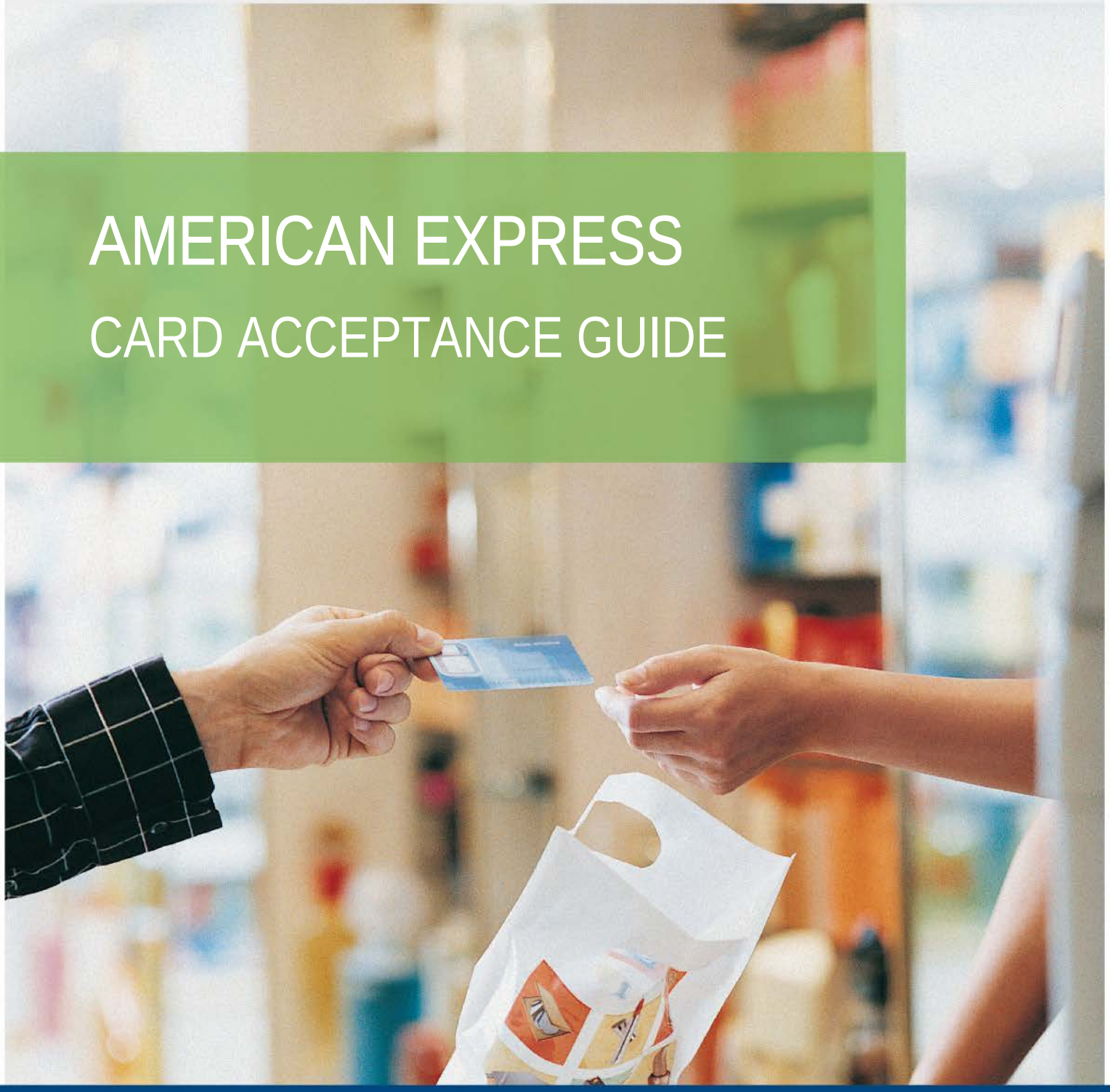
globalpayments

AMERICAN EXPRESS
CARD ACCEPTANCE GUIDE



SERVICE. DRIVEN. COMMERCE

CONTENTS

INTRODUCTION

YOUR AMERICAN EXPRESS AGREEMENT

Acceptance of American Express cards are subject to the American Express Terms and Conditions for Card Acceptance (American Express Terms and Conditions) entered into between you and American Express Payment Services Limited (American Express). .

