include Mail/Telephone Order, E-commerce (Internet) and Recurring Transactions.

Please remember that if you process any of the above Transactions without Authorisation they may be rejected by the Card Issuer and charged back to you.

Pay by URL

The Payment URL functionality allows you to provide a link to your customers (e.g. in an email invoice, WhatsApp message, SMS, QR code, etc.) which then takes the customer to a webpage where they can securely make the payment with their preferred payment method, whenever convenient for them.

This is especially useful in scenarios where goods get paid after delivery, where no goods get shipped at all (e.g. final payment for trips that have been booked months ago) or for the payment of monthly bills. With the Payment URL functionality enabled for your store, you will find an option to select Generate Payment URL under the Order Information.

Virtual Terminal: Dedicated checkbox for Payment URL generation

Point of Sale

Required fields Optional fields

Product Catalogue

Select Products

Order Information

Generate Payment URL:	<input checked="" type="checkbox"/>		
Payment URL Expiry Date and Time:	DD/MM/YYYY	HH:mm:ss	
Order Number:			
Subtotal:			
Total Amount:			
Currency:	GBP		

Customer Details

Delivery Information

Comments

Continue

If the checkbox is selected, the Card section (Credit Card, Direct Debit) and Recurring sections will be hidden. You can then complete the required information for the payment URL and continue the transaction as usual.

The generated URL will be shown on the Transaction Result page where it can be selected (copied) to provide it to the customer. The URL can also be copied from the Order Details page at a later point.

Virtual Terminal: Generated Payment URL to be copied by clicking Select button

Transaction Result

Transaction Information

Transaction Type:	Sale
Transaction Status:	APPROVED
Payment URL:	https://test.ipg-online.com/connect/gateway/processing?storename=2220540004&oid=TestTransaction001&paymentUrlId=3ea51f7c-943b-454e-8a83-28056a667a77 <input type="button" value="Select"/>
Transaction date and time:	17-Jan-2022 16:14:42
Approval code:	? :Payment URL created:

Order Information

Generate Payment URL:	true
Payment URL Expiry Date and Time:	17/01/2022 23:59:59
Order Number:	TestTransaction001
Subtotal:	30.00
Total Amount:	30.00
Currency:	GBP

Card

Transaction Origin:	Mail Order/Telephone Order
Are You Swiping The Card?:	No

Customer Details

Address:	1
Country:	United Kingdom
Post Code:	W2 3AT

Delivery Information

Back Next Transaction

Accepting Transactions

Please note that a created Payment URL is shown in the Reports with an approval code “?:Payment URL created”. Once the consumer has accessed the URL and made the payment, the Reports will show the result of the payment transaction.

Virtual Terminal: Overview of a Payment URL transaction completed by the customer

Order Details

TestTransaction001 17-Jan-2022 16:14:42 (Europe/London)

Date	Terminal ID in each msg	User ID	Type	Card/Account number	Exp. Date	Approval	Payment URL Expiry Date and Time	Amount
17-Jan-2022 16:14:42		2220540004	Sale			? :Payment URL created:	17/01/2022 23:59:59	30.00 GBP
Comments:								
Payment URL: https://test.ipg-online.com/connect/gateway/processing?storename=2220540004&oid=TestTransaction001&paymentUrl=3ea517c-943c-454e-8a83-26056a667a77								
<input type="button" value="Void"/>								
17-Jan-2022 16:18:24		214041562220540004	Sale	433287_1977	08/2024	Y:286801:4586914521:NNNP:0001		30.00 GBP
<input type="button" value="Send Notifications"/>								
<input type="button" value="Print Receipt"/>								
Comments:								

Benefits of using Pay by URL:

- Send a payment URL link directly to your customers via email
- Add payment links to invoices so a payment can be made directly
- Simple set up – send the link to make a payment using an email through the Virtual Terminal
- Make it easier for your customers to pay without the need for logins and passwords
- Reduce cost – no need to setup a website to accept payments.

Further details and more information about Pay by URL can be found on lloydsbankcardnet.com

CARDNET HELPLINE



Call **01268 567 100**

8am to 9pm Monday to Saturday

Call our knowledgeable UK-based team with any questions about Data Security, who can also provide you with a Key Facts Document regarding the PCI DSS.

Biometric Checkout

Biometric checkout in-store is an emerging payment experience, which offers cardholders the ability to use biometrics to identify themselves and pay for in-person purchases, without use of a payment card or a cardholder's mobile device. To support the responsible development of such solutions, Mastercard is introducing the Biometric Checkout Program, which leverages standards and specifications that address end-to-end security, biometric performance, privacy controls, and other considerations for added convenience and safety.

Customer Benefit

- Drive differentiation via an innovative method to engage customers
- Enable a positive, frictionless cardholder experience for payment, plus loyalty and preference
- Protect loyalty by offering cardholders a more secure and simple way to verify their identity
- Generate more sales with faster checkout, reducing queuing time
- Secure transactional information through tokenization

Cardholders:

- Enjoy a touchless, convenient, and secure checkout experience
- Greater choice in how and where to use biometrics for payments
- Peace of mind with the added security, privacy controls and touchless experience at the point of interaction(POI)

Digital Wallets

1) Pass-Through Digital Wallets

Pass-Through Digital Wallets are typically mobile phone-based solutions that allow customers to pay in-store (as a tap to pay transaction) or online, usually via a tokenized, digital version of their physical Visa product. Pass-Through Digital Wallets may also be embedded on "wearables" (e.g. smart watches) or browser-based "card on file" solutions specifically for conducting online/E-commerce transactions.

Key Requirements

Transactions initiated using Pass-Through Digital Wallets transmit the customer's payment credential to the seller, who then processes the transaction directly with their acquirer like any other Visa Payment transaction. The wallet operator, therefore, is not involved in the movement of funds, and no funds are stored in/by the wallet.

2) Stored Value Digital Wallets

Stored Value Digital Wallets operate like prepaid cards by assigning a separate "account" to the customer, which the customer pre-loads with funds using their Visa payment credential, before being able to transact with sellers connected to the digital wallet's platform or complete a P2P transfer to other users of the wallet's platform. Generally, customers and sellers are either transacting within the Stored Value Digital Wallet's proprietary network of connected users, or within the Visa ecosystem if the wallet has attached a Visa product (e.g. a prepaid credential) to the "front" of the wallet, so the wallet uses Visa to make purchases, cash withdrawals etc.

Key Requirements

The wallet may allow different funding options for the customer (e.g. manual/ad-hoc loads, recurring loads or balance-driven loads), but the customer's wallet-assigned account must always hold a balance of pre-loaded funds to be able to transact.

Sellers directly connected to the digital wallet's platform are connected to the digital wallet to accept pre-loaded funds from digital wallet assigned accounts, via the digital wallet's brand; they are not accepting Visa payment credentials directly for payment when the customer pays using the digital wallet.

Stored Value Digital Wallets must only work with acquirers located in the same country¹ to load funds from a linked Visa payment credential. When loading funds into the digital wallet account from a linked Visa payment credential, the Stored Value Digital Wallet and the wallet's acquirer must process the transaction as an Account Funding Transaction (AFT) with a Business Application Identifier (BAI) of "FT" (Funds Transfer), along with the Stored Value Digital Wallet's Merchant Category Code (MCC).

¹In Visa's Europe region, the acquirer, Staged Digital Wallet and seller may be in different countries within Europe. Consult the Visa Rules for more information.

3) Staged Digital Wallets

Staged Digital Wallets are capable of conducting "back-to-back funding" transactions – also known as a "live-load" or "real-time load" – which permits the customer to undertake transactions with sellers on the digital wallet's platform when there are not sufficient funds in the digital wallet-assigned account to complete the transaction (which may include a "zero balance").

For a "back-to-back funding" transaction, the funding or reimbursement transaction from the underlying Visa payment credential:

- (i) Exactly matches the amount of the transaction attempted by the customer
- (ii) Equals the remainder of the purchase amount, if also partially funded by an existing balance in the digital wallet assigned account (which may include another store of value e.g. "pay with points"), or
- (iii) Is completed by multiple automated loads of a pre-determined value

Key Requirements

Transactions within Staged Digital Wallets are always between connected users i.e. customers who hold accounts with the Staged Digital Wallet and sellers directly connected to the Staged Digital Wallet's platform. Staged Digital Wallets must hold acceptance contracts with all sellers on their platform and must not contract with sellers located in another country².

Unlike Stored Value Digital Wallets, Staged Digital Wallets are not permitted to assign a Visa or other general-purpose payment network product (e.g. a prepaid credential) to the “front” of the digital wallet account to make purchases, cash withdrawals etc. Use of the Staged Digital Wallet must only occur within the wallet’s own proprietary network of connected users and sellers.

In order to load funds or complete “back-to-back funding” transactions from a linked Visa payment credential, Staged Digital Wallets must only partner with an acquirer who (i) meets Visa’s minimum equity requirements, and (ii) is located in the same country².

Staged Digital Wallets must differentiate “load” or “top-up” transactions and “back-to-back funding” purchases to ensure that the applicable data elements in the Visa transaction are correct. When loading funds into the digital wallet account from a linked Visa payment credential, the Staged Digital Wallet and the wallet’s acquirer must process the transaction as an AFT with a BAI of “WT” (Wallet Transfer), along with the Staged Digital Wallet’s MCC. Finally, when completing a “back-to-back funding” transaction, the transaction must be processed as a Purchase, also with a BAI of WT, but with the seller’s MCC and not the wallet’s MCC.

²In Visa’s Europe region, the acquirer, Staged Digital Wallet and seller may be in different countries within Europe.

Additional Visa Acceptance Entities

The Visa acceptance ecosystem covers all commerce types, including the face-to-face, unattended, mobile and E-commerce environments; it helps to increase electronic payment acceptance for sellers, allowing a variety of ways to connect to Visa either directly, through an acquirer or via a third-party.

Payment Facilitator (PF)

A Payment Facilitator (PF) – also known as a “master merchant” or “merchant aggregator” – is a third-party agent that can both (i) sign a merchant acceptance agreement with a seller on behalf an acquirer, and (ii) receive settlement proceeds from an acquirer, on behalf of the underlying seller (known as a Sponsored Merchant or “submerchant”); an entity that performs either one of these functions is considered a PF, even if they don’t perform both functions. A PF may also process transactions via a gateway link between the acquirer and seller and may also provide point of sale (POS) infrastructure to sellers. PFs mostly operate across one of two verticals:

- As a dedicated “acquirer-lite” entity specialising in payment acceptance for either small sellers or narrow/highly-specialized industry segments with unique needs (e.g. rent, education, or government payments).
- Other types of service providers who include payment processing and “on-behalf-of” funds settlement as a value-added service, alongside their suite of services to sellers.

PFs must partner with an acquirer who meets Visa's minimum equity requirements. Although PFs hold the primary relationship with their sponsored merchants, PFs must ensure that the acquirer is added to the merchant acceptance agreement if the sponsored merchant's annual Visa sales exceed a certain volume¹ However, the PF may continue to service their sponsored merchants, including processing transactions and receiving settlement.

In general, there are no merchant category restrictions for PFs, however additional obligations and requirements apply for PFs working with sellers in certain high-risk categories. Additionally, PFs are not permitted to acquire transactions from other PFs and Staged Digital Wallet Operators.

Aside from rules that enable a PF to sign the merchant agreement, process transactions and receive settlement³, all Visa requirements apply equally to a sponsored merchant, as if the sponsored merchant was contracted directly with an acquirer.

³Local laws or regulations in some jurisdictions may require PFs or Marketplaces to obtain a money transmission license (or similar) to be entitled to receive and transmit settlement funds.

Marketplace

A Marketplace is an online entity that brings together customers and sellers on a single, Marketplace-branded platform (i.e. E-commerce website or mobile application), processes transactions and receives settlement² proceeds on behalf of those sellers; entities that do not process transactions on behalf of sellers are not considered Marketplaces. In this model, it is the Marketplace's brand that attracts the customer and connects them with sellers operating on the Marketplace's platform; the customer can see that they are purchasing from the seller on the Marketplace and not the Marketplace itself. Marketplaces are not permitted to operate in a "card present" environment.

Marketplaces may operate with sellers in a single line of business (e.g. restaurant/food delivery) or multiple lines of business, selling a variety of goods or services that don't fall under a single category.

In this context, it is the Marketplace that contracts with the acquirer – not the underlying sellers. The Marketplace also manages the primary customer experience, processing the customer's purchase and issuing a transaction receipt under the name of the Marketplace, even if the customer is buying from multiple sellers in a single transaction. The Marketplace also handles refunds and disputes between the buyer and seller.

Like the PF model, acquirers must meet minimum equity requirements to be eligible to acquire a Marketplace. Further, Marketplaces must ensure that no single seller exceeds both U.S. \$10,000,000 (or local currency equivalent) and 10% of the Marketplace's annual Visa sales volume.

However, unlike the PF model, there are some merchant category restrictions for Marketplaces. Specifically, Marketplaces are not permitted to work with travel agents, franchises or sellers in certain high-risk categories. Also unlike the PF model, although the acquirer and Marketplace must be located in the acquirer's licensed country, independent sellers on the Marketplace's platform may be located in another country (providing that it is legal to do so in both countries).

Third-Party Bill Payment Providers

Visa recognizes that not all sellers accept electronic payments for goods or services, e.g. some public utilities or commercial billers; however, many customers still want to be able to pay bills with their Visa payment credentials. Therefore, Visa created two categories of third-party bill payment providers where there is a pre-existing relationship between the customer and biller. Both models operate with a similar construct; however, they differ based on who is paying who, and for what:

- The Consumer Bill Payment Service (CBPS) enables customers to pay bills using their Visa payment credentials, in categories where electronic payments are not widely accepted. Applicable biller categories differ based on local country needs⁴ but mostly include segments such as utilities, healthcare, rent or government/tax payments.

- Like the CBPS model, Business Payment Service Providers (BPSP) enable customers to pay bills using their Visa payment credentials, even though the underlying biller does not accept electronic payments through Visa. However, the BPSP model is focused on commercial or business-to-business payments, usually for invoices based on pre-negotiated terms.

BPSPs are not permitted to enable transactions for billers who do accept Visa for payment through other channels.

In the CBPS and BPSP models, it is the CBPS/BPSP that contracts with the acquirer – not the underlying sellers – meaning acquirers can leverage the scale and reach of their CBPS or BPSP partner, without needing to on-board every underlying biller where traditional Visa acceptance is generally not available. The CBPS/BPSP also manages the end-to-end customer experience, processing the customer's purchase and issuing a transaction receipt under the name of the CBPS/BPSP; the CBPS/BPSP also manages customer service inquiries, refunds and disputes, though these are usually low on the basis that most payments are post-paid bills for products/services that have already been consumed or delivered.

Acquirers must meet minimum equity requirements to acquire transactions from both CBPS and BPSP entities and must ensure that both the CBPS/BPSP and the underlying biller is located in the acquirer's licensed country.

