Business Operations Agreement

Schedule 2

Appendix 08 –
Finance Best Practice

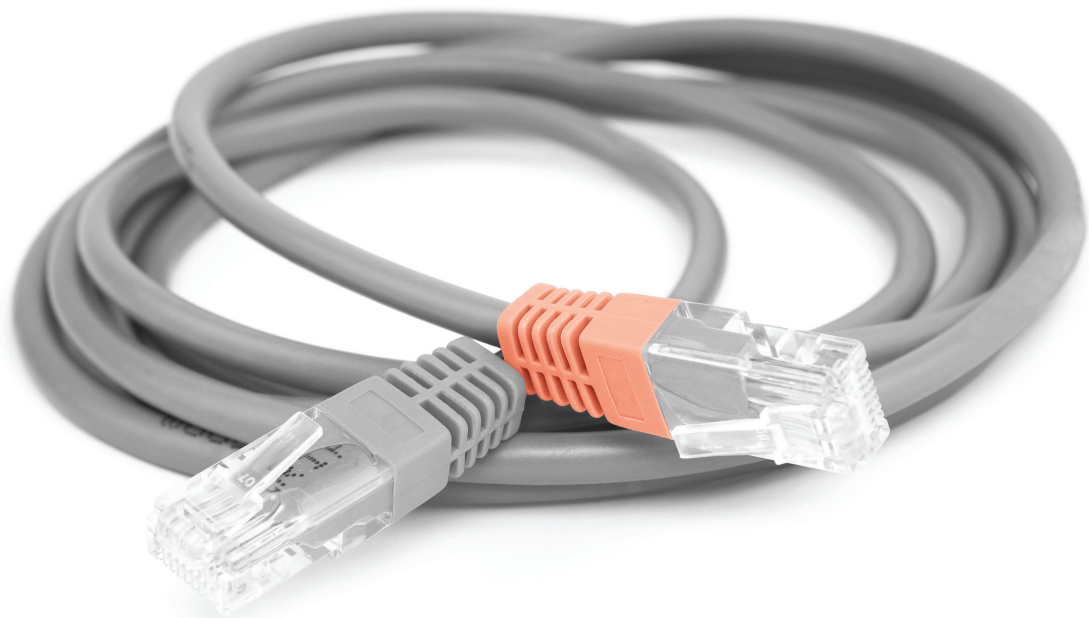*Service Operations Directorate*
Transport for London
4th Floor, Palestra
197 Blackfriars Road
Southwark London SE1 8NJ

AUDDIS

Automated Direct Debit Instruction Service

Contents

Introduction

Making Direct Debit even easier and more cost-effective

Direct Debit is one of the most widely used and accepted payment methods in the country. It saves time for everyone – consumers, businesses, utilities, charities, banks and building societies.

It's simpler for your customers, too, and is increasingly recognised by the consumer as being the 'easiest way to pay'.

AUDDIS – the Automated Direct Debit Instruction Service – automates the transfer of Direct Debit Instructions (DDIs) between you and the bank. Quite simply it makes the processing of DDIs easier, faster, more efficient and cost-effective than ever before.

Increasing the benefits of Direct Debit

AUDDIS benefits everyone involved in a Direct Debit payment.

For service users:

- Lowers postage and set up costs for DDIs

- Provides faster identification of invalid account information significantly reducing unpaid Direct Debits

- Allows a reduction in the time between lodgement, when the bank receives and accepts the DDI, and the collection of the first payment

- Enables you to provide a better quality of service through reduced processing delays and fewer manual steps

- Provides more accurate identification of a DDI through a mandatory reference

- Offers greater uniformity and ease of DDI processing

- Reduces the potential for re-keying errors, further improving the quality of service.

For banks it:

- Reduces processing time

- Reduces the potential for error

- Minimises paperwork and manual input

- Takes paper out of the banking system – and is now the accepted standard throughout the banking industry.

For consumers it:

- Increases efficiency of the Direct Debit service/product offered.

AUDDIS – the benefits

Practically, AUDDIS has only one primary change from conventional DDI processing: the original paper Instruction is retained by you, not the bank.

You simply enter the customer's details into your own system and send them electronically via the Bacstel-IP service to the customer's bank.

It might seem a small change, but it brings major additional advantages for you.

Earlier collection of first payment

A major benefit which AUDDIS brings is the advantage of allowing collection of the first Direct Debit, two working days after the lodgement of the AUDDIS DDI with the bank, provided the customer has received advance notice. It is however, recommended that 5 working days are left before the first collection to ensure that no lodgement rejections are received.

Reduced paperwork

As Direct Debits become the preferred payment option, the amount of paperwork will continue to increase, which is expensive for all concerned and can also result in processing errors and delays.

AUDDIS significantly reduces the amount of paper passed between you and the banks.

Fewer errors

The current system of double keying information from a DDI by both you and the bank increases the possibility of input errors. These, in turn, waste time and money for everyone, and reduce the consumer's confidence in service users and banks, and ultimately the Direct Debit itself. AUDDIS reduces the opportunity for input errors by only requiring the information to be keyed in once.

Time savings

Add to these benefits a reduction in time in processing an AUDDIS Instruction, as well as the improvement in quality resulting in fewer customer queries, and the strength of the business case for changing to AUDDIS becomes even more compelling.