Global Payments will provide the card processing services on behalf of American Express as their service provider. Global Payments will provide the following services on behalf of American Express:

- Process your American Express transactions
- Debit and credit your bank account
- Provide you with an invoice
- Answer any queries you might have.

ABOUT THIS DOCUMENT

This document is provided for guidance to merchants that have signed an American Express Card Acceptance Agreement whose processing and servicing of American Express transactions is performed by Global Payments. American Express is the acquirer of all American Express transactions and you accept American Express cards pursuant to your American Express Terms and Conditions. Where you have a contract with Global Payments for other services, that contract does not apply to your American Express transactions. This document is intended solely for informational purposes and does not form part of your American Express Terms and Conditions.

CARD PRESENT (CP) TRANSACTIONS

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

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

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

CHECKING CARDS

How To Perform Card Validation Checks On American Express Cards

The validation checks listed below apply to the majority of cards issued by American Express. Failure to follow these checks may result in you being subject to a chargeback:

1. Chip

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

2. Card Number

- The Cardmember (cardholder) account number begins with 34 or 37

3. Cardmember Name

- The Cardmember name appears on the front of the card, however, in the case of pre-paid cards, there might not be a name present.
- Check for obvious discrepancies between the Cardmember and card, such as a woman using a card with the title ‘Mr’, or a teenager using a card with the title ‘Doctor’ or ‘Sir’.

4. Cardmember Since

- Not relevant to the card acceptance process. Cardmember information only.

5. Valid Thru

- This is the expiry date of the card and will appear on the front of the card above the Cardmember name.
- The card should be carefully examined for the effective validity date. You must not accept cards presented after their valid thru date. The terminal will perform certain checks on the card, but we cannot be held liable if the terminal accepts an expired card.

6. Hologram

- Some American Express cards may have a hologram and if present, it can appear on the front or the back of the card.
- Check that it has not been tampered with. The hologram should be smooth to the touch, should not have a rough or scratched surface and the 3D image should move when tilted. Counterfeit cards often feature poor hologram reproductions.

7. Signature Strip

- The signature should be written clearly and be smooth to the touch. Be suspicious if the card isn’t signed, if the signature appears to have been erased, if the card appears to have been re-signed, or if the signature is written in block capitals or felt pen.
- Check that the signature agrees with the name on the front of the card.
- Check that the signature strip has not been tampered with or that the word ‘void’ isn’t visible.
- Check that the signature on the card matches the one on the terminal receipt.
- If you’re presented with an unsigned card, advise the Cardmember that you can’t proceed with the transaction.

8. Card Identification Number (CID)

- This is a four digit number validation code that appears on the front of an American Express card. This will appear on the right, above the card number. The CID is also referred to as the Card Security Code (CSC).

9. Magnetic Stripe

- Ensure that the card has a magnetic stripe on the back. Be suspicious of a counterfeit if the magnetic stripe feels unusually rough or scratched.

11. Card Logos

- The American Express logo (see next page) may appear on the front or the back of the card. Some cards are co-branded with logos of the partner that has issued the card. In these cases, the logo of the partner and the American Express logo will appear on the front of the card.