⁴The CBPS model is only permitted in a limited number of countries and biller categories. Please refer to the Visa Rules for specific details.

Digital Wallet Operators

Digital wallets are software-based systems that (i) store information about a customer's Visa credentials used to fund the wallet's account and (ii) are used to make payments – either purchases from sellers or money remittance (i.e. person-to-person “P2P” transfers). In Visa's ecosystem, digital wallets share the following common features:

- Functionality that can be used at more than one seller⁴
- Stores and transmits payment credentials from the customer to the seller to initiate transactions, or from the sender to the recipient for a P2P transfer (e.g. Visa account number (PAN) or payment token).

There are many distinct features that digital wallets may support, based on the flows of funds, processing infrastructure supported on their platform and ultimately the role Visa's payment credentials play in the wallet. These different features determine the way Visa categorizes the digital wallet, and therefore what activity is permitted or prohibited.

Visa defines three different types of digital wallets.

- Pass-Through Digital Wallets are typically mobile phone-based solutions that allow customers to pay in-store (as a tap to pay transaction) or online, usually via a tokenized, digital version of their physical Visa product. Pass-Through Digital Wallets may also be embedded on “wearables” (e.g. smart watches) or browser-based “card on file” solutions specifically for conducting online/E-commerce transactions. Transactions initiated using Pass-Through Digital Wallets transmit the customer's payment credential to the seller, who then processes the transaction directly with their

acquirer like any other Visa payment transaction; no funds are stored in/by the wallet.

- Stored Value Digital Wallets operate like prepaid cards by assigning a separate “account” to the customer, which the customer pre-loads with funds using their Visa payment credential, before being able to transact with sellers connected to the digital wallet's platform or complete a P2P transfer to other users of the wallet's platform. Generally, customers and sellers are either transacting within the Stored Value Digital Wallet's proprietary network of connected users, or within the Visa ecosystem if the wallet has attached a Visa product (e.g. a prepaid credential) to the “front” of the wallet, so the wallet uses Visa to make purchases, cash withdrawals etc. Customers using Stored Value Digital Wallets need to make sure the wallet-assigned account must always hold a balance of pre-loaded funds to be able to transact. Stored Value Digital Wallets are not permitted to conduct “back-to-back funding” transactions⁵.

Sellers connected to the DWO's platform are connected to the DWO to accept pre-loaded funds from DWO-assigned accounts, via the DWO brand; they are not accepting Visa payment credentials directly for payment when the customer pays using the DWO wallet. Stored Value Wallets must only work with acquirers located in the same country.

Accepting Transactions

- Staged Digital Wallets are capable of conducting “back-to-back funding” transactions⁵ which permits the customer to undertake transactions with sellers on the digital wallet’s platform when there are not sufficient funds in the digital wallet-assigned account to complete the transaction (which may include a “zero balance”).

For a “back-to-back funding” transaction, the funding or reimbursement transaction from the underlying Visa payment credential:

- (i) Exactly matches the amount of the transaction attempted by the customer
- (ii) Equals the remainder of the purchase amount, if also partially funded by an existing balance in the digital wallet assigned account (which may include another store of value e.g. “pay with points”), or
- (iii) Is completed by multiple automated loads of a pre-determined value

Transactions within Staged Digital Wallets are always between connected users i.e. customers who hold accounts with the Staged Digital Wallet and sellers directly connected to the Staged Digital Wallet’s platform. Unlike Stored Value Digital Wallets, Staged Digital Wallets are not permitted to assign a Visa or other general-purpose payment network product (e.g. a prepaid credential) to the “front” of the digital wallet account to make purchases, cash withdrawals etc. Use of the Staged Digital Wallet must only occur within the wallet’s own proprietary network of connected users and sellers.

Like Stored Value Wallet platforms, sellers connected to the Staged Digital Wallet’s platform are connected to the DWO to accept funds through DWO-assigned accounts, via the DWO brand; they are not accepting Visa payment credentials directly for payment. Further, Staged Digital Wallets must differentiate “load” transactions and “back-to-back” purchases to ensure that the applicable data elements are included for the different transaction types.

Like PFs, Staged Digital Wallets must only partner with an acquirer who (i) meets Visa’s minimum equity requirements, and (ii) is located in the same country. Staged Digital Wallets must hold acceptance contracts with all sellers on their platform and must not contract with sellers located in another country⁶.

In general, there are no merchant category restrictions for DWOs, however additional obligations and requirements apply for DWOs working with sellers in certain high-risk categories. Additionally, WOs are not permitted to link to other DWOs or be acquired by Fs.

⁴Single merchant wallets (where stored funds cannot be used outside the single merchant’s environment) are not categorized as digital wallets in the Visa Rules.

⁵Also known as a “live-load”, “purchase-drive load” or “realtime load”

⁶In Visa’s Europe region, the acquirer, Staged Digital Wallet and seller may be in different countries within Europe. Consult the Visa Rules for more information.

5 : Authorisation and referrals

This section explains when Authorisation is required for Transactions and how to conduct a referral. It also covers the processes for splitting sales with other payment types, cancelling a Transaction and providing a Refund.

When to obtain Authorisation

Authorisation must be obtained (in accordance with your Terminal operating instructions and your Agreement) before the sale is concluded.

Your Terminal will, in most cases, obtain Authorisation for Transactions equal to or over zero (or equal to or over your agreed floor limit). However, it is your responsibility to ensure that all the relevant checks are carried out-see Section 3, 'Checking the Card' (p40).

Manual Authorisation

You must manually authorise the Transaction if:

- Your Terminal indicates that it is necessary to do so. You must make an Authorisation call and let the Authorisation Centre know that you are calling as a result of a Terminal referral.
- You are using the paper Fall back procedures-see Section 9, 'Exceptions' (p147).
- There is a split sale – See p110 in this section.
- You are suspicious of a Card/Cardholder -in these circumstances a 'Code 10' Authorisation should be made see Section 7, 'Security, Suspicious Transactions' (p128).

Remember: Authorisation is not a guarantee of payment. It confirms that the Card has not been reported lost or stolen at the time of the Transaction and that adequate funds are available.

Authorisation adjustments/reversals

If there is any change in the authorised amount of the sale, or if the sale is cancelled or a Refund issued, please contact the Authorisation Centre stating you wish to cancel or amend an Authorisation.

You will be asked to provide:

- The Card number.
- Your Cardnet Merchant number.
- The amount of the original Authorisation.
- The Card expiry date.
- The issue number of the Card (if applicable).
- The original Authorisation code.

Mastercard transactions may no longer be cancelled after the Authorisation is approved in full (excluding non-completion for reasons of technical failure) See page 111.

Pre-Authorisation and Final Authorisation

Effective 1 January 2016 Mastercard requires Authorisations to be categorised as either a Pre-Authorisation (this is when the final spend is unknown) or a Final Authorisation (when the final spend is known). This enables a more accurate and transparent management of the Cardholders 'open to buy' (available spend), in order to improve Card holder satisfaction.

What is a Pre-Authorisation?

Pre-Authorisations typically occur in the travel and entertainment sector, such as when a Cardholder is checking into a hotel or hiring a rental car, but can also occur in the E-commerce environment when the Merchant is unable to fulfil the full order request, i.e., goods out of stock.

Previously, Mastercard permitted a 15% or 20% tolerance between the authorised amount and the clearing amount for Merchants operating in the hotel, vehicle and cruise line sector. With this new procedure, these tolerances will be removed, and you must complete a reversal request if the final spend is less than the Pre-Authorised amount. This will need to happen within 24 hours of the final Transaction.

What is a Final Authorisation?

Final Authorisations occur when the final spend is known and should meet the following technical characteristics,

- Authorisation must be requested for the final Transaction amount
- Transactions may no longer be cancelled after the Authorisation is approved in full (excluding non-completion for reasons of technical failure)
- The Transaction must be presented within 7 calendar days of the Authorisation date
- The currency of the Transaction must be the same in Authorisation and settlement

What do you need to do?

Please speak with your third party Payment Service Provider if you believe you are carrying out Pre-Authorisations to ensure that you and they are fully compliant. If you are a Merchant whose business practice means that you would only ever use a Final Authorisation, then no further action is required on your part.

For more information contact the Cardnet Helpline on **01268 567 100**. Lines are open 8am-9pm, Monday to Saturday.

Update to Visa T&E Transaction Rules

Effective 16 October 2015, Visa Europe and Visa Inc. updated their rules to introduce more precise and effective regulations for the Travel and Entertainment (T&E) sector and to align with the changing needs of the industry.

T&E now includes all of the following Merchants and Merchant types:

- Airlines
- Car rental Merchants
- Cruise lines, where overnight accommodation is provided
- Hotels, which is redefined as lodging Merchants
- Passenger railways where the Merchant is located in the US Region only
- Travel agencies

Rules specific to hotel reservations, car rental and priority check-out have been replaced with guaranteed reservations, which will be permitted across the following range of Merchants:

- Aircraft rental
- Bicycle rental
- Boat rental
- Car rental Merchants
- Equipment rental
- Motor home rental

- Lodging Merchants
- Motorcycle rental
- Trailer parks or campgrounds
- Truck and trailer rental

The requirements for disclosing any terms of cancellation and the rules that permit Merchants to process a “no-show” Transaction if a Cardholder does not cancel or take up the reservation are clarified and are available to a wider range of Merchants.

Rules for advance deposit Transactions and delayed delivery Transactions have been replaced with prepayments, which will now be permitted across a wider range of Merchants. Merchants are allowed to take either partial or full prepayment for goods and services that are to be provided at a later date.

The requirements for proper disclosure at the time of making a reservation and the rules for disclosing Refund and return policies at the time of Transaction have been aligned with current industry practice and now give Merchants more options for providing the proper disclosure of their cancellation and Refund policies.

There are new requirements to reverse Authorisation requests within given timeframes when a Transaction is not completed or where an estimated amount differs from a final Transaction amount. The aim is to help issuers to manage the open-to-buy/available balance of their Cardholders:

- If a Transaction is not completed, it must be reversed within 24 hours for Card-present Transactions and 72 hours for Card-absent Transactions;
- If the final Transaction amount is less than the authorised amount, the difference must be reversed within 24 hours for Card-present and 72 hours for Card-absent Transactions; and
- For estimated Transactions, if the final Transaction amount is less than the authorised amount, the difference must be reversed within 24 hours of check-out, disembarkation or rental return;
- These procedures may not be available on some devices. If you are unsure, please contact the Cardnet Helpline on **01268 567 100**.

Hotels and cruise lines are no longer allowed to make cash disbursements. This change reflects feedback from members which suggests that cash disbursements are no longer widely used at hotels and cruise lines.

Delayed or amended charge Transactions are replaced with delayed Transactions. Previously only hotels, car rental Merchants and cruise lines could charge for delayed or amended charges. By introducing delayed Transactions, a wider range of Merchants are permitted to process delayed Transactions. The Merchants are eligible for delayed Transactions (including damages) as

long as they have given proper prior disclosure to the Cardholder:

- Aircraft rental
- Bicycle rental
- Boat rental
- Car rental Merchants
- Cruise lines
- Equipment rental
- Lodging Merchants
- Motor home rental
- Motorcycle rental
- Trailer parks and campgrounds
- Truck and trailer rental

The above Merchants now have the ability to charge for damages by following the requirements for delayed Transaction charges. A delayed Transaction is defined as “A Transaction for goods, services or other charges that remain unpaid and for which a Cardholder has given prior consent to charge that Cardholder’s Account Number”. An eligible Merchant may only process a delayed Transaction within 90 calendar days of the rental return date, check-out date, or disembarkation date. Previously only car rental Merchants were permitted to charge for damages.

Referrals

Occasionally your Terminal may request that you call the Authorisation Centre. If this happens, call the Authorisation Centre on the telephone numbers detailed on page p111 as the Card Issuer may have grounds to suspect that the Transaction could be fraudulent.

The Card Issuer may ask you to relay some simple Cardholder identification questions or ask to speak to the Cardholder direct. If this happens please make sure that you take the telephone back from the Cardholder before the call is terminated so that you can check that the issuer is happy for the Transaction to proceed. The issuer will then give you an Authorisation code to enter into the Terminal. You must ensure that you only accept the Authorisation code from the operator, otherwise you could be liable if the Transaction is disputed at a later date. Any Transactions processed with an invalid Authorisation code may be charged back to you.

Referrals can occur for a number of reasons, for example, high value Transactions.

However, they do not necessarily reflect on the creditworthiness of the Cardholder.

Split sales with cash, cheque or second credit Card

If the total price for goods or services is equal to or exceeds your floor limit and payment is offered partly by Mastercard or Visa and partly by cheque, cash or any other method, Authorisation must be obtained for any part of the Transaction being paid for by Card-even if the Card amount is below your floor limit. The Authorisation Centre must be informed that the request for Authorisation is in respect of a split sale. They may require further details.

A single Card Transaction should never be completed as two or more Transactions on the same Card, as there is a high risk that you will receive a Dispute for these split sales.

If you have any questions or require guidance in relation to Authorisation issues, please ensure that enquiries are directed to the Cardnet Helpline on **01268 567 100**.

Cancelling a Transaction

If a Transaction has been processed in error or the Transaction amount changes you must, wherever possible, cancel the Transaction.

1. Cancel the Transaction: refer to the procedures in your Terminal operating instructions.
2. Receipt: give the Cardholder a copy of the cancelled receipt.
3. Cardholder's available credit: let the Cardholder know that they may need to contact their Card Issuer as the cancellation could affect their available credit.

Refunds

1. If you wish to provide a Refund, the Refund Transaction must be completed using the same Card as the one used for the original sale.
2. You may only process Refunds in respect of original sales. Failure to observe this could lead to settlement funds being withheld pending further investigation by us.
3. You must not make a Refund to a Card where the original sale was made by cash or cheque.
4. You should verify the Cardholder (for the Refund) in the same way you did for the sale.
5. If your Terminal indicates that a Manual Authorisation is required, you must telephone the Authorisation Centre.
6. You may only perform a Refund agreed on the telephone or in correspondence if you manually key enter Transactions. Please follow the manual key entry procedures in your Terminal operating Manual.

7. For Point of Sale Transactions you must enter the Card into the Terminal or swipe it. If the Terminal cannot read the Card, refer to the failed Transactions procedures in Section 9, 'Exceptions'.
8. You must sign the Terminal Sales Receipt, and make a note of the exchange and/or return of any items.
9. From April 2022 any Purchase Returns (Refunds) will incur a Scheme authorisation fee.

Remember: Authorisation is not a guarantee of payment. It confirms that the Card has not been reported lost or stolen at the time of the Transaction and that adequate funds are available.

FOR AUTHORISATION PLEASE TELEPHONE



01268 822 822

Point of Sale (Over the Counter)

01268 278 278

Card Not Present (CNP)

Lines are open 24 hours a day,
seven days a week.