First step towards Paperless Direct Debit

With ongoing rapid growth of direct marketing, telesales, e-commerce and the internet, the importance of Paperless Direct Debit – which is only available to AUDDIS users – cannot be over emphasised.

With Paperless Direct Debit DDIs can be set up over the telephone or internet, via telephone keypad or face-to-face without the customer having to sign a paper Instruction.

- Direct Debit sign up at 'point of sale' eliminates much of the paperwork and postage associated with setting up Direct Debits

- First payments can be collected earlier as you don't need to wait for the customer to complete and return the DDI

- Bank details can be checked at 'point of contact', eliminating administration problems later

- Telesales techniques can help increase conversion of sales opportunities.

The customer also benefits from the certain knowledge that a letter confirming all the details of the paperless sign up will be sent to them.

Getting it right first time

The earlier in the process that discrepancies are detected, the less chance of error when Direct Debit payments are processed. Indeed, AUDDIS service users have reduced the number of unpaids due to the reference and modulus checking processes introduced by AUDDIS.

Core reference

All AUDDIS Instructions must contain a core reference which is quoted on subsequent payments. This results in a more accurate matching of payments with Instructions.
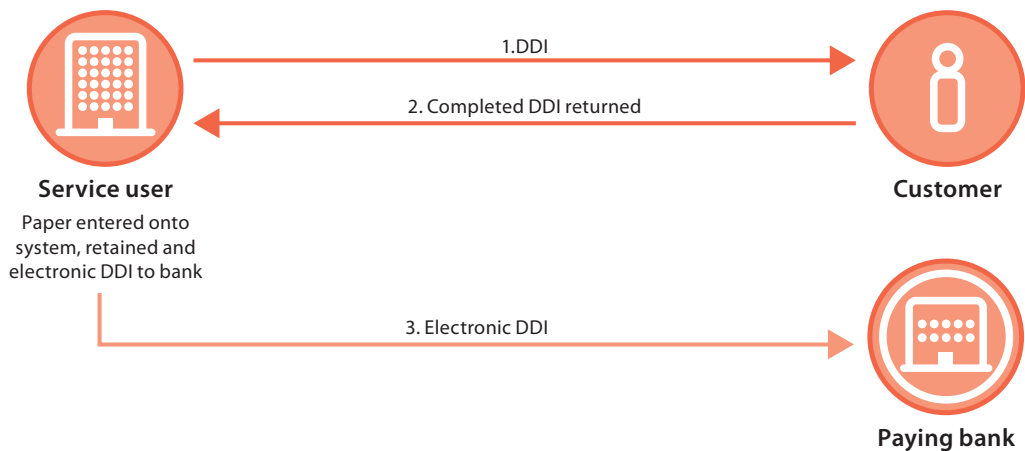
Modulus checking

It is all too easy for customers to provide incorrect details when giving their sort code or account number, which delay setting up and collecting payments. AUDDIS guards against this through modulus checking which ensures the account number is valid for the sort code.

Modulus checking is a core part of the AUDDIS service, you can enhance your progress by incorporating modulus checking in your own systems. This ensures that the customers account details are checked at the time of input, identifying any discrepancies at the outset. All Bacs Approved Software Solutions will supply modulus checking routines as part of standard AUDDIS solutions.

Increased customer satisfaction

AUDDIS means customers will notice an improvement in your customer service, even though the operational changes are invisible to the consumer.

Service user
Paper entered onto system, retained and electronic DDI to bank

1.DDI

2. Completed DDI returned

Customer

3. Electronic DDI

Paying bank

Direct Debit Guarantee

The Direct Debit Guarantee protects customers in the event of an error by you or the paying bank. AUDDIS, does not affect the Guarantee. In fact AUDDIS makes the Guarantee easier to implement by reducing manual involvement and therefore the risks of error and indemnity claims.

In the event of an error the customer's bank still remains responsible for making an immediate refund to the customer. If the error is caused by you the bank will reclaim the amount from you.

How to get AUDDIS working for you

Time to switch to AUDDIS

AUDDIS is standard throughout the banking industry. All banks accept AUDDIS Instructions, so it does not matter who your customers bank with, you can expect the same level of service.

There has never been a better time to switch to the simpler way of managing your Direct Debits.

How to start

Contact your bank who will assess the benefits that AUDDIS will bring to your Direct Debit operations and your ability to satisfy the AUDDIS criteria. If you both agree that AUDDIS is suitable for your organisation, the next steps are:

- Complete and submit an AUDDIS application form

- Prepare your systems, including software, to accept the new submission and message formats

- Complete the AUDDIS testing procedures

- Go live on AUDDIS.

Don't delay, contact your bank today. They will provide you with the best available support to ensure a smooth transfer over to AUDDIS.

Full details on switching to AUDDIS are covered in the 'AUDDIS Service Definition' and 'AUDDIS Migration Guide', both of which are available from your bank.

Are you overlooking the benefits of ADDACS?

ADDACS, the Automated Direct Debit Amendment and Cancellation Service, is another valuable enhancement to the Direct Debit service. It improves the speed of processing DDI amendment and cancellation information between you and the bank.

Customers notify their bank of any changes or cancellations to their DDIs. The paying bank consolidates all amendment and cancellation details and passes the information to you using ADDACS. This is sent electronically and offers a wide range of benefits.