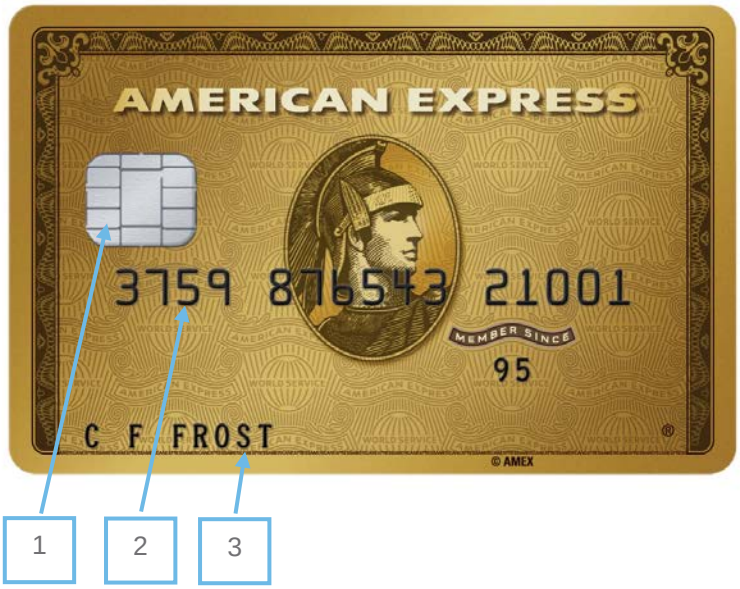
EXAMPLE OF CARD LOGO

American Express Logo

EXAMPLE OF CARD AND CARD FEATURES

Key to card images:

1. Chip
2. Card Number
3. Cardmember Name



AUTHORISATION

Authorisation must be obtained at the time of the sale whilst the Cardmember is present, in the case of CP transactions.

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

What Is An Online Authorisation?

Online authorisation is when your terminal automatically:

- checks certain card details
- seeks confirmation that the Cardmember has sufficient available funds on their account at the time of the transaction
- checks that the card has not been reported lost or stolen at the time of the transaction.

However, it **doesn't**:
- confirm the Cardmember's identity
- guarantee payment.

All transactions must be authorised. Your terminal will seek authorisation automatically:
- Cardmember when a chip and PIN card is signature-verified
- when a card contains no chip, only a magnetic stripe
- when a transaction has been key-entered
- when a chip and PIN card is accepted using the magnetic stripe.

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

If you're in any way suspicious about the card or Cardmember, make a 'Code 10' call (see page 4).

When Is Telephone Authorisation Sought?

You must call our authorisation service (see page 13 for contact details) if:
- you're unable to obtain automatic authorisation
- you're in any way suspicious about the card or Cardmember (see 'Code 10 Call' on page 4)
- prompted by the terminal.

What Does Telephone Authorisation Do?

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

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

'CODE 10' CALLS

A 'Code 10' call should be made to our authorisation service (see page 13 for contact details) if:
- you're suspicious of the card, the Cardmember or the circumstances of the transaction
- you've been instructed to do so by us as a fraud prevention measure.

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

What You Need To Make The 'Code 10' Call

- Your merchant number
- the transaction amount rounded up to the nearest pound; if the transaction isn't in sterling, state the currency and amount
- the authorisation code if a code was granted with the original transaction, for example with an online authorisation
- you'll need to be clear about why you're suspicious of the card and/or Cardmember
- you should ensure that you handle the call as discreetly as possible

- you may be instructed to ask the Cardmember a number of questions for security purposes.

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

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

Remember to:
- advise the Cardmember that a routine security check is to be undertaken or that your card processor has requested a routine security check on the transaction. Hold on to the card and goods until the security checks have been completed
- turn on any surveillance equipment you may have
- telephone our authorisation service (see page 13 for contact details)
- ensure that a manual imprint of the card is taken whenever you process a transaction following a 'Code 10' call as evidence of the transaction. American Express transactions can only be processed electronically
- obtain the authorisation code directly from us, and not from either the Cardmember or anyone else, such as the card issuer, who may be involved with the call
- don't telephone any number given to you by the Cardmember
- don't make a 'Code 10' call if you feel threatened or consider it's unsafe to do so, for example, if you're alone in the shop; in this case call us immediately after the Cardmember has left, as this may help to prevent potential fraudulent activity elsewhere.

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

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

If You're Still Suspicious

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

RECOVERED CARDS

Retaining A Card

If we ask you to retain a card, please try to do so. However, you should not endanger yourself or your colleagues in endeavouring to retain a card.

If the person presenting the card becomes violent or abusive, always return the card to them, even if we've asked you to retain the card. In these circumstances, you should always:
- try to record details of the appearance of the person presenting the card and use any surveillance equipment that you may have
- telephone our authorisation service (see page 13 for contact details) and explain to us that you were unable to retain the card as requested.