If you have multi-currency or dynamic currency conversion facilities please call **01268 662 520**

Visa Digital Authentication Framework

The Visa Digital Authentication Framework (DAF) outlines an expanded set of capabilities and requirements to enable merchants to deliver frictionless shopping experiences while ensuring effective fraud management for E-commerce transactions.

Under the Digital Authentication Framework, Visa has developed a set of performance standards to help achieve outcomes comparable to face-to-face transactions. These requirements, which include defined rate thresholds for authentication success, authorization approvals and fraud, will be effective on 23 April 2022.

Requirements for Merchants

Merchant global fraud rate and monthly fraud amount must be below the thresholds outlined below.

Fraud rate 10bps

Monthly Fraud amount USD100,000

Fraud will be measured separately for transactions processed through the Visa Token Service or Visa Secure using EMV® 3-D Secure (3DS). Identification in the fraud program is based on an “AND” condition when both thresholds are exceeded.

The following conditions will apply when a merchant exceeds both thresholds outlined above.

- Month 1: Notification

Merchants will be contacted and acquirers will be sent an advice for their merchants when program thresholds have been exceeded in the previous month.

- Month 2-5: Monitoring Period

Merchants retain fraud dispute protection on DAF transactions during the Monitoring Period but are expected to show progress on reducing fraud if they want to maintain fraud dispute protection.

If fraud falls below the thresholds during the Monitoring Period, the merchant will exit the Monitoring Period.

- Month 6 and beyond: Enforcement Period (including loss of fraud dispute protection)

Enforcement applies when fraud exceeds both thresholds for 5 consecutive months.

A merchant may exit the Enforcement Period and regain fraud dispute protection by demonstrating three consecutive months of global fraud performance below the re-entry fraud rate threshold on all E-commerce transactions. The re-entry fraud rate is two times the fraud rate threshold (i.e., 20bps).

Requirements for Multi-Merchant Token Requestors

Multi-merchant token requestor global fraud rate and monthly fraud amount must be below the thresholds outlined below. Identification in the fraud program is based on an “AND” condition when both thresholds are exceeded.

Fraud Thresholds for Multi-Merchant Token Requestors:

Fraud rate 10bps

Monthly Fraud amount USD100,000

The following conditions will apply when a multi-merchant token requestor exceeds both thresholds outlined above.

- **Month 1: Notification**

Token requestors will be contacted when program thresholds have been exceeded in the previous month.

- **Month 2-5: Monitoring Period**

Merchants using the token requestor’s token retain fraud dispute protection on DAF transactions during the Monitoring Period, but token requestors are expected to work on reducing fraud.

If fraud falls below the thresholds during the Monitoring Period, the multi-merchant token requestor will exit the Monitoring Period.

- **Month 6 and beyond: Enforcement Period (including loss of fraud dispute protection for merchants using tokens from the token requestor) Enforcement applies when fraud exceeds both thresholds for five (5) consecutive months.**

A multi-merchant token requestor may exit the Enforcement Period and regain fraud dispute protection for merchants using their tokens by demonstrating three consecutive months of global fraud performance below the re-entry fraud rate threshold on all E-commerce transactions. The reentry fraud rate is two times the fraud rate threshold (i.e., 20 bps).

6 : Banking and reconciliation

Information on submitting electronic and paper data, record keeping, your Cardnet paper statement and the online reporting tool.

Electronic data

All electronic data sent to us must be in the correct format (any equipment approved by us will be in the correct format). If you use your own equipment or if you would like further information, please request a copy of the Electronic Submissions Guide by calling the Cardnet Helpline on **01268 567 100**.

Make sure that you complete your end of day banking procedures and submit your Transactions at agreed times to ensure you receive prompt payment for all Card Transactions.

For details of agreed times contact the Cardnet Helpline on **01268 567 100**. The Cardnet Helpline will be able to give Merchants details of their timescales.



Paper vouchers (for Transactions accepted when your Terminal is not working)

Preparing Point of Sale sales and Refund Vouchers for processing*

The Retailer Summary Voucher comes in three parts. The yellow and blue parts are the Merchant's copies and the white part is the processing copy, which you need to send to us for processing.

You must take the following steps:

- 1 Complete a Retailer Summary Voucher with a ballpoint pen.
- 2 List the amount of each Sales Voucher and the total in the spaces provided on the back of the Retailer Summary Voucher.
- 3 Prepare a separate listing if there is insufficient space on the summary.
- 4 Please do not use staples, pins or paperclips.
- 5 Do not batch more than 200 vouchers on one summary.
- 6 Complete the front of the summary set (the retailer copy) as follows:
 - Enter the total number of Sales Vouchers and total amount.
 - Enter the total number of Refund Vouchers and the total amount.
 - Enter the net total amount by deducting Refunds from sales.

- 7 Detach the bottom copy and assemble the documents in the following order:
 - Retailer Summary (processing copy).
 - Separate listing, if used.
 - Sales Vouchers (in the same order as listing).
 - Refund Vouchers.
- 8 Place in the envelope provided for submitting paper vouchers to Cardnet.
- 9 Retain the two top (yellow and blue) retailer copies of the Summary Voucher and keep with your copy of the Sales Vouchers.

*Paper Transactions are not permitted for Discover® Global Network cards or partner Cards on Point of Sale Transactions, neither are they allowed for UnionPay, JCB or Amex Transactions.

Paper Transactions are not permitted for Merchants processing Transactions through multi-currency or dynamic currency conversion facilities.

Preparing your Card Not Present Transaction Schedules for processing

Each Retailer Summary Voucher completed will result in a separate credit entry to your bank account. Your bank account will be credited once the vouchers have been processed by us. If the value of Refunds is equal to the value of Sales Vouchers, then no credit will be made to your bank account.

If you have insufficient Sales Vouchers against which to offset the Refund Voucher(s), complete a Retailer Summary (see page 115) and enter the details of the Refund(s).

The value of the Refund(s) should be enclosed by brackets, preceded by a minus sign to clearly indicate that the total is a negative value.

The Retailer Summary Voucher and the corresponding Refund Voucher(s) should be sent to Cardnet at the address detailed on page 118.

The value of Refunds will subsequently be debited from your bank account.

It is important that you submit the vouchers within the timescales given. If you do not, the Transactions may be rejected by the Card Issuers (even though the proper Authorisation procedures have been followed).

You must retain copies of all Summaries, Sales and Refund Vouchers for at least 13 months. This will assist you in checking your statement and resolving any possible Disputes. If you are unable to produce a copy of the relevant Summaries,

Sales or Refund Vouchers, the Transaction may be charged back to you. It is also essential to Cardnet, in the event that any summaries or vouchers are lost en route.

Sending your Point of Sale vouchers and Card Not Present Transaction Schedules to Cardnet for processing

All vouchers and Card Not Present Transaction Schedules must be posted to Lloyds Bank Cardnet, PO Box 22, Sheffield S98 1BG at the end of each business day.

Important

Do not send paper vouchers into Cardnet if a Transaction has already been processed through an electronic Terminal. If in doubt, please telephone the Cardnet Helpline on **01268 567 100**.

Record keeping

In order to help us to defend potential Disputes, see Section 7, 'Security, Disputes' (p120), on your behalf, you must keep copies of all Transactions for a minimum of 13 months after the completion of each Transaction.

A Transaction is only completed on the final delivery of goods or services.

- In certain circumstances we will ask you to provide us with Sales and Refund Vouchers within a limited time scale. This is because strict time limits for the supply of this information are enforced by each of the Card Schemes.

When we ask you for a copy of a Sales Voucher, the Card Issuer may only supply us with the Transaction date and Cardholder number. It is important that you store your sales slips carefully and in date order, so as to ease the retrieval process.

- If, for any reason, you are unable to provide copies of the requested information you may receive a Dispute for the Transaction in question. See Section 7, 'Security, Disputes,
 - Under no circumstances must you retain Card Security Codes (CSC) when accepting 'Card Not Present' (CNP) Transactions. Card Security Codes must be destroyed once the Transaction is authorised. See Section 4, 'Accepting Transactions' (p46).
 - All electronic Card data (such as information stored in the magnetic stripe) must be retained in a fully secure environment at all times.
- For detailed information on how to store Cardholder Receipts and electronic Card data, please see Section 7, 'Security, Storage of Cardholder information' (p121).

Your Cardnet statement

Each month we will make a Cardnet Merchant Statement available to you. The statement breaks down your Card Transaction information in ways that are designed to be of most value to you. Our aim is to give you as much detail as we can so that you are in complete control of your Card Transactions and business analysis.

We also provide you with a separate statement guide to help you understand and get the best out of the information provided. To view this guide, please visit lloydsbankcardnet.com/Content/pdf/Statement_Guide_Sterling.pdf

Please check all the details shown in the statement against your own records. If you have any queries about your Cardnet statement please contact the Cardnet Helpline on **01268 567 100**, or write, quoting your Cardnet Merchant number and statement month, to:

Cardnet Merchant Services
Janus House
Endeavour Drive
Basildon
Essex SS14 3WF

Online statements

You can access your Cardnet statement through our online reporting tools. For further details please contact the Cardnet Helpline on **01268 567 100**.

Online reporting tools

Cardnet offer more than one online reporting tool, with one specifically for multi-currency facilities and dynamic currency conversion facilities. Our online reporting tools are secure websites which will enable you to manage your Card payments through Cardnet, on line, 24 hours a day, seven days a week. As well as giving you access to your monthly statement, it also has the following benefits to enable you to manage your business on a day-to-day basis more effectively:

- Ability to view six months of Transaction data.
- Detailed Transaction information for credit, debit, Disputes and adjustments.
- A snapshot of your processing information including recent Transactions, adjustments and bank deposits.

Managing your Cardnet Merchant Account online provides the opportunity to eliminate paper statements and other costly processes. This will also mean a reduction in paper usage and a contribution to reducing your business carbon footprint.

If you would like to take advantage of our online reporting tools simply call the Cardnet Helpline on **01268 567 100** or visit lloydsbankcardnet.com/resources-and-faqs/downloads

Manage your Card
payments through
Cardnet, online,
24 hours a day,
seven days a week

7 : Security

This section explains the security procedures you need to follow.

Data security

The Card payment industry is concerned about the increasing incidents related to stolen Card and Cardholder information. These thefts have resulted in Merchants and financial institutions suffering fraud losses and unanticipated operational expenses, and, of course, significant inconvenience to Cardholders.

Storage of Cardholder information

The following information must not be stored after receiving Authorisation for a Transaction under any circumstances:

- Information stored in the magnetic stripe that facilitates Card processing.
- The Card Security Code (CSC) or CVC2 (the threedigit number indent-printed on the signature strip and used for Mail/Telephone Transactions orders or E-commerce Transactions, or the four digits on the front of an Amex card).

Only the information that is essential to your business, for example name, account number or expiry date, can be stored. This must be kept in a secure area limited to authorised personnel and the data masked or encrypted.

Destruction of Cardholder information

You must destroy (through incineration, cross shredding or crushing) any media containing obsolete Transaction data with Card holder information. This includes paper Transaction records, which should never be thrown intact into the public rubbish system.

Reporting a security incident

- In the event that Card Transaction data is accessed or retrieved by any unauthorised entity, you must notify us immediately.
- You must also follow your business continuity plan.

This will not only minimise risk to the Card payment system, but more importantly protect your customer. Systems and procedures are in place to stop the unauthorised use of compromised data, but are effective only when you do your part to promptly report a security incident.

Point Of Sale Terminal security

Please be aware that criminals have been targeting Point Of Sale equipment in order to commit counterfeit fraud overseas. It is important that you and your staff remain vigilant at all times and ensure that no one has the opportunity to tamper with your point of sale Terminal.

If you have cause to be suspicious about an approach from an unauthorised person, please contact the Cardnet Helpline on **01268 567 100** and your Terminal vendor/supplier.

Your Terminal vendor will always contact you first before sending an engineer to you.

We continue to work on your behalf to reduce Card fraud. This information is designed to give you a better understanding and awareness of these issues, which will help minimise risk and protect your customers.

Payment Card Industry – Data Security Standards (PCI DSS)

To protect your business, your customers (Cardholders) and the integrity of the payments system, the Card Schemes (Visa, Mastercard, JCB, UnionPay International, Amex and Diners) have introduced a set of requirements governing the safekeeping of account information, known as the Payment Card Industry Data Security Standard (PCI DSS).

Compliance with PCI DSS is mandatory and applies to all entities, and any third parties that may be used to store, process or transmit Cardholder data.

We need to let you know that if your business does not comply with these standards you could receive substantial fines from the Card Schemes (Visa, Mastercard, JCB, UnionPay International, Amex and Diners) if a compromise of Cardholder data occurs. These are based on the cost of issuing replacement Cards and related fraud losses.

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the PCI DSS are organised.

Build and Maintain a Secure Network	<p>Requirement 1: Install and maintain a firewall configuration to protect Cardholder data.</p> <p>Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.</p>
Protect Cardholder Data	<p>Requirement 3: Protect stored Cardholder data.</p> <p>Requirement 4: Encrypt transmission of Cardholder data across open, public networks.</p>
Maintain a Vulnerability Management Programme	<p>Requirement 5: Use and regularly update anti-virus software.</p> <p>Requirement 6: Develop and maintain secure systems and applications.</p>
Implement Strong Access Control Measures	<p>Requirement 7: Restrict access to Cardholder data by business need-to-know.</p> <p>Requirement 8: Assign a unique ID to each person with computer access.</p> <p>Requirement 9: Restrict physical access to Cardholder data.</p>
Regularly Monitor and Test Networks	<p>Requirement 10: Track and monitor all access to network resources and Cardholder data.</p> <p>Requirement 11: Regularly test security systems and processes.</p>
Maintain an Information Security Policy	<p>Requirement 12: Maintain a policy that addresses information security.</p>

Remember

When you engage agents or third parties (software houses, Payment Service Providers, web hosting companies, EPOS & till vendors):

- You must tell us about any agent or third party that engages in, or proposes to engage in the processing or storage of Card Transaction data on your behalf.

Important next steps to ensure your business is compliant

All Cardnet Merchants are mandated to validate their compliance with the PCI DSS.

Option 1: You can complete your own Self Assessment Questionnaire (SAQ) available from the PCI Council website at www.pcisecuritystandards.org

You will need to upload your compliant SAQ or PCI Security Standards Council (PCI SSC) accredited third party certificate of compliance onto the Cardnet merchant PCI DSS online portal at lloydsbankcardnetpcidss.com so we know that you are compliant.

Cardnet does not charge a fee for this.

Option 2: You can manage your compliance using our assisted online service at lloydsbankcardnetpcidss.com which provides your business with assistance and information to help you manage and report your PCI DSS compliance. This solution helps your business to understand which requirements are appropriate to your business and guides you through the appropriate Self Assessment Questionnaire (SAQ) for your needs. It's an ongoing service that will help your business to maintain compliance with the PCI DSS.