- DDI amendments and cancellations are applied faster and more accurately

- There are no postal or handling delays. Details of your amendments and cancellations are accessible from 8.30am onwards the working day after they have been input by the paying bank

- Administrative and problem resolving costs associated with re-keying errors are virtually eliminated as you can feed the amendment and cancellation information automatically into your DDI database

- Your customer service is improved, as your systems can be adapted to generate standard letters, in accordance with the reason code, to keep your customers informed.

More information

To find out more about using AUDDIS and other services to improve the speed and efficiency of your Direct Debit scheme, contact your bank or visit www.bacs.co.uk/businesses

www.bacs.co.uk/usingdirectdebit

bacs

Electronic Business Guide

Version 3.0 January 2006

Contents

Introduction

This Electronic Business Guide (EBG) is designed to provide the information required by Merchants and Vendors in the UK to enable acceptance, processing and submission of American Express card transactions. It will also enable you to certify:

- your POS system for on-line authorisation, both single transaction and batch
- your file transmission method
- your submission file format

This guide contains all the information you should need, but if you have any further queries please get in touch with your Network Development contact direct or call the number below.

Network Development UK
American Express
UMC 53 00 002
Ground Floor
154 Edward Street
Brighton
BN88 1AH

Tel   01273 578899 option 2
Fax   01273 525833

networkdevelopmentuk@aexp.com

www.americanexpress.co.uk/merchant

Glossary of Terms

Term	Meaning
AAC	Application Authentication Cryptogram
AEIPS	American Express ICC Payment Specification
AC	Application Cryptogram (ICC term)
Agent	A third party bureau responsible for processing and submitting transactions on behalf of a Service Establishment.
AID	Application Identifier (ICC term)
AIP	Application Interchange Profile (ICC term)
ARPC	Authorisation Response Cryptogram (ICC term)
ARQC	Authorisation Request Cryptogram (ICC term)
AVS	Address Verification Service; the use of Cardmember address and postcode numerics to provide additional security information in authorisation requests.
CAPK	Certification Authority Public Key (ICC term)
CID	Card Identifier Digits; the four digits (unembossed) found on the front of an American Express card. They equate to the Card Security Code.
CNP	Cardmember Not Present: any transaction environment where the Cardmember is not physically at the POS. Includes mail order, telephone-order and internet.
DDA	Dynamic Data Authentication (ICC term)
EBG	Electronic Business Guide – this document
EMV	An acronym for Europay Mastercard Visa, the cardschemes responsible for establishing the standard relating to chip and PIN transactions.
Floor Limit	The transaction amount threshold above which all transactions must seek authorisation; Amex sets a floor limit of zero for most Merchants, thus ensuring that all transactions seek approval.
IAC	Issuer Action Code (ICC term)
ICC	Integrated Circuit Card, also known as a Chip Card or Smart Card.
Merchant	See Service Establishment.
NUA	Network User Address.
NUI	Network User Interface.
PAN	Primary Account Number; the account number embossed on the card
POS System	Point of Sale System. Refers to any electronic equipment used at the point of sale to capture card data. In the context of this Guide the term 'POS system' covers stand-alone terminals and integrated systems.
ROC	Record of Charge; a single transaction either electronic or on paper.
SDA	Static Data Authentication (ICC term)
SE (Service Establishment)	The company or organisation which is contracted with American Express to accept the American Express card as a method of payment. Also known as the Merchant.
SOC	Summary of Charge; a record used in settlement files to summarise batches of ROCs (transactions), detailing the number and value of debit and credit transactions.
Submitter	The Service Establishment or agent responsible for submitting settlement files to American Express on the Service Establishment's behalf.
TC	Transaction Certificate (ICC term)
Vendor	Software company producing POS software on a commercial basis.

General Information

This section of the Electronic Business Guide provides general information about card acceptance testing procedures for American Express.

Card Acceptance for American Express

Before starting to accept transactions from American Express Cardmembers and submitting the details for processing, you must obtain approval for:

- the authorisation interface
- the authorisation message format
- the settlement file transmission method
- the settlement file format

Support from American Express

The Network Development team within American Express provides consultancy and support for POS system certifications and manages the POS system approval process.

Notice Periods and Certification Timescales

You should allow the following periods for completion of testing:

- Four weeks for POS system authorisations testing of APACS 30 POS systems
- Six weeks for testing submissions.

How to request Certification

For **magstripe** authorisations or submissions testing please complete the Request for Certification Form in Appendix A. If you require test cards or account numbers please also complete and sign the Indemnity in Appendix B and send to us by post of fax.

For **EMV** testing please download an EMV Certification Request Form from our website, www.americanexpress.co.uk/merchant/chipandpin or contact Network Development.

General Information

Card Formats

American Express requires that you are able to process cards with magnetic stripes encoded to both ANSI and ISO standards. More information regarding track layouts is given in Appendix I.

American Express also issue Chip (ICC) cards verified by both PIN and signature. Formal EMV accreditation of your POS equipment is required if you wish to accept American Express Chip cards. Please contact Network Development to discuss our EMV accreditation procedure.

Validating Transaction Details

The POS system must be capable of validating the following, regardless of input method:

- Cardmember number (see Appendix H)
- Expiry date.   Expired cards should be declined in line with industry practice
- The transaction value.   Transactions for zero amounts are invalid; the POS system should prevent all such transactions being submitted to American Express.