In some circumstances we'll contact the police. If the police ask for the card:
- hand the card to the police officer

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

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

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

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

Finding A Card Or A Card Is Left At Your Premises

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

When a card is claimed, don't hand over the card until you've verified the Cardmember's identity:
- ask for satisfactory identification, such as a driver's licence
- check the signature on the card against a specimen signature of the person claiming the card
- if you're in any doubt, contact our authorisation service (see page 13 for contact details).

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

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

REFUNDS

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

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

Refunds for American Express cards can only be processed electronically.

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

Authorisation Reversals

American Express don't require you to reverse the authorisation for a transaction that's cancelled as the authorisation will expire after seven days. However, if a Cardmember is concerned about their credit limit, call our authorisation service (see page 13 for contact details) to reverse the authorisation.

CARD NOT PRESENT (CNP) TRANSACTIONS

In addition to the guidance provided in the rest of this document, follow the guidance provided in the American Express Terms and Conditions under Card Not Present Charges.

Note: American Express cards can only be accepted over the internet if you use Strong Customer Authentication i.e. SafeKey Refer to your copy of the American Express Terms and Conditions for more information on Strong Customer Authentication.

SPECIAL TRANSACTION TYPES

BUREAU DE CHANGE

American Express cards must not be accepted for Bureau de Change transactions**.**

GRATUITIES

Gratuities can be performed on American Express cards.

HOTEL AND CAR RENTAL TRANSACTIONS

Refer to your copy of the American Express Terms and Conditions for information on Lodging and Motor Vehicle Hire.

PREPAYMENTS/DEPOSIT/INSTALMENTS

Refer to your copy of the American Express Terms and Conditions for information on Advance Payment Charges in relations to prepayments and Delayed Deliver Charge in relation to deposits.

Note: Instalments aren't possible on American Express cards.

RECURRING TRANSACTIONS

Refer to your copy of the American Express Terms and Conditions for information on Recurring Billing Charges.

CREDITS AND DEBITS TO YOUR BANK ACCOUNT

CREDITS TO YOUR BANK ACCOUNT

Timescales For Our Processing

Following receipt of your transactions, we'll transmit them to American Express to request payment on your behalf. Amounts which we receive from them in respect of your transactions will be held to your account in our books and records on the same business day that we receive them. Payment will then be made to your bank account as agreed with you. Timescales for the payment will be in accordance with the American Express Agreement, or as agreed otherwise in writing, but generally you'll receive cleared funds in your bank account by the third business day after we receive your transactions for processing. The date the credit appears on your account is dependent on your account holding bank.

Timescales For Your Credit

The following is a typical guide to when you should expect any payments to be credited to your bank account, however, this depends on your account holding bank:

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

Crediting days are Monday to Friday, excluding public holidays.

Crediting Timescales may vary if:

- a different Crediting Timescale has been agreed
- you don't complete your terminal 'banking' procedures every day
- we've agreed any other arrangements in writing
- you haven't followed the guidance provided.

Bank Statement Entries

Unless we've agreed otherwise with you in writing, we'll credit your nominated bank account with a single credit for all the transactions we process on your behalf, including those processed for American Express.

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

SERVICE CHARGES

How Will We Collect Service Charges?

The invoice that we provide, or make available to you at the beginning of the month, details the service charges relating to the transactions that we've processed for you in the previous month, including any American Express transactions that you may have taken.

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

UNDERSTANDING YOUR INVOICE

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

CHARGEBACKS

INTRODUCTION

A chargeback is a transaction that has been disputed by the Cardmember or American Express and returned to us. A chargeback is also known as a 'dispute'.

Each chargeback has specific rules, regulations and time limits within which Global Payments must operate. We'll do everything possible within the rules to defend the chargeback on your behalf.

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

- request for information (see 'What Is A Retrieval Request?' below)
- fraud – the transaction was completed for an illegal or fraudulent purpose and you were or should have been aware of such illegality or fraud (see page 10)
- authorisation related – for example, the transaction exceeds your floor limit and was completed without authorisation (see page 3), authorisation has been declined etc.
- processing error – for example, duplicate processing of a transaction
- cancelled/returned goods or service – Cardmember has cancelled an order or returned goods and has not received a refund, or a refund has not been processed, or a refund has not been credited to the same Cardmember account that was originally debited (see page 6)
- non-receipt of goods/services - for example, in the case of late delivery of goods or services, or the wrong goods have been delivered.