A monthly management fee will be charged for ongoing use of the online portal as set out in your Merchant Specific Conditions.

Option 3: Use Cardnet's proactive data security service Compliance Plus (eligibility conditions apply) for your PCI DSS compliance and payment security requirements. With this proactive service we'll help you with all your PCI compliance needs. The service includes the provision of a range of cyber security tools, as well as software patches and update guidance so your organisation stays secure.

A monthly management fee will be charged for the ongoing use of this service as set out in your Merchant Specific Conditions. Further details and more information about PCI DSS can be downloaded via the dedicated PCI Security Standards Council website: www.pcisecuritystandards.org

Non-Compliance charges

Whichever option you choose you have 3 months to report your compliance with the PCI DSS free of charge, commencing from when we write to provide you with your access details to the Lloyds Bank Cardnet merchant PCI portal.

You will be liable to a monthly non-compliance charge, as set out in your application form (currently per outlet), for any periods of non-compliance after the initial 3 month period.

Please note that validating your PCI DSS compliance does not guarantee that you will not suffer a data breach or be liable for a fine from the Card Schemes. It is your responsibility to remain vigilant and protect Cardholder data.

Compliance with the PCI DSS must be maintained at all times and validated on an annual basis.

The Standards themselves are subject to change from time to time to adapt to new security threats or market requirements.

Normally, validating your PCI DSS compliance will be easier in subsequent years and the time it takes for you to complete your compliance steps should reduce significantly.

Depending on how you accept Card payments, you may also need to undertake quarterly vulnerability scans. This is to support Merchants who have a point of sale device with an Internet connection, are taking Card Not Present Cardholder payments through a Virtual Terminal or hosting their own E-commerce payment pages.

A vulnerability scan is designed to be non-intrusive and ensures that your systems are protected from the threat of external threats (such as hacking or malicious viruses). Vulnerability scans may be requested at no extra cost through the Cardnet merchant PCI portal.

A list of Qualified Security Assessors is available at www.pcisecuritystandards.org

You can find out more information about our PCI DSS Compliance Management Service in our Frequently Asked Questions section:

www.lloydsbankcardnetpcidss.com/services/content/faq

Please note, if your business is taking more than six million Visa, Mastercard, Discover® Global Network or partner Card Transactions annually then you will need to validate your compliance with the PCI DSS using either a PCI Security Standards Council accredited Internal Security Assessor (ISA) or Qualified Security Assessor (QSA).

To find a QSA please go to

www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf

Further details and more information about the Standards themselves can be downloaded via the dedicated PCI Security Standards Council website: **www.pcisecuritystandards.org**

CARDNET HELPLINE



Call 01268 567 100

8am to 9pm Monday to Saturday

Call our knowledgeable UK-based team with any questions about Data Security, who can also provide you with a Key Facts Document regarding the PCI DSS.

Protecting your point of sale and Card processing equipment

To help all Card-accepting businesses better protect themselves and their customers this guide has been developed to help minimise the chances of being targeted.

Transactions with your chip and PIN Terminal

Chip and PIN has been highly successful in reducing certain types of fraud but criminals will always try to target shops and businesses in order to obtain Card details and PINs to commit fraud.

These guidelines complement Card industry rules and regulations and advice provided by Visa, Mastercard, UnionPay International, JCB, Amex and Discover® Global Network and point of sale equipment providers.

Why do criminals target Cards, Card details and PINs?

Fraudsters try to capture Card details and PINs in order to produce fake magnetic stripe Cards, which can then potentially be used in shops or cash machines that haven't upgraded to chip and PIN – mainly overseas.

Threats

Listed below are some of the main forms of attack in the shop environment:

Electronic attacks

These are attacks on the chip and PIN Terminal or the software used to process Card details. Criminals attempt to place illegal, data-capturing devices, bugging equipment or software in chip and PIN Terminals or install pinhole cameras, focused on a keypad, that record Cardholders' PINs.

Substitution attack

Fraudsters attempt to remove parts or all of the chip and PIN Terminal and substitute them with doctored or bogus devices that capture Card data or PINs. Criminals may attempt to install fake equipment by posing as service engineers.

Theft

Criminals may try to steal chip and PIN Terminals with the aim of gaining access to any stored data held in the device; learning about their inherent security features, or attempting to doctor the device prior to reinstalling it in a shop environment.

Members of staff

Criminals may target businesses by applying for jobs or coercing existing shop staff into helping them so they can access chip and PIN Terminals, install pinhole cameras or skim Cards through the use of handheld Card readers.

Keeping chip and PIN equipment safe and secure

Chip and PIN Terminals need to meet specific levels of security that are set by Visa, Mastercard, UnionPay International, JCB, Amex and Discover® Global Network and the UK Cards Association.

On top of this it is essential that the location where they are being used is physically secure and that the devices are safely looked after. The following guidelines can help keep chip and PIN equipment safe and secure.

Physical security of equipment

- The physical location of the chip and PIN Terminal and security of its parts should be considered. Can it be removed easily? Are the separate parts physically protected to prevent tampering or theft?*
- Chip and PIN Terminals should always be placed in a location that allows the Card holder to use them in a way that prevents other Cardholders from seeing the PIN. Where practical, Terminals should include PIN shielding.
- Secure cradles should be used to minimise opportunities for criminals stealing the Terminal.*
- CCTV should be used to cover the till area. Cameras must be fixed so that a Cardholder's PIN cannot be identified. Access to CCTV footage should be restricted to authorised staff and measures in place to ensure that it is not possible to interfere with the recordings.†
- Routines should be implemented to check the condition of chip and PIN equipment on a regular basis to ensure that it has not been tampered with. Checks should include an inspection of the cabling to ensure that nothing has been added.

- Only authorised personnel should be allowed access to chip and PIN equipment so always ask for identification and be very suspicious of any engineers turning up without prior arrangement.
- A process that oversees any changes to chip and PIN equipment – with appropriate audit trails – should be in place, especially where external suppliers provide maintenance checks.
- Employee application processes should include checking an applicant's work history and work record, as far as allowed by law.
- A documented security policy should be developed that is available to all staff and, where possible, responsibility for security matters should be allocated to a manager who can act as a single point of contact for all staff.
- Security training should be carried out to remind staff of their responsibilities at least annually (and more regularly where staff turnover is high). This training should be an integral part of the induction of new staff.

* Care must be taken to balance these security needs with the requirements of the Equalities Act 2010.

† See also the Information Commissioner's CCTV Code of Practice www.ico.gov.uk

- Staff should be made aware of all the potential ways that criminals target Card data and encouraged to report any issues or concerns they may have.
- Any security-related activities involving chip and PIN equipment should be carried out under the supervision of more than one employee or manager.
- Staff access to sensitive data should be managed accordingly. This includes staff who have no operational responsibility but have physical access to buildings (for example, staff not directly employed by your organisation – such as cleaning and maintenance staff).
- Staff who are approached or coerced by criminals into acting fraudulently should contact the police immediately.
- When employees leave the employment of an organisation it is important to ensure that all of their access rights and security related entitlements are revoked. In particular ensure that all keys are returned and that any physical access codes are changed so that they cannot subsequently enter secured areas.

Managing chip and PIN equipment

Chip and PIN Terminals are valuable assets and should be treated as you would the cash in a till. They should also be subject to good management routines.

- Merchants should devise an inventory to record the serial numbers of their Terminals and the location where they are installed (including replacements and spares).
- Regular checks should be carried out to ensure that these devices are where they should be and that any changes are authorised and noted in an asset management record.
- Shop managers should also have systems in place to review inventories and asset management records on a regular basis and have procedures in place when any inaccuracies are spotted.
- Where equipment consists of several different components, each part should authenticate itself to the Terminal – this may take the form of a regular heartbeat check. Any unusual events (such as missing heartbeats) should be flagged for supervisor attention.

Staff security

A standardised recruitment and vetting procedure, including criminal record checks, should be adopted that covers all employees (full time, part time, temporary and contract).

Suspicious Transactions

If you suspect something is wrong, or the Card checks you make show inconsistencies, then you must telephone the Authorisation Centre on 01268 822 822 and state that “This is a Code 10 Authorisation” then follow their instructions. If you have multi-currency or dynamic currency conversion facilities please call 01268 662 520.

Code 10 Authorisation must be sought in the following circumstances:

- The four digits on the signature strip on the back of the Card are different from the last four digits of the Card number on the front of the Card.
- The Card holder’s signature differs (if taken at the time of transaction) from that on the Card.
- The title on the Card does not match the Card holder’s.
- The signed name is not the same as that embossed on the front of the Card.
- The word void is visible on the signature strip or there is any indication that the strip has been tampered with.
- There has been any attempt to disguise or amend the signature.
- The Card is unsigned.
- The hologram is damaged or missing.
- There is no UV mark on the Card, see Section 3, ‘Checking the Card’ (p40).
- The Card has been mutilated in any way.
- You have any reason to be suspicious about the sale, the Card or the Card holder.

- The amount of the Transaction is significantly higher than normal for your business.
- Your Terminal requests that you call the Authorisation Centre.

You must hold on to the Card (and goods) and telephone the Authorisation Centre immediately on **01268 822 822** – you should not call the police unless instructed to do so by the Authorisation Centre.

When you make a Code 10 Authorisation you should have the following details ready:

- The Card number.
- The Card issue number (if applicable).
- Your Cardnet Merchant number.
- The exact amount of the Transaction, in pounds and pence.
- The Card expiry date.

You must tell the operator:

“This is a Code 10 Authorisation.”

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

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

*UnionPay International does not participate in the process of ringing a centre for an Authorisation code 10 call. UnionPay Transactions must be processed online.

Reward

If the Card Scheme participates in the reward scheme, a reward may be paid to any Cardnet Merchant who recovers a Card, when requested to do so by the Authorisation centre. The amount of the reward is dependent on the Card Scheme.

Recovering a stolen Card

After recovering a Card you should:

- Cut the bottom left-hand corner from the front of the Card.
- Attach both parts of the Card to a Cardnet Card Recovery Advice Form. You'll find two copies of the Card Recovery Advice Form in your Cardnet Starter Pack. For further copies, contact the Cardnet Helpline on **01268 567 100**.
- Return it to:

Cardnet Rewards Department

Merchant Operations
Janus House
Endeavour Drive
Basildon
Essex SS14 3WF

If the police ask for the Card recovered by you, you must:

- Allow the police officer to take it.
- Obtain the officer's name and police station.
- Obtain a receipt if possible.
- Inform Cardnet at the address above left.

Card Recovery Advice Form LLOYDS BANK CARDNET

Please use this form to return any cards reported. Remember – you could receive a reward!

Cardholder Name: S O D A B

PLEASE USE BOTH CARDS:

Report for Recovery Please tick (X) as appropriate

Cardholder Name: [Field]
 Last Name: [Field]
 Name: [Field]
 Number: [Field]
 Reported to Cardnet Authorisation Centre: [Field]
 Date of Recovery: [Field]
 Contact Telephone Number: Please tick (X) which card you have reported (you may prefer to contact your bank)

Address where card recovered: [Field]
 Home use: [Field]
 Business: [Field]
 Card not reported for recovery: [Field]

Card Issue Number: [Field]

Cardholder Name: [Field]

Card Expiry Date: [Field] Card Issue Number (if applicable): [Field]

IF POLICE HOLD CARD PLEASE STATE:

Police Station: [Field]
 Station Telephone Number: [Field]
 Police Officer: [Field]

Please attach the smaller copy of this form and the smaller corner of the card to the form.

Cardnet Rewards Dept, Merchant Operations,
Janus House, Endeavour Drive, Basildon, Essex SS14 3WF

Cardnet is an authorised member of the Lloyds Bank Group.
 Lloyds Bank plc, Registered Office: 25 Abchurch Lane, London EC4A 3DF
 Registered in England and Wales No. 2026067
 Please refer to the Cardnet Rewards Department for further information.
 Please note that this form is not valid for use in conjunction with the Cardnet Rewards Department.

CH5904 (09/13)

A Code 10 Authorisation should only be made if you are suspicious or if you have received instructions from Cardnet. You must not use a Code 10 Authorisation to validate Cardholder addresses or for Card Not Present Transactions.

How to guard against fraud

Point of Sale Transactions

Please make sure that all staff accepting payment by Card on your behalf have read and understood the following guidelines which aim to reduce the possibility of fraud.

These suggestions could help you to prevent fraudulent Transactions that could result in a Dispute to you.

- Be extra vigilant if you are presented with a Card that does not carry a chip as these are less secure and more likely to be used to perpetrate fraud.
- Ask yourself does the Card holder appear nervous/ agitated/hurried?
- Is the Card holder making indiscriminate purchases?
- The Card holder makes an order substantially greater than your usual sale, for example, your average Transaction is £40, but this Transaction is for £400.
- The Card holder insists upon taking the goods immediately, for example, they are not interested in free delivery, alteration or if the goods are difficult to carry.
- If a voucher is being used the Cardholder takes an unusual amount of time to sign and refers to the signature on the back of the Card.
- The Card holder takes the Card from a pocket instead of a wallet.
- The Cardholder repeatedly returns to make additional orders in a short period of time causing an unusual/ sudden increase in the number and average sales Transactions value over a one-to three-day period.
- Never transfer funds on a customer's behalf. Such Transactions (for example, on behalf of translators or couriers) are highly likely to be fraudulent.
- The sale is at an unusual time of day for your business.
- Do not under any circumstances Refund a payment in part or in full to a Card (or account) other than to the Card used to process the original sale.
- The Cardholder tells you that he/she has been having problems with his/her Card for payment where multiple Transactions are subsequently declined but eventually an Authorisation is obtained for a lower amount. (Most genuine Cardholders know how much available credit they have).
- A fraudster may present more than one Card, often to find a Card that will be successfully authorised. If this happens, take particular care and also look out for Cards presented, issued by the same bank, where the Card numbers are sequential or very similar. When in doubt, make a Code 10 call to the Authorisation Centre.
- Most floor limits are zero. However, if you have an electronic Terminal with a floor limit and you wish to reduce exposure to fraud, you may request a reduction to your Terminal floor limit. Not only will this reduce fraud but it may also reduce Disputes due to invalid Cards. Please contact your Terminal supplier to arrange this reduction.

- You should be on guard when chip and PIN Cards are presented and the PIN is blocked or the incorrect PIN is entered. You should check that this is the genuine Cardholder because you are at risk if you continue to proceed with a magstripe transaction.

Remember: If the appearance of the Card being presented or the behaviour of the person presenting the Card raises suspicion, you must call the Authorisation Centre on **01268 822 822** and state “This is a Code 10 call” and follow the operator’s instructions.

Please note – not all Card schemes participate, e.g. UnionPay International does not participate in this process, all UnionPay Transactions should be processed online.