The POS system must also prompt the operator to confirm that for Cardmember-present magstripe transactions the Cardmember signature is acceptable.

BIN ranges

American Express does not issue detailed ('refined') BIN ranges; any account number starting with 34 or 37 should be accepted as an American Express card. If a 6-digit BIN range is required please use:

340000 - 349999
370000 - 379999

Keyed Input

The operator may need to key card details in a Cardmember Not Present (CNP) environment, or if a swipe or chip read has failed. The following information should be keyed:

- Card account number, as embossed in the middle of the front of the card
- Expiry date, as embossed on the lower left-hand side of the front of the card

The start / effective date is **not** required.

Cancelling (Reversing) Transactions

The POS system must be capable of cancelling a transaction before completion, either at the request of the Cardmember or Service Establishment, or because it has been declined after referral to American Express. Reversals should be performed locally and should **not** be sent online.

Details of the transaction and the cancellation / reversal should be kept by the POS system for audit trail purposes, but should not be submitted for settlement to American Express.

Audit and Traceback Requirements

A paper record/receipt must be produced for every transaction at an attended POS system. It must contain all the information necessary to provide a full audit trail capable of resolving queries from our Cardmembers. Appendix C covers receipt requirements, layouts and checklists for use when magstripe testing. An audit trail is also essential for transactions on Unattended and Cardmember Not Present POS systems, although a paper receipt is not – see Appendices C3 and C4 for more details.

Receipt Requirements for EMV transactions are given in Appendix K.

General Information

File Acknowledgements

Our two file acknowledgement products offer a simple way of confirming electronically that your direct submissions to American Express have been received and processed.

The file 'Echo' provides confirmation that a submission has been received, and is available in plain text format 30 minutes after the file has been submitted.

The 'Enhanced File Acknowledgement' provides information at a Service Establishment level and details the status of data, accepted or rejected, 90 minutes after whichever of our three daily processing runs the data is processed in (see the section on Submissions, later in this document). It is available in fixed-length or delimited formats which can be imported and manipulated as required.

These reports are only available to Service Establishments that submit directly to American Express and we would recommend that you are set up for the 'Echo' report as a minimum. Please speak to your Network Development contact for further information and Technical Specifications.

Electronic Payment Advice (EPA)

Standard paper-based statements are sent by post, subject to a possible fee. It may be preferable to receive our electronic version of statements, the EPA, for which no charge is made. The EPA is a detailed report of transactions for which a Merchant is to be paid, and acts as a useful reconciliation tool. The file is available electronically, in fixed and delimited formats, to Merchants with direct connectivity to American Express. EPA is not available to, or via, Third Parties. Please speak to your Network Development contact for further information and Technical Specifications.

Online Merchant Services (OMS)

Where EPA is not appropriate we offer this comprehensive, free, reconciliation tool. More information and self-enrolment is available at www.americanexpress.co.uk/oms.

Euro and Multi-Currency Processing

If you have a requirement to offer transaction currencies other than sterling please contact Network Development to request the **Multi-currency Addendum** to this Guide.

Authorisations

This section covers the certification of POS systems for APACS 30 version 18 for on-line authorisation.

If you are a terminal provider and wish to certify APACS 30 or APACS 40 stand-alone devices, please contact us for details.

Certification of Electronic Authorisations

POS systems must be certified before they can be used to process electronic authorisations for American Express. American Express currently makes no charge for this certification service.

Approval for Commercial POS Systems

If you are a vendor developing software commercially, you can obtain full approval for your POS system or software before selling it to third parties and distributors. The third party or distributor may also obtain approval on behalf of the customer, if required.

Scope of the Tests - POS system Types

Test scripts are given in Appendix C. Most of the scripts contain tests for both keyed and swiped transactions. If the POS system you are testing only uses one of the entry methods, you only need to carry out the tests for the method applicable. If both methods are available to POS users, even if one is preferred over the other, all tests in the appropriate test script should be completed.

Transaction Types

Your POS system must be capable of processing sale and refund transactions for both ISO and ANSI card formats. Tests for both transaction types are included in the scripts.

Floor Limits

A merchant must seek authorisation from American Express if a transaction amount is over the mandated floor limit.

The scripts include tests for sale transactions which are below and above your set floor limit. If, as is normally required, the floor limit for your Service Establishment is set to zero, you do not need to carry out any tests on below floor limit values; this should be indicated on your completed test script.

Methods of Authorisation

American Express supports authorisation requests from the following types of device. Scripts (in brackets below) to test each of these are provided in Appendix C.

- Attended (C2): eg. retail or restaurant
- Unattended (C3): eg. car park payment terminal or self-service ticket machine
- Cardmember not Present (C4): eg. telephone order, mail order , internet
- Batch Authorisation (C4): eg. mail order

Refunds and Reversals

The American Express authorisation system is not set up to handle refund or APACS 30 reversal authorisation requests. Neither message type should be sent online; POS systems must be capable of processing refunds and reversals locally.

CID & AVS

The American Express product for Card Security Code and Address checking is known as CID (**C**ard **I**dentifier **D**igits) and AVS (**A**ddress **V**erification **S**ervice). Testing is required if you wish to implement this for American Express transactions; please contact Network Development for more information.

Authorisations

Requests for Certification

In order to request Authorisation certification, please complete the following forms provided in the appendices and return them to Network Development by post or fax, together with a covering request on company headed paper.