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

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

Requests for such documentation can be received up to 180 days after the transaction has been debited to the Cardmember's account or the service received. However, in some circumstances, for example when fraud is involved, documents can be requested up to two years after the transaction date. It's therefore essential that you're able to retrieve such documents easily.

Please contact us (see page 13 for contact details) if you need to discuss a chargeback letter or if you're unsure what documentation is required.

WHAT IS A RETRIEVAL REQUEST?

A retrieval request, also known as a request for information, is when a Cardmember queries a credit or debit card transaction. This is often because the Cardmember can't remember undertaking the transaction.

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

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

DATA SECURITY

Under your American Express Agreement, you're required to achieve and maintain Payment Card Industry Data Security Standard (PCI DSS) compliance.

A copy of the American Express Data Security Operating Policy is available at:
www.americanexpress.com/data security

PCI DSS compliance achieved and maintained via Global Payments will be notified to American Express to satisfy their requirements.

HOW TO REDUCE FRAUD

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

Authorisation doesn't guarantee payment!

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

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

HOW CAN I PROTECT MY BUSINESS?

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

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

If you process CNP transactions, you need to be even more vigilant. There's a greater inherent risk in accepting CNP transactions because you're unable to guarantee that it's the genuine Cardmember providing the information. Therefore, accepting CNP payments considerably increases your

vulnerability to fraud, chargebacks and ultimately financial loss. This is because you can't physically verify the transaction by performing card validation checks and checking the Cardmember's signature or PIN.

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

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

Fraud Prevention Tools

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

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

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

Card Identification Number (CID): The CID provides additional security information designed to confirm that the customer is physically in possession of the card. The CID is a four digit number validation code that appears on the front of an American Express card.

The CID can also be referred to as CSC, CVV, CVV2 or CVC2.
Note: You must not store this data. This is strictly prohibited under PCI DSS.

SafeKey: For American Express ecommerce transactions, an additional layer of security must be incorporated into websites. Refer to the American Express Terms and Conditions for more information on Strong Customer Authentication.

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

Fraud Screening

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

As a minimum these checks should include:

- statement address
- statement address country
- number of previous declined transactions on same card or same order
- delivery address

- phone numbers
- same value transactions
- number of times a card has been used in a given time.

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

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

Other Helpful Tools

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

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

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

Financial Fraud Action UK
Working together to prevent fraud

www.financialfraudaction.org.uk

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

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

ADDITIONAL IMPORTANT INFORMATION

STATIONERY

If you use a terminal to process card transactions, we'll provide you with a starter pack that contains display material to let your customers know that you accept American Express cards.

To order further supplies please call us on the number provided on page 13. Allow five business days for delivery.

PRODUCING YOUR OWN ADVERTISING

If you want to produce your own materials to tell your customers that you accept cards as a means

of payment, please ask us for an artwork pack.

The artwork pack gives full details about reproducing the card logos.

HOW TO END THE CARD ACCEPTANCE AGREEMENT

If you no longer wish for Global Payments to process your American Express transactions, you will need to contact American Express directly to discuss your available options, for more information visit their website at www.americanexpress.co.uk

HOW TO CONTACT US

If you have any questions about American Express card processing, please contact our helpdesk in the first instance. We'll be able to assist you on behalf of American Express.

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

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

GLOBAL PAYMENTS HELPDESK: 0345 702 3344

We're here to help, so please call us but please don't use this number for authorisations (see below). We're open for card processing enquiries every day (except Christmas Day) between 8.00am and 11.00pm Monday to Saturday, 10.00am and 5.00pm Sunday and between 10.00am and 4.00pm on public holidays.

We also provide a textphone service on 0345 602 4818.

You can also contact us via:

Our website: www.globalpaymentsinc.co.uk

And email: customerservices@globalpay.com

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

GLOBAL PAYMENTS AUTHORISATION SERVICE: 0345 770 0600

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

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

IF YOU WANT TO COMPLAIN

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

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

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

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

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

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

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

The Financial Ombudsman Service

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

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

Please note calls to both these numbers are recorded.

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

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

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

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

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

AMEXAOI 08/2016 | GP468