Registering business logos with Mastercard

Mastercard have launched a secure portal where you can enter your business logo and other business information which is used to improve your customers experience and support them in recognising your transactions, minimising disputes. Please refer to the Logo Microsite, available at logo.ethoca.com

Mastercard PSD2 Optimization Program

The Mastercard PSD2 Optimization program aims to optimize approval rates of electronic commerce (E-commerce) transactions that are subject to Payment Service Directive 2 (PSD2) by helping ensure adherence to Identity Check program requirements and other Standards.

The Mastercard timeline for soft decline retry rate targets:

From 1 February 2022 60 percent of soft decline retry rate will become effective.

From 1 June 2022 80 percent of soft decline retry rate will become effective.

To satisfy the SCA requirements under PSD2, customers are required to use the EMV¹ 3-D Secure (3DS) authentication protocol or any other SCA compliant method.

¹EMV is a registered trademark or trademark of EMVCo LLC in the United States and other countries.

AUTHORISATION CENTRE



Call **01268 822 822**

State “This is a Code 10 call” and follow the operator’s instructions.

Call **01268 662 520** if you have multi-currency or dynamic currency conversion facilities.

Counterfeit Cards

Chip and PIN Cards have reduced this type of fraud as most cases of counterfeit fraud involve 'skimming' or 'cloning'. This is where the genuine data in the magnetic stripe on one Card is electronically copied onto another Card without the legitimate Cardholder's knowledge. This type of fraud can be identified by checking that the Card number printed on the voucher is the same as that embossed on the front of the Card. If these numbers differ, call the Authorisation Centre immediately on **01268 822 822** stating "This is a Code 10 Authorisation".

To help avoid receiving Disputes as a result of counterfeit fraud and disputed key entered Transactions, follow the 'Failed Card Swipe Procedure', see Section 9, 'Exceptions'.

Card Not Present (CNP) fraud

Card Not Present fraud occurs when fraudulently obtained Card details are used to order goods by telephone, mail order or electronically such as over the Internet.

If the goods that you sell can be easily resold such as computers, TV and hi-fi equipment, you may be especially vulnerable to being targeted by fraudsters using fraudulent or stolen Cards. You should be particularly suspicious of unusually high value or bulk purchase Transactions from new customers.

The Card Security Code (CSC) and Address Verification Service (AVS) will help you decide whether to progress with a Transaction. See Section 4, 'Accepting Transactions, Card Not Present Transactions' (p50). Please do not use the Code 10 Authorisation facility to undertake address checks.

Important

Under no circumstances can goods purchased by mail or telephone be handed Point of Sale to, or collected by, the Cardholder.

If a Cardholder wishes to collect the goods, then they must attend your premises in person and produce their Card. Any Sales Voucher already prepared must be destroyed and an Point of Sale Transaction processed. If you have already completed a CNP order you must either cancel the Transaction or perform a Refund. If you perform a Refund, please let the Cardholder know that the original Transaction, a Refund and the Point of Sale Transaction will all appear on their Card statement.

There are a number of extra checks you can make to help make sure you are dealing with a genuine Cardholder including:

- Use Visa Secure, Mastercard Identity Check, Diners Club International®, Discover® ProtectBuy and American Express SafeKey® for E-commerce Transactions. See Section 4, 'Accepting Transactions'.
- For business Cardholders not known to you, check their details in your local business directory or Internet search engine.
- Private Cardholders' addresses not known to you can be checked against the Electoral Register, telephone directory, from a BT CD-ROM phone disk or Internet map searches.
- Obtain a telephone number for the Cardholder's address using a Directory Enquiry Service, if possible, and telephone the Card holder back on that number to confirm the order (not necessarily straightaway).
- Be aware if the Card holder is suggesting unusual arrangements such as going back for another Card number if the one given is refused.
- Check your records to see if you have had a number of Transactions over a short period of time from a company or individual with whom you have not had any previous dealings.
- Also check to see if there are any unusual features or consecutive sequences in the Card numbers given over a period. (Usually fraudsters will offer Card numbers that are the same except for the last four digits. This could mean that a batch of Cards has been stolen).
- Be especially wary if the delivery or Cardholder's address given is overseas and products purchased are readily available in that locality.

Also be particularly wary of:

- Demands for next day delivery.
- Alterations of delivery address at short notice.
- Phone calls on the day of delivery asking what time the goods are due to be delivered.
- Multi-tiered address for example, units, flats.

Danger signals

If any of the following happen, we recommend you make extra checks. This list does not cover every eventuality – some fraudsters spend a long time building up credibility and then request an extremely large order that is 'too good to be true'.

- Is the sale almost too easy? Is the caller disinterested in the prices/precise details of the goods, particularly if it is a new customer? Is the stock ordered of high value or easily resold merchandise?
- Is the sale excessive in comparison with your usual orders? Is the Cardholder ordering lots of different items? Does the spending pattern fit your average customer?
- Is the customer giving you a third party's Card number, claiming to be acting on behalf of a 'client'?
- Does the caller match the Card? Do not accept orders from someone quoting someone else's Card details, for example, a woman using her husband's Card or a business using a personal Card. It may well be a genuine call, but it pays to check.

- Never split an order to avoid Authorisation, or at the suggestion of the Cardholder – for instance, if they offer two Card numbers to cover one order.
- Is the caller suggesting any unusual arrangements? For example, “if the Card number I’ve given you doesn’t have sufficient funds let me know and I’ll give you another number”.
- Is the caller being prompted by a third party whilst on the telephone?
- Does the caller seem to have a problem remembering their home address or telephone number or do they sound as if they are referring to their notes?
- Does the Cardholder seem to lack knowledge of their account?
- Is the Card Issuer/building society based overseas?

Please remember you remain ultimately responsible should a Transaction be confirmed as invalid or fraudulent, even if the AVS and CSC data matches and an Authorisation code is given.

Delivery warning signals

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

- Goods should not be released to third parties such as ‘friends’ of the Cardholder, taxi drivers, chauffeurs, couriers or messengers. (However, third party delivery of relatively low value goods such as flowers is appropriate).
- Insist that goods may only be delivered to the Cardholder’s permanent address. If you agree to send goods to a different address, take extra care and always keep a written record of the delivery address with your copy of the Transaction details.
- Don’t send goods to hotels or other temporary accommodation. Only send goods by registered post or a reputable courier and insist on a signed and dated delivery note.
- Be wary of sending goods abroad that may be readily available in the buyer’s local market.

Couriers should be instructed:

- To make sure the goods are delivered to the specified address and not given to someone who ‘just happens to be waiting outside’.
- To return with the goods if they are unable to effect delivery to the agreed person/address.
- Not to deliver to an address which is obviously vacant.
- To obtain signed proof of delivery, preferably the Cardholder’s signature.

Other important fraud considerations

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

Do not, under any circumstances, process Transactions for any business other than your own. Some fraudsters offer commission to process Transactions while they are awaiting their own credit Card facilities or where they have not been successful in obtaining their own. If you process Transactions on behalf of any other business/person you will be liable for any Disputes and could put your own Cardnet facility at risk.

Fraud prevention

Transaction laundering

If you are approached with a proposal to buy Card Transactions, you must contact us immediately on **01268 567 100**. This is a form of money laundering and is contrary to the terms of your Agreement.

Phishing emails

If you receive an email from somebody claiming to be a bank or an official business asking for Transaction details of all Cards recently accepted for payment, you must report this to Cardnet straight away on **01268 567 100**. This is a fraud tactic to obtain Card details. A bank or any other official business would never make contact in this way to request Card information.

Fraud prevention programmes

Some businesses are more prone to fraud than others and you may be unfortunate enough to suffer a fraud attack, particularly if you offer goods that are attractive to fraudsters and can be easily, but illegally, resold.

It is your responsibility to protect your business from financial loss. It is also imperative that you and any staff that you employ follow the contents of this Manual carefully at all times.

If you are concerned that you may be vulnerable to fraud attack, perhaps because of your business location or local intelligence, please contact the Cardnet Helpline and ask to speak to our Fraud Department who will be happy to help with guidance on best practice.

Please remember – following the procedures contained in this Manual is no guarantee that you will avoid incurring financial loss if you suffer a fraudulent Transaction. You will remain ultimately responsible for any financial loss you incur as a result of any fraudulent Transaction.

Further information on fraud prevention can also be found at **www.financialfraudaction.org.uk** as well as in literature for staff awareness.

Disputes

A Cardholder, or the Card Issuer has the right to question/ dispute a Transaction. Requests for a copy of the Transaction can be received up to 180 days after the Transaction has been debited to the Card holder's account and in some circumstances beyond 180 days.

The following section describes the procedures which you must follow together with suggestions which will help you reduce the risk of Disputes being debited from your account.

Remember, you may be liable for a Dispute in some circumstances even if you obtained Authorisation for a Transaction, and followed all of the processes and procedures in this Manual and your Agreement with us.

Retrievals

In many cases, before a Dispute is initiated, the Card Issuer requests a copy of the sales slip, via a 'retrieval request'. Once a retrieval request is received from the Card Issuer, we will respond by sending a copy of the Transaction, if available.

Where you hold Terminal receipts for electronically processed Transactions or E-commerce authentication data, it is your responsibility to respond to all retrieval requests received from Cardnet within 10 calendar days of our initial request. You are responsible for retaining and providing copies of Transactions for a minimum of 13 months from the original Transaction date.

Please mail your responses to Cardnet:
Cardnet Merchant Services, Janus House, Endeavour Drive,
Basildon, Essex SSI 4 3WF.

We recommend recorded delivery or registered post when you send us evidence of high value Transactions.

If you fax your response, please set your fax machine to print your fax number and name on the documents you send.

We can use this information to contact you in the event the transmission is not clear or complete. Also, when using the fax machine, please set the scan resolution on the machine to the highest setting. The higher resolution setting improves the clarity of characters and graphics on the sales documents transmitted and helps reduce Disputes for illegible copies.

If you prefer to email your documents, please email to:

CardnetChargebacks@firstdata.com

If Cardnet does not receive a clear legible copy of the sales slip within 10 calendar days of the initial retrieval request you may be subject to a Dispute. However, the potential liability remains with you if the item is not supplied in time and you may become liable for the Dispute simply by failing to meet the payment scheme time frame.

Disputes for 'non-receipt of requested item' cannot be reversed unless the requested documentation is provided within 10 calendar days of the initial request.

Please remember: Due to time frames imposed by Mastercard, Visa, UnionPay International, JCB and Discover® Global Network it is extremely important that you respond to/resolve a retrieval request or Dispute enquiry immediately. The more information we have at the time of the retrieval request or Dispute, the better we can dispute the item on your behalf.

We recommend that when you send a copy of a Transaction, you send all the relevant documents (for example, till receipt together with any supporting invoices/sales tickets) as evidence of the Transaction including any documents signed by the Cardholder. In the case of Card Not Present (CNP) Transactions, details of the goods ordered together with evidence of delivery, for example, a signed delivery receipt, should also be sent.

Dispute/reversal procedure

When we receive a Dispute from a Card Issuer we will normally debit your bank account and let you know accordingly. Our letter will provide details of the Transaction in dispute, together with the information/documentation required from you. Our letter will also tell you the latest date by which you must reply with the information/documentation needed.

If the information provided is:

- a. sufficient to warrant a reversal of the Dispute and
- b. within the applicable time frame

we will defend (reverse) the Dispute, if possible, but reversal is dependent upon the Card Issuer's agreement. A reversal is not a guarantee that a Dispute has been resolved in your favour. If the Dispute is reversed, the Card Issuer has the right to present the Dispute a second time and your account will be debited again if you have not complied fully with the terms of your Agreement and this Manual.

Please refer to the situations described in the table detailed on pages p138 to p139 which highlight the common reasons for Disputes and how they can be avoided. In the majority of cases, where the Cardholder is present, you can reduce your exposure to Disputes by following the guidelines in the table.

We will do our best to help you to defend a Dispute. However, due to the short time frames and the supporting documentation necessary to successfully (and permanently) reverse a Dispute in your favour, we strongly recommend you take the following steps to reduce your Dispute risk:

- Convert or upgrade your Point of Sale Terminal to accept chip and PIN Transactions electronically.
- Ensure Transactions are completed in accordance with the terms of your Agreement/Manual.
- If you do receive a Dispute, always investigate and send in the appropriate documentation within the required time frame.
- Whenever possible, contact the Cardholder directly to resolve the inquiry/dispute but still comply with our request for information just in case this does not fully resolve the matter.
- If you take payments from credit and debit Card holders over the Internet we recommend that you introduce Visa Secure, Mastercard Identity Check, Diners Club International®, Discover® ProtectBuy and American Express SafeKey® for your Transactions. Mastercard Identity Check is mandatory for accepting Maestro and International Maestro.

Common causes and reasons for Disputes

Reason	How to reduce your Dispute risk
The Card account number indicates that it has chip and PIN capability but is subsequently found to be fraudulent.	<ul style="list-style-type: none"> ▪ Upgrade your Point of Sale Terminal to chip and PIN capability
Refund not processed – the Cardholder is claiming that a Refund Voucher or Refund acknowledgement issued by you was not processed.	<ul style="list-style-type: none"> ▪ Ensure proper disclosure of your Refund policy is on the Transaction receipt, for example the words 'NO EXCHANGE, NO REFUND' must be clearly printed on the Sales Voucher or Terminal receipt ▪ Process Refunds immediately ▪ Refunds must be applied to the same Cardholder account as the original sale ▪ Do not issue in-store or merchandise credit ▪ Do not issue a cash or cheque Refund, if the original Transaction was made by Card
Transaction not authorised.	<ul style="list-style-type: none"> ▪ Authorise all Transactions which are equal to or above your floor limit and use the proper method of Authorisation ▪ Clearly write the Authorisation number on your paper vouchers
Non-receipt of goods – Cardholder is claiming they did not receive the goods or goods were paid for by other means.	<ul style="list-style-type: none"> ▪ Do not process a Transaction until the goods are dispatched ▪ Do not process any Card Transaction where the Cardholder has already paid for the goods or services using another method of payment ▪ Obtain the Cardholder's signature on your delivery note
Card used before effective date or after expiry date.	<ul style="list-style-type: none"> ▪ Carefully examine the Card for the effective start and expiry dates when accepting it for a Transaction ▪ Do not process a Transaction prior to the effective date appearing on the Card ▪ Do not process a Transaction after the expiry date appearing on the Card
The Merchant fails to respond to requests for a copy of the sales slip.	<ul style="list-style-type: none"> ▪ Prepare clean, legible sales slips at the point of sale and store in a secure and orderly fashion so that you are able to respond to retrieval requests within the required time frame ▪ To identify a Transaction you will be given the Cardholder number, date and amount of the Transaction. (Card Issuers are not obliged to supply Cardholder names or addresses so it is important that you store your records carefully)

Common causes and reasons for Disputes (continued)