- *Request for Certification Form*
- *Indemnity and Request for Test Details*

Our address and fax number are given at the front of this document.

Test Cards

A standard set of test cards for testing attended POS systems contains 4 cards:

- one valid ANSI card
- one expired ANSI card
- two valid ISO 7813 cards

Test cards for testing unattended POS systems are slightly different – some are configured for particular transactions. A set comprises 7 cards:

- two valid ISO cards set up to authorise £1
- one valid ANSI card set up to authorise £1
- one valid ISO card set up to decline £1
- one valid ISO card set up to retain card £1
- one expired ISO card
- one valid ISO card set up to refer £1

Please do not use ordinary personal cards to carry out your tests or use the test cards to attempt to submit real transactions. Please ensure that transactions using the test card number are **not** submitted along with live data to American Express. Any transactions that are accidentally submitted on a live merchant number must be refunded.

Testing without Cards

If you are testing for Cardmember Not Present (CNP) transactions you do not require plastic test cards; we will contact you with test account details.

Sending the Results for Approval

The following documentation must be submitted to American Express before approval can be given.

- the completed test script(s)
- the receipts / vouchers / prints
- the completed receipt checklist

The Review Process

On receipt of all the testing documentation, American Express will review the results. Please allow two weeks for this review to take place.

Once the POS system has successfully fulfilled the requirements of all the tests, a certification letter from American Express will be issued approving its technical functionality. This letter will also contain live connectivity details.

It is important that live connectivity details are substituted for test details once testing is complete, otherwise the American Express authorisation service cannot be guaranteed.

Authorisations

Summary of the APACS Standard 30 Testing Process

	Merchant or Software Vendor	American Express Network Development	American Express Authorisation Testing Dept.
1	Contacts Amex to discuss certification.	Consultancy provided; Electronic Business Guide (this document) issued.	
2	Submits the Certification Request Form (by fax or e-mail) and Indemnity (by fax) to Network Development.	Project raised.	
3			Contacts merchant to arrange testing slot; issues test cards / test account number.
4	Agrees testing slot.		
5	Contacts Authorisation testing Dept. at agreed slot.		Starts authorisation trace.
6	Completes authorisation test script/s and submits results and receipts to Authorisation Testing Dept. for review.		
7			Reviews test scripts and receipts. Results approved or retest(s) required.
8			Testing completed. Approval letter issued.
9	Merchant proceeds to Submissions testing (if required) or 'go live'.		

Authorisations

Referrals and Exception Codes in the live environment

In the live environment American Express may return a referral in response to an authorisation request, and the POS device should be capable of displaying a code indicating the reason for the referral.

The following codes may be present in field 10 of the authorisation response message:

Code	Meaning
E1	Invalid Service Establishment number
E2	Invalid Cardmember number
E3	Invalid amount
E4	Card has expired
E5	Card is not yet valid
E6	Invalid POS system type
E7	Invalid message type
E8	Invalid format
E9	Timeout

If a referral of this kind is received in the live environment the transaction should not proceed until a manual Authorisation code has been obtained from American Express. The voice referral telephone number is

020 8551 1111

Submissions

This section documents the procedures for certifying both the file submission method and the format of the settlement file sent to American Express.

Submitting Data to American Express

The following certification must be completed before transmissions of live data can take place:

- File Submission Connectivity
- Data and File Format

American Express currently makes no charge for the certification service.

Testing Timescales

Please allow up to six weeks for testing submissions.

File Format Data Certification

APACS Standard 29 v.18 ('APACS 29') is the standard format for submitting transactions to American Express for processing. Please see Appendix E for our APACS 29 Technical Specification and Appendix L for a sample APACS 29 file layout.

If you wish to submit airline or car rental itinerary data, or submit via one of American Express's proprietary formats, please contact Network Development for further information.

Submission via Third Parties

If you plan to submit transactions via a Third Party please contact Network Development to discuss the options available and the testing required.

Communication Links

Chosen communication and connectivity protocols may depend on the following:

- CPU hardware and operating system
- preferred / available line type
- available communications protocols
- estimated traffic volumes

The American Express primary file Transmission platform is an IBM AS/400. We support the following:

Physical Links

- PSTN
- ISDN
- X.25 – TNS / BT
- Internet / VPN

Communications Applications

- FTP (File Transfer Protocol)
- C:D Connect Direct
- SIFT (Secure Internet File Transfer)
- XCOM 6.2

Protocols

- TCP / IP (Transmission Control Protocol / Internet Protocol)
- SNA (Systems Network Architecture)

Please contact us if your requirements are not met by the above.

Submissions

Summary of the File Submission Certification Process

	Merchant or Software Vendor	American Express Network Development	American Express Submissions Testing Dept.
1 *	Contacts Amex to discuss File Submission.	Consultancy provided; Electronic Business Guide (this document) issued.	
2 *	Submits Certification Request Form (by fax or e-mail) and Indemnity (by fax) to Network Development.	Project raised and ongoing consultancy provided.	
3			Contacts Merchant / Vendor to agree connectivity solution.
4	Configures system and builds test file.		Configures Amex system to receive test file.
5	Test file sent.		Test file received and reviewed.
6			Approved or retest required.
7	Submit retests as required.		
8	Second 'approved' test file submitted to prove connectivity and format.		Approval given to Merchant / Vendor via e-mail. Support documentation for live submissions issued.
9	Advise Amex when live submissions will start.		Set to live on Amex systems.