Reason	How to reduce your Disputes risk
<p>Cardholder did not authorise the Transaction (primarily CNP Transactions).</p>	<ul style="list-style-type: none"> ▪ Mail/Telephone Transactions – follow the recommended procedures in Section 4, 'Accepting Transactions', Card Not Present (CNP) Transactions ▪ E-commerce Transactions – Visa Secure, Mastercard Identity Check, Diners Club International®, Discover® ProtectBuy and American Express SafeKey® to authenticate payments. See Section 4, 'Accepting Transactions', pages p59 and p60.
<p>Non-matching account number – this is where a Transaction has been processed on a non-existent Card account. By way of example, it is possible that a Card has been created by a fraudster or that an existing Cardholder's account details have been 'skimmed', i.e. copied on to another Card.</p>	<ul style="list-style-type: none"> ▪ If you use an electronic Terminal, the chip Card must be inserted into the Terminal or, if you do not have a chip Terminal, swipe the Card through the swipe slot and ensure the displayed Card number matches the number on the Card ▪ Alternatively, you can compare the Card number with the number on the sales slip produced by the Terminal ▪ If the chip or magnetic stripe cannot be read, for example, failed read or the Terminal is inoperable, follow procedures in Section 9, 'Exceptions' ▪ Carefully examine the front and back of the Card at the time of the Transaction. Follow the procedures in Section 3, 'Checking the Card' ▪ Check the signature ▪ Telephone Transactions – confirm the account number provided by the Cardholder by repeating the number back to them ▪ Properly authorise all Transactions
<p>Transaction was processed more than once to the same Cardholder.</p>	<ul style="list-style-type: none"> ▪ Settle and reconcile batches of sales and Refunds on your Terminal/register daily. Ensure that the total amount submitted (displayed on Terminal) balances with/matches to the Card Receipts. See your Terminal operating instructions
<p>Sales slip was not imprinted. The sales slip provided was not imprinted using a manual imprinter machine nor was the Card or magnetic stripe read (for example, the Transaction was key entered into your Terminal and the Cardholder denies participation in the Transaction).</p>	<ul style="list-style-type: none"> ▪ If you are unable to read a Card through your Terminal or capture the Cardholder's information via the magnetic stripe, you must imprint a Cardnet Sales Voucher with the Cardholder's card to prove the Cardholder was present at the time of the Transaction ▪ Manually key entering the information into the Terminal does not protect you from this type of Dispute. See Section 9, 'Exceptions' ▪ If you need an imprinter these can be purchased by calling the Cardnet Helpline on 01268 567 100

A Transaction will also be regarded as invalid and may be charged back to you if:

- The signature (if taken at the time of transaction) is incompatible with the signature on the Card.
- The Sales Voucher sent to Cardnet differs from the Cardholder's copy.
- The Card is not yet valid, or has expired at the time of the purchase.
- You have been advised that the Card is void.
- The sale is equal to or exceeds your floor limit and Authorisation has not been obtained.
- The Sales Voucher is incomplete -for example, it is unsigned, has not been imprinted, is not dated, or the Authorisation code obtained is not quoted on the voucher.
- The Sales Voucher is completed for an illegal Transaction.
- Two or more vouchers have been made out for a purchase which exceeds the floor limit.
- You have in any way failed to comply with this Operating Manual or are otherwise in breach of your Agreement with Cardnet.
- The correct Authorisation telephone number was not used.
- You are unable to provide a copy of the Transaction proving that the Card holder authorised the sale.
- There was a delay in presenting the original Transaction and it is then disputed by the Cardholder/Card Issuer.
- The goods or services have not been supplied, or are defective or not as described.

- The voucher was not sent to Cardnet for processing on the day of the Transaction and consequently rejected by the Card Issuer for late presentation to the Cardholder's account.
- It is clearly evident that the Transaction was made with a counterfeit Card.
- For any reason you process a Transaction on the same Card number that has failed both chip/PIN and magnetic swipe.
- The Transaction in respect of which the Sales Receipt was issued is for any reason illegal or of no legal effect.
- The Cardholder denies having authorised the Transaction and you are unable to provide evidence satisfactorily to the Bank that the Transaction was authorised.
- The Transaction is a Card Not Present sale and is disputed by the Cardholder and/or Card Issuer.

Please note

Authorisation does not confirm the identity or authority of the Cardholder and therefore is not a guarantee of payment. It confirms that the funds are available on the account and that the Card has not been reported lost or stolen at that time.

Please remember, due to the time frames imposed by Mastercard, Visa, UnionPay International, JCB, Maestro and Discover® Global Network it is extremely important that you respond to/resolve a retrieval request or Dispute enquiry immediately. The more information we have at the time of the retrieval request or Dispute, the better we can dispute the item on your behalf.

For further information about reducing your Dispute risk, contact the Cardnet Helpline on **01268 567 100**.



What customers want

With Cardnet you can offer more services like Cashback, mobile phone top-up and foreign currency Transactions.

8 : Additional facilities for you and your customers

Cardnet offers more than just quick
and convenient payments.

You can offer your customers more with these additional facilities, available with prior written agreement from Cardnet.

Purchase with Cashback*

Provided you have received written agreement from Cardnet you may, when presented with a Visa Debit, Debit Mastercard, Maestro or V PAY Card as a means of payment, offer the Purchase with Cash back service.

Complete the Transaction the same way as a standard purchase, but you must also take the following additional steps:

- 1 Cashback: can only be provided in conjunction with a purchase. The cash amount should be entered in accordance with your Terminal operating instructions. This amount must not exceed your cash ceiling limit. (Your cash ceiling limit is the maximum amount of cash you can provide as part of a Purchase with Cashback facility.)
- 2 Authorisation: all Purchase with Cashback Transactions must be authorised.
- 3 Charges: you are not permitted to charge Cardholders for the Cashback service.
- 4 The Cashback amount and total Transaction amount (retail purchase plus Cashback amount) must be shown separately on the Transaction receipt.
- 5 Electronic Authorisation must be sought on all Transactions with Purchase with Cashback. Cash must not be dispensed if Fallback procedures have to be used.

Mobile phone top-up*

Electronic mobile phone top-ups are available on selected Terminals, enabling you to top up your Cardholder's mobile phone.

E-Top-Up

E-Top-Up is the electronic system that allows a mobile phone user to top up their phone through a Terminal using a plastic Card. The Cardholder's network provider or a Merchant offering the service will have supplied this Card. The Card is linked to their mobile phone.

Making an E-Top-Up Transaction

- Cardholder pays you by cash, cheque or debit/credit Card.
- Your Cardholder's top-up Card is swiped through the Terminal.
- The amount they wish to top up should then be entered into the Terminal.
- The top-up amount is automatically added to their mobile phone.

* Purchase with Cash back and mobile phone top-ups are not supported by Discover® Global Network or partner Cards.

E-Voucher

E-Voucher allows prepay mobile users to top up their mobile phone, even if they don't have a swipe Card.

Making an E-Voucher Transaction

- Choose the network via the Terminal menu and the desired top-up amount using the designated function keys. (These will be detailed in the user Manual supplied with your Terminal).
- An E-Voucher will then be printed out in the form of a receipt.
- The Cardholder then pays you and you hand the E-Voucher to the Cardholder.

The Cardholder then calls the Interactive Voice Response (IVR) number as detailed on their receipt and enters their unique PIN, also printed on their receipt. This will then top up the Cardholder's mobile phone.

At the end of the day you simply print out the end of day report from the Terminal and this shows you the amount of E-Top-Ups and E-Vouchers you have sold.

This service could help you generate extra revenue through commission. If you are interested in this service call the Cardnet Helpline on **01268 567 100** for further information.

Recurring Transactions

If you want to set up Recurring Transactions to charge a Cardholder's account periodically (for example for monthly insurance premiums, yearly subscriptions, annual membership fees, etc.), you will need Our written approval.

Recurring payments can be accepted on Visa Debit, Visa Credit, Debit Mastercard, Mastercard Credit, Maestro, Diners Club International®, Discover®, BC Global, Troy Global, RuPay Global, and Elo Global cards. Recurring transactions is also available on American Express.

To ensure that you comply with current Card Scheme regulations and your Cardholders' requests, please remember to follow these requirements at all times.

You must:

- Ensure that clear contact details are available for Cardholders to amend or cancel payments and that their instructions are carried out properly. You should also ensure that the Cardholder understands the ongoing nature of the commitment they have taken.
- Obtain an Authorisation for every Recurring Transaction.

You must not:

- Include partial payments for goods or services purchased in a single Transaction.
- Accept instructions for Recurring Transactions on V PAY cards.

- Impose a finance charge in connection with a Recurring Transaction.
- Complete a Recurring Transaction after receiving a cancellation notice from the Cardholder or Card Issuer. If a request for Authorisation has been declined or if a previous Transaction using an existing Card holder instruction has resulted in a Dispute to you, you must approach the Card holder to obtain a new authority.
- Key enter a Recurring Transaction into a point of sale Terminal. You will need a software solution from one of our approved third party Payment Service Providers (PSPs) to manage these payments on a recurring basis. Please contact your chosen PSP to see if they can support this service.

Best practice for Recurring Transaction Merchants is to obtain a written authority from the Cardholder for the goods or services to be charged to their account. In the case of E-commerce Merchants, the authority should be contained within the website and an electronic or hard copy held. If you offer a free trial period, there are specific requirements to follow. Please contact Cardnet to discuss.

The written authority signed by the Cardholder must at least specify:

- The Transaction amounts.
- The frequency of recurring charges.
- The duration of time for which the Cardholder's permission is granted; however, this must not exceed one year.

If the Recurring Transaction is renewed, the Cardholder will need to complete a new authority for the continuation of such goods or services to be charged to their account.

Recurring Transactions are a convenient way to collect payments but they can be a source of Cardholder disputes.

To address some of these concerns, both Visa and Mastercard have introduced solutions which enable Merchants to validate and update the historic Card details they have on file.

These solutions are known as Visa Account Updater (VAU) and Mastercard Automatic Billing Updater (ABU). There is no equivalent solution for Discover® Global Network or partner Cards.

How do VAU and ABU work?

Transactions are submitted by Merchants through our approved third party PSPs to the Card Schemes for validation and checking. Through this validation, you can clearly see when a new Card number has been issued, when an account has been closed or when the Card holder has asked for a payment to be terminated. You can then update the Card details you have on file and proceed with Authorisation of the Transaction.

VAU and ABU can help increase your Recurring Transaction approval rates and improve Cardholder satisfaction.

Gratuities

The Transaction amount may be changed in order to add a gratuity if:

- You have been authorised by Cardnet to do so.
- Your Terminal provides this function.
- The Cardholder has given permission.

Dynamic Currency Conversion (DCC)

With DCC you can offer more choice and flexibility to your international customers. They can choose to pay you in their own currency using Visa, Mastercard and Discover® Global Network.

Your customers will be shown the price in Sterling and their own currency, along with the exchange rate used, at the point of sale. Your Terminal is automatically updated with exchange rates so you don't need to continually amend your pricing when rates fluctuate.

Commission is normally paid to you for every DCC Transaction you process.

Call the Cardnet Helpline on **01268 567 100** to find out more about DCC for your business.

With DCC you can offer more choice and flexibility to your international customers. They can choose to pay you in their own currency using Visa, Mastercard, Discover® Global Network and partner Cards.

Accepting currency Transactions

We can help you trade more easily with overseas customers by accepting payments in different currencies. Cardnet supports a wide range of Transaction currencies and funding options, which can be tailored to suit your business.

Call the Cardnet Helpline on **01268 567 100** to find out more.

Cash Advance

The Cash Advance facility is available to Bureaux de Change Merchants only. This facility allows you to accept Cards to dispense travellers cheques, foreign currency, travel money Cards and money orders.

There are specific requirements for these types of Transactions. For example, secondary identification. If you are interested in this facility, please contact the Cardnet Helpline on **01268 567 100**.

Additional Cards

In some instances you may need to apply for acceptance facilities direct with the schemes and confirm that your Terminal is able to support them also.

9 : Exceptions

How to proceed when your Terminal
is unable to read the chip or
magnetic stripe.

Exceptions

Most of the Cards presented to you that are chip read or swiped will process without any problems. However, if there are occasions when your Terminal is unable to read the chip or magnetic stripe, please ensure you follow these procedures.

To help reduce losses through fraud and Chargebacks, the table below shows you at a glance the action you need to take for the following Card types for failed chip read and magnetic stripe Transactions:

- | | |
|----------------------|------------------------------|
| ■ Visa Credit. | ■ Diners Club International. |
| ■ Visa Debit. | ■ Discover. |
| ■ Mastercard Credit. | ■ BC Global Card. |
| ■ Debit Mastercard. | ■ Troy Global Card. |
| ■ Maestro. | ■ RuPay Global Card. |

	Revert to mag-strip*	Revert to PAN key entry
Chip Cards unable to read	✓	✗
Magnetic stripe Cards unable to read mag-stripe	N/A	✓†

The following guide shows you at-a-glance the action you need to take for the following Cards:

- Internationally issued Maestro.
- Visa Electron.

	Revert to mag-strip*	Revert to PAN key entry
Chip Cards unable to read	✓	✗
Magnetic stripe Cards unable to read mag-stripe	N/A	✗

There is no Fall back action for V PAY. If the chip cannot be read, please ask for an alternative method of payment.

UnionPay Transactions – Cards must be chip read initially (if chip on the Card), and magnetic stripe transactions and PAN key entry are permitted but no paper voucher processing is permitted.

JCB Transactions – Cards must be chip read initially (if chip on the Card) and if this fails, magnetic stripe Transactions and PAN key entry are permitted, but no paper voucher processing is permitted.

If you have multi-currency or dynamic currency conversion facilities, paper-based Fallback actions do not apply. If the Card cannot be read, please ask for an alternative method of payment.

*When swiping a Card through the Terminal, you may be prompted to key enter the last four digits of the number embossed on the front of the Card. The Terminal will then check these numbers against those held in the Card's magnetic stripe.

† Ask the Card holder for an alternative method of payment or key enter the Transaction into the Terminal and take an imprint of the Card for your records.

Failed chip Card read

- 1 If the Card offered contains a chip, the Card must be entered into the Terminal. If for any reason, the chip on the Card cannot be read, where permitted, you may revert to the magnetic swipe method.
- 2 After three unsuccessful attempts to swipe the Card, your Terminal will indicate that it has not been possible to read the magnetic stripe on the reverse of the Card. If the Card is still unable to be read you must request an alternative source of payment.

Please note: if you swipe or key enter a chip Card and the Transaction is later found to be fraudulent, the Transaction may be charged back to you.

Failed magnetic stripe Transactions – key entry (excluding internationally issued Maestro, Visa Electron and UnionPay cards)

- 1 After three unsuccessful attempts to swipe the Card, your Terminal will indicate that it has not been possible to read the magnetic stripe on the reverse of the Card.
- 2 Check the Card by following the step-by-step instructions in Section 3, 'Checking the Card' (p40). Only when you are satisfied with all checks, should you proceed to key enter the Card details.
- 3 You must manually key enter the Card details in accordance with your Terminal operating instructions, ensuring they have been entered correctly.

- 4 Once you have key entered the Transaction details, you must ask the Cardholder to sign the Terminal Sales Receipt and check that the signature matches the one on the reverse of the Card.
- 5 When key entering the Card number into a Terminal it is necessary to take an imprint of the Card and obtain a signature on the Terminal receipt in order to be able to prove (if required) that the Card and Card holder were both present at the time of the Transaction. Do not take a photocopy instead of an imprint as this will not be sufficient proof that the Card was present and could result in a Dispute.
- 6 Using a standard Sales Voucher and imprinter, take an imprint of the Cardholder's Card.
- 7 Complete the Sales Voucher with the amount of the Transaction and record the Terminal Sales Receipt number in the Quantity and Description box. Finally, write clearly across the left-hand side of the Sales Voucher, the words 'FAILED ELECTRONIC SWIPE'.

Do not ask the Card holder to sign the Sales Voucher. This is not required as the Terminal Sales Receipt is the only item that requires a signature.
- 8 Explain to the Card holder why this process is taking place and reassure them that the Sales Voucher will not be banked but will be held as a record which will be produced to Cardnet if the Transaction is disputed. (If, in conversation, it transpires that the Card holder is suffering recurring 'Card read' problems it would be helpful to suggest they contact their Card Issuer). If you feel that there may be a problem with your Terminal, please contact your Terminal supplier helpline.

Exceptions

- 9 Give the Cardholder the top copy of the Sales Voucher and also the relevant copy of the Terminal Sales Receipt.
- 10 Attach the retailer copy of the Terminal Sales Receipt to the retailer copies of the Sales Voucher. These copies must be retained for a period of not less than 13 months and must be produced to Cardnet upon request. If you fail to produce copies of the Terminal Sales Receipt and Sales Voucher, the disputed Transaction may be charged back to you.

Please note: if you key enter a magnetic stripe Card, you do so at your own risk. Any Transaction which is later found to be fraudulent may be charged back to you.

If you do not have an imprinter you should request an alternative method of payment. Alternatively imprinters can be purchased by calling the Cardnet helpline on **01268 567 100**.

If you need help or have any questions about the information in this section, please contact the Cardnet Helpline on **01268 567 100**.

If a key entered Transaction is disputed and you have not completed this procedure, the disputed Transaction may be charged back to you.

Important

- Please take extra care if the chip and/or magnetic stripe fails to 'read' because the Card may have been deliberately damaged.
- The imprinted Sales Voucher is only a record of the Transaction. Please do not process this voucher for payment.
- Merchants with electronic Terminals should ensure that they have a sufficient supply of paper vouchers in order to continue to accept Cards in the event of Terminal malfunction.
- If your Agreement with Cardnet allows you to process Transactions through an electronic Terminal, you may only process paper Transactions for a failed magnetic stripe Card Transaction.

Using the paper Fallback system to process Point of Sale Transactions when your Terminal is not working

Please note this is not permitted for internationally issued Maestro, Visa V PAY, Visa Electron, Diners Club International, Discover, BC Global, Troy Global, Elo Global, and RuPay Global cards.

If you have multi-currency or Dynamic Currency Conversion facilities this procedure is not permitted.

If your Terminal is not functioning correctly, or if you have a power or telephone network failure, you may have to use the paper Fallback system and complete the Transaction using a Sales Voucher. This process must be for Sterling (£) Transactions only.

Point of Sale Transactions

A Transaction can be completed by using the standard Cardnet Sales Voucher.

The Sales Voucher contains the following copies:

- 1 Cardholder's Copy (top copy): a record of the Transaction to be given to the Cardholder.
- 2 Processing Copy (white): a copy to be sent to Cardnet.
- 3 Retailer's Copy (yellow): a copy of the Transaction for your records. A copy of the Transaction must be produced to Cardnet if requested and therefore must be kept for at least 13 months. If you are unable to produce a copy the Transaction may be charged back to you.
- 4 Duplicate Copy (blue): a further record if you should need one.



Exceptions

Completing the Sales Voucher

- 1 Complete the Sales Voucher with a ballpoint pen as shown in the illustration, giving brief details of the goods purchased. Do not mark copies with pencil, paper clips or staples, as these can transfer through the carbons and obscure details.
- 2 Check that all details are clear especially on the processing copy of the voucher set. If the detail is not clear, a Dispute may occur. If you make a mistake please complete a new voucher and destroy the old one.
- 3 Retain the Card and check the Card details carefully as detailed in Section 3, 'Checking the Card' (p40). Ask the Card holder to sign the voucher.
- 4 When the voucher is signed check that the signature is compatible with the one on the Card. If the Cardholder's title is shown on the Card, ensure that the presenter of the Card matches the title, for example, if 'Mr' is printed, ensure the presenter is male.
- 5 You'll need to obtain an Authorisation for every paper Fall back Transaction you take. The telephone number to call is **01268 822 822**. (Please refer to your Agreement for your Card net floor limits).
- 6 The operator will ask you for the details needed to authorise the Transaction.

Occasionally the operator may ask you to obtain further identification from the Card holder or ask to speak with the Card holder directly. If this happens, please co-operate as fully as possible and ensure that the telephone handset is

passed back to you to speak with the operator to confirm the conversation with the Cardholder and obtain the Authorisation number from them, if given, before replacing the receiver. The operator may also ask you to check some additional forms of identification, for example, a driving licence.

- 7 If the operator authorises the Transaction, write the code in the space provided on the voucher.
- 8 When you are satisfied that everything is in order, hand the Cardholder the top copy of the voucher and their Card.
- 9 Once the Cardholder has left, do not alter the copies in any way. If there are subsequent queries or disputes, the Cardholder's copy will normally be treated as correct.



Please note

- If you print vouchers on your own tills, then the name and address of your outlet must appear on all copies.
- If voucher details are not able to be clearly read, this may result in a Chargeback to you.

Authorisation is not a guarantee of payment. It confirms that the Card has not been reported lost or stolen at the time of the Transaction and that adequate funds are available.

If the sale is declined

No reason will be given if the sale is declined. In these circumstances, please return the Card to the Cardholder, discreetly explaining that the Card Issuer has declined the Transaction, and ask for another method of payment.

The operator may ask you to keep the Card. Again this should be done as politely as possible and only if you feel you face no physical risk. After the Cardholder has left, cut the bottom left hand corner from the front of the Card. Attach the two pieces of the Card to a completed Cardnet Card Recovery Advice Form (see page p129 for details on how to request further copies), and return it to the address on the form.

Remember a £50 reward is normally paid to any Cardnet Merchant when a stolen Card is recovered.

Please note: Discover® Global Network do not participate in the reward scheme. This means we are unable to pay a reward for the recovery of Diners Club International®, Discover®, BC Global, Troy Global, RuPay Global or Elo Global cards.

Paper Refunds

The Refund Voucher consists of four parts; a top copy printed in red for the Cardholder, a white copy for processing, and yellow and blue copies for your own records.



Exceptions

Completing a Refund

If you wish to complete a Refund using the paper Fallback system, you must follow the steps below.

1. Check the Card following the instructions in Section 3, 'Checking the Card' (p40).
2. Complete the voucher: Refund Vouchers must be completed in the same way as Sales Vouchers. Make a brief note on the Refund Voucher about the exchange and/or return of any items. Do not mark copies with pencil, paper clips or staples, as these can transfer through the carbons and obscure details.
3. Authorisation: where an Authorisation code was obtained for the original Transaction, telephone the Authorisation Centre on **01268 822 822**. See Section 5, 'Authorisation and referrals' (p105).
4. Signature: you must sign the Refund Voucher.
5. Return the Card: once you have completed all the above steps, return the Card to the Cardholder together with any original receipt and a signed copy of the Refund slip.

If the cost of the replacement item differs from the returned item, a Refund for the original item should be completed on the same Card as the original Transaction. A new sale should be completed for the new Transaction and Authorisation obtained.

Remember: never Refund a Card where the original Transaction was made by another method of payment. For example, cash or cheque.

Authorisation is not a guarantee of payment. It confirms that the Card has not been reported lost or stolen at the time of the Transaction and that adequate funds are available.

LLOYDS BANK CARDNET VISA

5404 1234 5678 9000
08109 0711
Mr T M Grey

08111109
108 RJ
1 Jumper

599 9999 99
Whites of London
London NW5

PLEASE KEEP THIS COPY FOR YOUR RECORDS

REFUND AMOUNT: 29.99

Rob Jones

£ = 29.99

Processing Card Not Present (CNP) Transactions when your Terminal is not working

Provided you have received written agreement from Cardnet you may accept a telephone or written order from a cardholder who wishes to pay using a Visa, Mastercard, Maestro, Diners Club International, Discover, BC Global, Troy Global, RuPay Global, Elo Global or American Express card. Visa Electron cards can be accepted for CNP, as long as you authorise the Transaction, see Section 5, 'Authorisation and referrals'.

You must not accept internationally issued Maestro or V PAY cards for CNP Transactions.

To process your CNP Transactions you need to record the information on form CMS910 'Card Not Present Transaction Schedule'.

These forms are available by calling the Card net Helpline on **01268 567 100**.

The CMS910 is a two part carbonated form containing a perforated section which allows you to record the Card holder's Card Security Code (CSC) on the top copy only. This means that the CSC will only be recorded on the copy that you send to Card net for processing. This ensures that you comply with the Card Scheme regulations which state that the CSC information must not be stored by a Merchant (the perforated section on the top copy that you send through to Card net is destroyed once the Transaction has been processed).

It is important that you use the CMS910 to process these Transactions, as the standard Sales Vouchers do not comply with the Card Scheme regulations in relation to the

non-storage of the CSC data. For all CNP orders using the CMS910 you must collect the Card and Cardholder details following the instructions in Section 4, 'Accepting Cards, Card Not Present Transactions' (p50).

1. Complete a Cardnet 'Card Not Present Transaction Schedule' CMS910.
2. At the end of the day total up each sheet and list each CNP Transaction separately on a Retailer Summary Voucher. (Please do not submit more than 16 schedules behind one Retailer Summary Voucher).
3. Any Refunds must be entered on a separate sheet which should be clearly marked 'Refunds' and sent to us for processing with the sales pages. The value of Refunds must be offset against the value of sales.
4. Keep the carbon copy of the schedule for your records. These must be kept for a period of 13 months as Cardnet may ask you to provide a copy of the Transaction in the event of a dispute. For details on how this information must be stored see Section 7, 'Security'.
5. Send the top copies and Retailer Summary Voucher into Cardnet at the following address: Lloyds Bank Cardnet, PO Box 22, Sheffield S98 1BG.
6. Send a receipt to the Cardholder to confirm the order. Please remember that for security reasons the Cardholder receipt must not include the full Card number or from 15 Oct 2022 the full Merchant identification number or full terminal identification number.

Exceptions

The image shows a 'Card Not Present Transactions Schedule' form from Lloyds Bank Cardnet. The form is titled 'Card Not Present Transactions Schedule' and 'LLOYDS BANK CARDNET'. It includes a 'Retailer No.' field and a 'Merchant No.' field. The main body of the form is a table with columns for 'Date', 'Card No.', 'Cardholder Name', 'Cardholder Address', 'Cardholder City', 'Cardholder Country', 'Cardholder Postcode', 'Cardholder Telephone', 'Cardholder Email', 'Cardholder Mobile', 'Cardholder Fax', 'Cardholder Business', 'Cardholder Occupation', 'Cardholder Profession', 'Cardholder Industry', 'Cardholder Company', 'Cardholder Job Title', 'Cardholder Job Description', 'Cardholder Job Function', 'Cardholder Job Role', 'Cardholder Job Level', 'Cardholder Job Grade', 'Cardholder Job Class', 'Cardholder Job Code', 'Cardholder Job Title', 'Cardholder Job Description', 'Cardholder Job Function', 'Cardholder Job Role', 'Cardholder Job Level', 'Cardholder Job Grade', 'Cardholder Job Class', 'Cardholder Job Code'. The form also includes a section for 'Cardholder Details' and a section for 'Merchant Details'.

Authorising Card Not Present Transactions when your Terminal is not working

Authorisation must be obtained for all sales by calling **01268 278 278**. This enables you to carry out the usual status check so that you can confirm whether your customer has the funds to pay you. It also allows you to find out whether or not the Card has been reported lost or stolen.

When you call the Authorisation Centre, the operator will ask you for the Card and Cardholder information needed to authorise the Transaction(s).

If you use the Address Verification Service the operator will check the details you have provided, and give you one of the Authorisation responses detailed in the table in Section 4, 'Accepting Transactions, Card Not Present Transactions' (p50).

You can then make an informed decision whether or not to accept the Card as payment.

However, please remember that you remain ultimately responsible should a Transaction be confirmed as invalid or fraudulent, even if the data matches and an Authorisation code is given.

Important: if you choose to deliver goods to an address other than the Cardholder's address, you are taking additional risk. See Section 7, 'Security, How to guard against fraud', for some helpful tips.

Banking

Please remember to submit your Retailer Summaries, Sales Vouchers, Refund Vouchers and Card Not Present Transaction Schedules to Lloyds Bank Cardnet, PO Box 22, Sheffield S98 1BG at the end of each business day.

For full details on how prepare these Transactions for processing, please refer to Section 6, 'Banking and reconciliation' (p114).

10 : Additional information

Keeping us informed of changes to your business, plus other information including Authorisation telephone numbers and what to do if your business experiences financial difficulties.

Notifying us of changes to your business

You must notify Cardnet immediately if there are any changes to your business. Please refer to the Contact us lloydsbankcardnet.com/forms/contact-us.html section on the Lloyds Bank Cardnet website for details of how to notify us, and what supporting information will be required.

Change of bank and/or branch

If you do not tell us your bank account details have changed there will be a delay in funds reaching your account. In certain circumstances we will also need a new Direct Debit mandate.

Change of address

If you change your business or registered office address (or any other contact address you have asked us to use), you must notify us.

Closure or change of ownership

Your Cardnet facility is not transferable to anybody under any circumstance without Cardnet's written agreement. If you selling or closing your business you must let us know.

If the purchaser of your business wishes to use Cardnet, a new account will have to be opened that reflects the new ownership and we will make our usual pre-contract enquiries. If you fail to tell us that you no longer own the business you will continue to be liable for any liabilities that the subsequent owner(s) generate.

Change of legal entity

If you are changing the legal entity of your business, for example, from sole trader to limited company status, adding a partner to your business or if a partner leaves, you must let Cardnet know immediately.

In most cases we will (subject to the usual risk checks) ask you to sign a new Agreement and Direct Debit mandate (in the name of the new entity) and depending on what other changes may have occurred, we may ask you for further information in order that we may conduct a further risk assessment.

Change of products or services sold or other details

When you join Cardnet you give us various product details that your business sells and we categorise your account accordingly. These details, including your Card turnover and average sale value, are important in terms of the ongoing risk assessments that Cardnet regularly undertake.