* If as part of your certification with us you have performed Authorisations testing, steps 1 and 2 above may have taken place as part of that process.

Submissions

Submitting Test Files

The first submission should contain:

- a minimum of 15 transaction
- a minimum of 2 batches
- A mixture of debit and credit transactions

All fields must be populated as detailed in the APACS file format specification in appendix E.

A list of test Cardmember and test Service Establishment (SE) numbers to create dummy transactions are given in Appendices F and G. Please advise which SE numbers you will be using in the submissions file.

Please allow two working days for processing and approval of each test file. When two test files have been successfully submitted and processed approval will be given. You will be advised when you can begin submitting live files.

Live Submissions during Testing

If you currently submit live data to us continue to use your existing live submission method until approval is given.

Adding New Service Establishments

If you wish to add new Service Establishment numbers after going live please contact American Express New Business on 0800 339911.

Details to be Obtained Before You Go Live

Before you begin the submission of live settlement files please provide American Express with details of a nominated contact for dealing with any submission-related issues.

Sending Live Settlement Files

You may submit a file at any time, every day of the year. Files are processed throughout the day.

Processing Times

Processing of settlement data takes place at fixed times as detailed below. **These times are for information only and subject to change without notice.**

Live

Monday to Friday	11:30 14:30 19.00 hrs
Saturday	16:00
Sunday	21:00

Test

Monday to Friday	11.00 13:00 15.00 17.00

Ongoing Support

If you experience problems submitting data once live please contact our Technologies Helpdesk on 01273 576040.

File Acknowledgements

Please see page 7 for information about our File Acknowledgement products and other ways to assist your data reconciliation.

Nil Return (empty) files

If your system automatically generates and transmits submissions files, even if there is no transaction data to submit, to avoid unnecessary rejection notifications please ensure it contains the following seven records:

VOL1
HDR1
HDR2
UHL1
EOF1
EOF2
UTL1

Submissions

Preparing Submissions

The following details must be provided for each transaction contained in the submission:

- The Service Establishment number, name and abbreviated address for each branch
- The Cardmember number, transaction amount, transaction date and transaction reference
- A brief, meaningful description of the goods or services supplied, to appear on Cardmembers' monthly statements. This will differ depending on the type of outlet, as defined in Segment 3 of the transaction details. See page 16 for more details on this Descriptive Data.

General Rules

- A batch must only contain one Service Establishment number
- The only limit to the number of transactions which may be included in a Net Summary is that the total net amount expressed in pence must not exceed 11 digits in length
- Sales and refunds may be included in a single batch, or divided between batches.

Data Validation

Before submitting the transactions, you must:

- Ensure that the Service Establishment number corresponds to the branch where the transaction took place
- Validate the check digit of every Service Establishment. Please see Appendix H
- Ensure that only American Express Transactions are contained in the file. All American Express Cardmember numbers start with **34** or **37**
- Validate the check digit of Cardmember numbers. Please see Appendix H
- Remove all invalid Cardmember numbers and zero-value transactions from the submission.

Data Reconciliation

- Each batch of transaction records (n1/n2) must be aggregated into a Net Summary Record
- All Net Summary Records (n4/n5) must reconcile by value and number with the preceding batch
- Net Summary Records must be aggregated into a Net Claim Record *
- The Net Claim Record (n7/n8) must reconcile by value and number with the preceding Net Summary Records
- The UTL1 Trailer Record must reconcile with the Net Claim Record.

Any file that does not self-reconcile will be rejected.

* If the file is multi-currency there must be one Net Claim Record per Net Summary Record.

Duplicate Data

Please refer to Appendix J if you think you have submitted duplicate transactions to American Express.

Submissions

Submission Records

Most records within an APACS29 submission file are the same for all industry types.

There is, however, some variation within the transaction record segment 3 (positions 174 - 380). This is because some industries require different levels of descriptive information to be returned to the customer. The descriptive information from the transaction records of these charge formats appears on our Cardmembers' monthly statements. Statement examples are given on the following page.

Retail Format and **General** Format are the charge formats currently available within the APACS 29 file standard.

A full Technical Specification of the contents and format of the fields in segment 3 is provided in Appendix E.

Retail Format

This format has been designed to meet the needs of Retail establishments and contains the following:

- Tax and discount fields are available on the transaction record and appear on our Cardmembers' statements, enabling them to view net tax and any discount on items bought

- Up to six purchases may be itemized by quantity, department and value. At least one set of purchase details must be included for each transaction, to appear on the Cardmember statement.

See transaction number 1 in the following statement, for an example of suitable descriptive data which shows useful information about the purchase. Transaction number 2 shows how insufficient descriptive data can cause confusion to Cardmembers and increase the likelihood of queries and chargebacks.
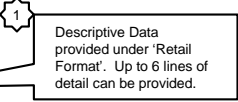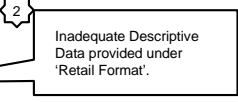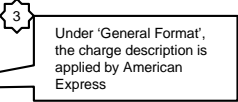
General Format

This format has been designed to provide detailed records for Service Establishments who do not fall into the 'Retail' category.

The descriptive information that appears on Cardmembers' statements is applied by American Express (transaction 3 in sample statement) and is **not** picked up from the file. Although it will not appear on the statement, we will be unable to process your file unless some basic descriptive information is provided.

Submissions

Example Cardmember Statement

Details	Foreign Spending	Amount £
22 May Payment received. Thank you. Reference 252465		1,250 CR
1 June HARRINGTONS DEPARTMENT STORE Qty Description 1 Linens 3 Childrenswear Reference 34280184 1 00	⟨1⟩ Descriptive Data provided under 'Retail Format'. Up to 6 lines of detail can be provided.	104.89
7 June JONES BROS, BRIGHTON Goods Reference 1280184 1 00	⟨2⟩ Inadequate Descriptive Data provided under 'Retail Format'.	35.50
12 June CASA NOSTRA, LONDON Restaurant Reference 4983098 1 00	⟨3⟩ Under 'General Format', the charge description is applied by American Express	53.87
Total New Transactions for JOHN SMITH		194.26

List of Appendices

A   Request for certification – non EMV

Please complete and return to your Network Development contact by e-mail or fax (01273 525833).

Company Name	
Merchant / Establishment number (10 digits)	
Address (for test card despatch)	

Technical contact name		Telephone number		E-mail address	
Software supplier contact		Telephone number		E-mail address	

Certification Type Requested (please tick as appropriate):

Authorisation		Submission Connectivity		Submission File Data	
Approximate target live date					

Authorisation Testing:
NB: If you are conducting Authorisation Testing, you will need either Test Cards or a Test Account Number. Please complete the *Indemnity and Request for non-EMV Test Details* in the next appendix and send in addition to this request.

Card member Present (script C2)	Yes / No
Unattended (script C3)	Yes / No
Batch Authorisation (script C4)	Yes / No
Cardmember not present (script C4)	Yes / No
Continuous Authority	Yes / No
Proposed auths connectivity (eg: ISDN, PSTN, X25, Paknet)	

Submission File Connectivity:

Are you currently sending electronic submissions to American express?	Yes / No
If yes, do you **currently** submit to us direct or via a third party (eg Bank acquirer, payment solution provider) ?	Direct / other (give details)
What is your **proposed** submission route (that to be tested / certified ?)	Direct / other (give details)
Proposed File Transmission Software	
Proposed connectivity (eg: ISDN, PSTN, X25, Paknet)	

Submission File Data Certification:

What Submission format will you use ? (eg AMEX 8, AMEX 11, APACS29 / IBRO, AFIA)	
Which File format will you use (if known) ? (General, Retail, Car Rental, Airline, Telecom)	

Do you wish to test for currencies other than £ Sterling ?	Yes / No
If *yes* please give details (eg EUR, USD etc)	

B   Indemnity & Request for Test Details – non EMV

This Indemnity Form is an undertaking of responsibility for the treatment and use of American Express test account numbers. The form should be completed and returned to us, by **fax or post** as detailed at the beginning of this guide, together with an additional request on your company's letterhead paper.

If you are developing equipment or software for a specific client, American Express requires a copy of the Indemnity Form signed by the person who will take responsibility for the account number. This could be the person carrying out the testing, or the tester's client.

On receipt of the completed and signed indemnity form American Express will arrange to issue the test cards or test account number to you.

In consideration of American Express Europe Limited ("American Express") supplying to you the following for use by you in POS system testing:

- One set of four white test American Express Cards for use when testing *attended* POS systems and / or
- One set of seven white test American Express Cards for use when testing *unattended* POS systems and / or
- Test Card account number for use when testing *Cardmember not Present* POS systems

the undersigned agrees:

- That while the test Cards / Card account number are/is not in active use, to keep them/it in maximum security in a safe;
- To control access to the test Card(s)/Card account number, and to appoint one or more specifically named individuals to assume responsibility for control of same;
- To pay American Express and be responsible for any charges improperly incurred on the test Card(s)/Card account number, acknowledging that, although the Card account numbers are not valid, it is not always within the power of American Express to prevent transactions being effected;
- To immediately notify American Express of the theft or loss of the test Cards / Card account number, or disclosure of same to any unauthorised third party;
- To return the test Cards / Card account number to American Express on demand, or to destroy them/it upon instructions of American Express;
- To retain as confidential any information obtained about the American Express Card service which is not a matter of public record and not to disclose the same to any third party without the express written permission of American Express; and
- To ensure that all your employees, agents or sub-contractors who have access to the Test Cards / Card account number comply fully with the terms of this letter.

Accepted on behalf of: ………………………………………………………………………………………….
Full legal name of Service Establishment

Signature: ……
Person responsible for the control of the Test Cards / Account number

Name: ………………………………………………………………………………………………..…………
Name printed

Position held: …..…………………………………………..   Date: …………………………………………

C   Authorisation Test Scripts

Completing the Tests

Take the following steps to complete the tests required to certify your system:

Step	Action	Complete ?
1	Schedule testing with American Express Authorisation Testing Team.	
2	Set up the POS system, as described in this appendix.	
3	Copy/print the POS System Detail Form (appendix C1) and complete it.	
4	Select the appropriate test script(s), copy/print and complete it.	
5	Record the actual results obtained during testing on the script in the **Actual Text Received** or appropriate column, and add any comments which may be needed to clarify test results, eg. if the test floor limits were used.	
6	Collate all receipts/vouchers/prints produced during testing, numbering each one with the test script number of the test that produced it.	
7	Attach them to the test script(s).	
8	Complete the appropriate Receipt Checklist for Cardmember-present and unattended systems.	
9	Submit all documentation to the American Express Authorisation Testing Area.	