Therefore, it is important that you let us know if the nature of your business changes, for example, a change of product or service or if you expand into an additional line of business, different from your existing business. You must also tell us if any other details that you have provided to us, whether in your application or otherwise, change.

If you do not tell us about any change, we may withhold our Services or Settlement payments pending our investigations and reassessment of risk.

Changing your trading terms

You must let us know immediately if you make any changes to your trading terms, for example, any changes to your Refund policy, or to the terms and conditions issued to your customers, or to the delivery time frames you have previously notified us of.

Write to us at:

Cardnet Merchant Services
Janus House
Endeavour Drive
Basildon
Essex SS14 3WF

Other changes affecting your business

You must tell us immediately if any of the following events occur:

- Any insolvency event affecting your business.
- You make any arrangement with creditors.
- You experience any financial difficulties.

Changing method of taking Cards

If you would like to change your method of taking Cards – either to Card Not Present or E-commerce Transactions, you must have Cardnet's written agreement. For further details on changing your method of taking Cards, contact the Cardnet Helpline on **01268 567 100** or write to us at the address above.

How to complain

Please tell us and we will do our best to put it right

Cardnet aims to give you the highest level of service. So if we make a mistake, or if there is something you feel we could do better, please tell us and we'll do our best to put it right.

This is to let you know what to do if you're not satisfied with the service we provide and the steps we ask you to take to help us deal with your complaint as quickly as possible.

Remember, most problems that arise can be resolved quickly if you talk to us as soon as possible.

When you call us you will need to have your Merchant Account number(s) to hand. Please remember, for security reasons, never to send this information to us by email.

Contact us

We need to know the nature of your complaint and how you think the problem should be resolved.

You can do this by:



Telephoning our Cardnet Helpline on **01268 567 100**



Emailing us at **cardnet_complaints@lloydsbanking.com**

Writing to us at the following address:

Lloyds Bank Cardnet
Phoenix House
Christopher Martin Road
Basildon
Essex SS14 3EZ

We will handle customer complaints as follows:

If your complaint relates to payment services we aim to issue a final response within 15 days after receiving your complaint. Should something outside of our control cause a delay, we will have a maximum of 35 days.

For other types of complaint, where the Financial Conduct Authority's (FCA) rules apply, the FCA gives us eight weeks to issue a final response, but we will aim to resolve all complaints well before this deadline.

Contact the Financial Ombudsman Service

If you remain dissatisfied:

You may be able to refer your case to the Financial Ombudsman Service* for an independent review. This is a free, independent dispute resolution service for customers of most UK banks, building societies, insurance companies and other financial institutions.

Their details are as follows:

Financial Ombudsman Service
Exchange Tower
London E14 9SR

Telephone **0800 0234567** (from a landline)
or **0300 1239123** (from a mobile).

You will find more information on the Financial Ombudsman Service website, including details about eligibility at **www.financial-ombudsman.org.uk**

We value your custom and want to resolve your complaint for you.

The Financial Ombudsman Service will only consider your complaint once you've tried to resolve it with us, so please take up your concerns with us first and we'll do all we can to help.

Raising a complaint with us will not affect any rights you may have to pursue the issue through formal (legal) proceedings.

* Please note that due to the schemes' eligibility criteria not all Lloyds Bank business customers will be covered by the scheme

What to do if you experience financial difficulties

You will usually spot financial problems before us and you should let us know of your difficulties as soon as possible.

If we become aware of problems we will let you know in writing.

Disputes will usually be the main reason for financial problems connected with your Card acquiring facility, which is why it is important that you follow the procedures outlined in the Manual carefully. The most common type of Dispute is in respect of CNP Transactions where you need to be particularly vigilant to avoid being targeted by fraudsters. See Section 7, 'How to guard against fraud' (p130). Most other Disputes arise when Transactions have not been read through the Terminal, imprinted or authorised correctly.

This list gives a few examples of problems that can concern us, particularly if you do not explain what is happening:

- There is a large increase in your Card turnover.
- The value of a Transaction is significantly larger than you told us you would process or usually process.
- There are unusual numbers of 'key entered' Transactions.
- We start to see Disputes from issuers on your account particularly if Cardholders are not receiving goods that they have ordered.
- Transactions are not being correctly authorised.
- Direct Debits are returned unpaid by your bank branch.

We can offer guidance to help protect you from financial loss. If you are concerned about fraud, we can send you training information and materials. If you are concerned about suffering a Dispute, or experience financial difficulties as a result of a Dispute, we will do all we can to help you. We will also try to reach agreement with you on how and when debts will be repaid and tell you where you can get advice-see page p163 for details. We will be happy to work with your advisers in order to reach a satisfactory conclusion to your difficulties.

Financial implications of Cardnet

If you are a sole trader you are liable for any debts that may arise under the Agreement that you signed when joining Cardnet.

If you are a partner in a business, or a trustee or committee member of a charity or club/society, you are jointly and severally liable for any debts or other liabilities that may arise under the Agreement from using our services. Each of the partners, trustees or committee members is separately responsible for keeping to its terms and repaying any debts or other liabilities and not just a share of it, even though they may not be a signatory to the Agreement. If any of you fails to comply with them, we can take action against one or more or all of you either individually or together. For example, we can take action to recover the whole of any debt from any one or more or all of you. If we are owed money when a partner, trustee or committee member dies, the deceased's estate remains responsible for paying the debt and we may require payment from it.

If we are owed money when a partner, trustee or committee member leaves the business, trust fund, charity or club/society, the outgoing partner, trustee or committee member remains separately responsible to repay the existing debt.

If you are a director of a limited company or a member of a limited partnership, your personal liability to Cardnet under the Agreement is limited to the capital you have invested in the company or partnership. Under the terms of the Agreement, the company or limited liability partnership will be fully liable for any debts arising under the Agreement.

Agencies offering financial assistance

You may find the following phone numbers and websites useful.

Business Debtline

0800 197 6026 (www.birminghamsettlement.org.uk)

Gov.UK

0845 600 9006 (www.gov.uk)

Citizens' Advice Bureaux

(www.citizensadvice.org.uk)

Citizens' Advice Scotland

0808 800 9060 (www.cas.org.uk)

Federation of Small Businesses

0808 202 0888 (www.fsb.org.uk)

Financial Conduct Authority (FCA)

www.gov.uk (www.fca.org.uk)

Prudential Regulation Authority

020 3461 7000 (www.bankofengland.co.uk)

National Federation of Enterprise Agencies

01908 605 130 (www.nfea.com)

Northern Ireland Association of Citizens' Advice Bureaux

028 9023 1120 (www.citizensadvice.co.uk)

The British Chambers of Commerce

020 7654 5800 (www.britishchambers.org.uk)

The Insolvency Service

0300 678 0015 (www.insolvency.gov.uk)

The Forum of Private Business

0845 130 1722 (www.fpb.org)

The Institute of Directors

020 7766 8866 (www.iod.com)

Authorisation telephone numbers

Point of Sale (OTC) sales

01268 822 822

Point of Sale (OTC) sales for JCB

0800 252 244

Card Not Present (CNP) Transactions

01268 278 278

Transactions processed through multi-currency or Dynamic Currency Conversion facilities

01268 662 520

Lines are open 24 hours, Monday to Sunday.

Merchant services

Cardnet Helpline – For any queries with your Cardnet account, please telephone

01268 567 100

Lines are open 8am to 9pm, Monday to Saturday

Alternatively, you can write to Cardnet at the following address:

Cardnet Merchant Services
Janus House
Endeavour Drive
Basildon
Essex SS14 3WF

Please ensure that all Cardnet related enquiries are referred to Cardnet. You should not seek advice or guidance in respect of Cardnet issues from your local branch or manager.

Cardnet stationery

Stocks of stationery, i.e. Sales, Refund and Summary Vouchers, and deposit envelopes, are available by completing the re-order form which you'll find in each box of vouchers. Simply place the completed re-order form behind the Sales Vouchers when sending into Cardnet.

Please be aware that we can only accept paper Transactions made on official Cardnet stationery.

In an emergency, vouchers can also be ordered by telephoning **01268 296 601** (24-hour answerphone service). You will be required to give your Cardnet Merchant number.

Point of sale and display material

A varied selection of point of sale material such as tent cards, window and till stickers are available by telephoning the Cardnet Helpline on **01268 567 100**.

Recommended tally roll supplier

Primatel

For further supplies of tally rolls, call Primatel direct on:

Tel: **02086 794428** or **020 8679 4428**

Lines are open 9am to 5pm, Monday to Friday.

Fax: **020 8679 4420**

E-mail: **enquiries@primatel.co.uk**

Website: **www.primatel.co.uk**

Cards left on your premises

Any Cards left at your premises must be kept safely until the end of business on the day when the Card was found. If the Cardholder returns to claim the Card, you must request the Cardholder to sign the refund voucher. If you are suspicious that the claimant is not the Cardholder, you must telephone the Authorisation Centre and state "This is a Code 10 call". Only release the Card if you are satisfied that the claimant is the Cardholder. Unclaimed Cards should be cut across the bottom left-hand corner of the front of the Card and both parts attached to a Cardnet Card Recovery Advice Form. Please complete the form and send it to:

Cardnet Rewards Department
Merchant Operations
Janus House Endeavour Drive
Basildon
Essex SSI 4 3WF

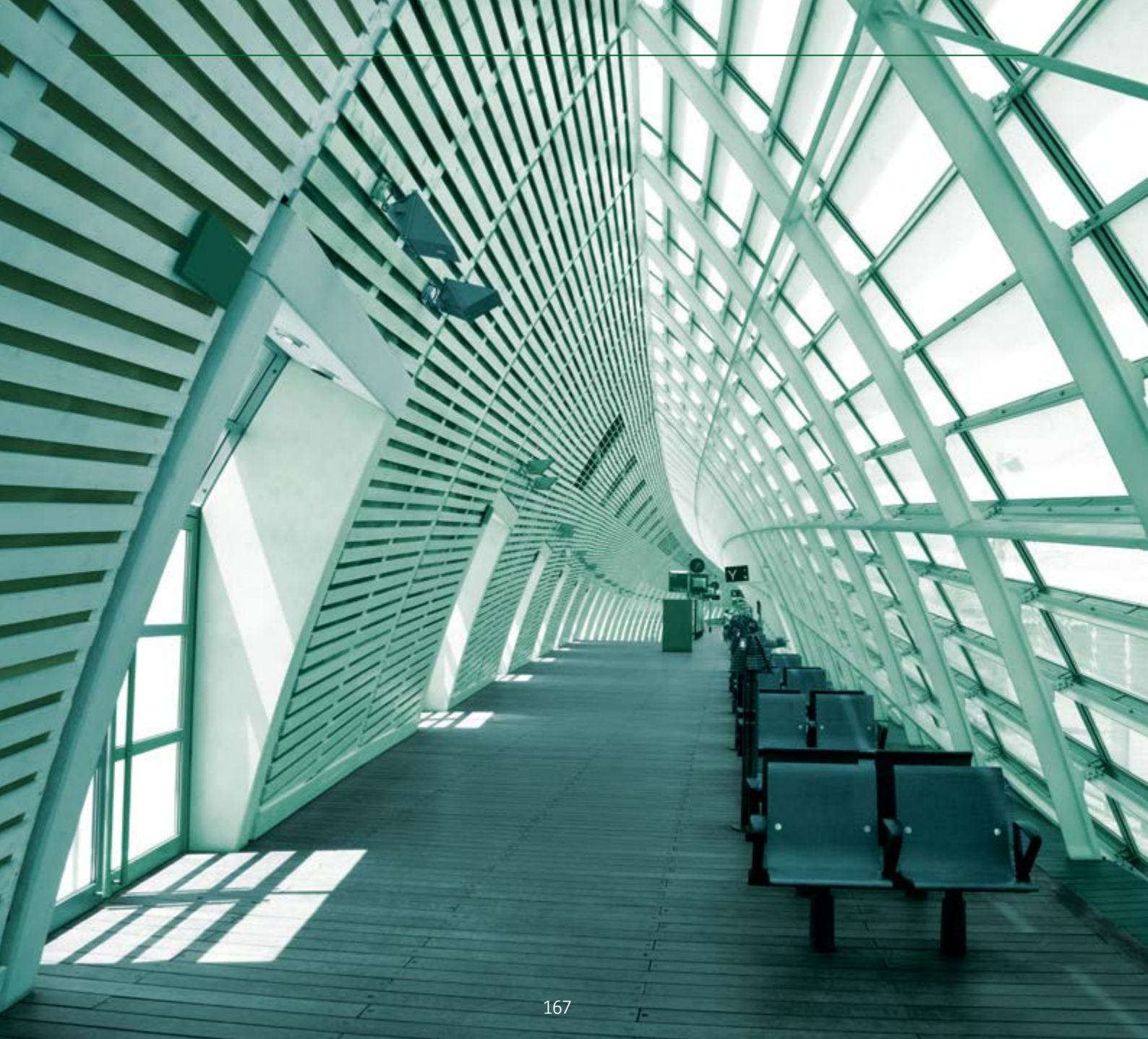
A financial reward is not given in these circumstances.

Emergencies and disruptions

In case of any disruptions to the postal or telephone services, you should hold a supply of Sales Vouchers and banking stationery.

If a disruption does occur, the following procedure will apply:

- Your Cardnet statement will be sent to you as soon as possible.
- As your account is settled by Direct Debit to your bank, this will continue to be done and we will notify you as soon as possible.
- You will be able to continue monitoring credits received by Cardnet by checking your bank statement.
- Disputes will be processed in the normal way but you will not be able to receive details until the emergency or disruption is over.



Our service promise. If you experience a problem, we will always try to resolve it as quickly as possible. Please bring it to the attention of any member of staff. Our complaints procedures are published at lloydsbankcardnet.com/contactus

Important information

Calls may be monitored or recorded in case we need to check we have carried out your instructions correctly and to help improve our quality of service.

Please remember we cannot guarantee the security of messages sent by email.

Cardnet® is a registered trademark of Lloyds Bank plc. Mastercard® and the Mastercard Brand Mark are a registered trademark of Mastercard International Incorporated, Maestro® is a registered trademark of Mastercard International Incorporated.

Discover® is a registered trademark of Discover Financial Services. Diners Club International® is a registered trademark of Discover Financial Services.

ProtectBuy® is a registered trademark of Discover Financial Services.

Lloyds Bank plc. Registered Office: 25 Gresham Street, London EC2V 7HN. Registered in England and Wales No. 2065. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.

Lloyds Bank plc is covered by the Financial Ombudsman Service. (Please note that due to the eligibility criteria of this scheme not all Lloyds Bank customers will be covered.)

This information is correct as of August 2022.

Get in touch



Go to lloydsbankcardnet.com



Call us on 01268 567100

Lines open 8am-9pm Monday to Saturday

Please contact us if you'd like this information
in an alternative format such as Braille,
large print or audio.



LLOYDS BANK

CARDNET

CMS200 (08/22)