C   Authorisation Test Scripts

The table below details the authorisation test scripts in this appendix.

You will only have to complete those applicable to your set-up, but all testers must complete Form C1 – POS System Detail Form, plus at least one of the following scripts - C2, C3 or C4.

All Cardmember-present testers must, in addition, complete a **Receipt Checklist** (see this appendix).

Code	Script Title	Function
C1	POS System Detail Form	Form identifying your POS system type (appendix C1). **Must be completed by all testers.**
C2	Functionality Script for Attended POS systems	Test used for all attended POS systems with on-line authorisation facility where the Cardmember is present, e.g. retail, restaurant environment. Includes **receipt checklist**.
C3	Functionality Script for Unattended POS systems	To be used only for POS systems that are Cardmember operated and not attended by Merchant staff, e.g. card-operated petrol pumps, car-park payment. Includes **receipt checklist**.
C4	Functionality Script for Cardmember Not Present POS systems	To be used for any scenario where the Cardmember is not present as the transaction takes place, e.g. telephone/mail/internet ordering. This script can also be used to test Batch Authorisation functionality.

Glossary of terms used in this appendix:

Test Details	Determines what should be entered at the point of sale. It is important to enter the test transaction exactly as specified to generate the correct response from Amex.
Request Message Type	The request message type, which should be sent to American Express, as detailed in the APACS specification.
Expected Response Message Type	The response message type that American Express will return, as detailed in the APACS specification.
Expected Amex Response Code	The code which will be returned by American Express in response to the sent message.
Expected Amex Response Text	The text that will be sent as part of the response message.
Text received	The actual text received at the point of sale.
Transaction sequence number	Generated by the POS system and submitted to American Express. Will be returned in the same format in the response message.
Transaction receipt number	The number printed on the receipt, or audit print. Created by the POS system.
Receipt date and time	The details printed on the receipt, or audit print. Created by the POS system.

C   Authorisation: POS Configurations

POS System configuration for APACS30 testing:

Test Merchant Number	942 582 173 3
Default Voice Referral Number	020 8551 1111

PSTN	**Test Telephone Number 300 bps**	0800 3855072
	Test Telephone Number 2400 bps	0800 3855272
	Test NUA	72

ISDN	**Primary Telephone Number**	0800 3855406
	Test NUA	77770000000503

BT X.25	**Test NUA primary**	23423230012805
	Test NUA secondary	23423230013005

TNS (PSINET) X.25	**Test NUA**	77770000000503

Batch Authorisation PSTN	**Primary Telephone Number**	0800 3855222
	Test NUA	77772222122

Batch Authorisation ISDN	**Primary Telephone Number**	0800 3855422
	Test NUA	77772222122

Non-0800 Users: if you are unable to use any of these connections please contact Network Development.

Test Values

American Express test accounts are set up to generate standard responses to the following specific values. If you use values other than these you will not get the correct responses when testing.

Test floor limit *	**£5.00**
Test amount for values below floor limit	£4.00
Test amount for approvals	£8.00
Test amount for voice referral	£10.00
Test amount for deny response	£11.00
Test amount for pick-up card response	£12.00

* If the floor limit for your Service Establishment is set to zero you do not need to carry out any tests on below floor limit values; please indicate this on the test script.

C1 POS System Detail Form

Please complete this form to identify your POS system type and return to us with your test results:

	Please complete this column with details for the POS system.
POS system type	
Model	
Software version	
Method of authorisation (ie PSTN, Paknet, ISDN, X.25)	
Details (Attended/Unattended/ Cardmember Not Present/ Batch Authorisation etc)	
Tested by	
Company	
Signature	
Date	
Comments:	

C2 Script for Attended POS Systems

This script should be used where an Operator makes single authorisation transactions from a POS system at which the card is presented.

If your floor limit is zero you will not need to complete the below floor limit tests. Please indicate this on the test script.

Note: Remember to zero balance all transactions after each test.

For these tests the floor limit should be set to £5.00.

SWIPED TESTS – ANSI CARDS

Test No	Test Details	Request Message	Expected Response Message from Amex	Expected Amex Response Code	Expected Amex Response Text	Actual Text Received	Transaction Sequence Number	Receipt Number	Receipt Date and Time
1	Swipe valid ANSI card for transaction amount below your floor limit. Sale: £4	Not sent on-line	-	-	Locally generated by POS system – approved.				
2	Swipe valid ANSI card for transaction amount above your floor limit. Sale: £8	10	12	00	"AUTH CODE: NN"				
3	Swipe valid ANSI card for reversal. Reversal: £8	Not sent on-line	-	-	Locally generated by POS system – reversal approved.				

4	Swipe valid ANSI card for a voice referral. Sale: £10	10	12	02	"CALL AMEX: NNNN" - A 4 digit reference which should be quoted when the operator calls the Amex authorisation number 020 8 551 1111.			
5	Swipe valid ANSI card for a "deny" response. Sale: £11	10	12	05	"DECLINE"			
6	Swipe valid ANSI card for a "deny and pick up" response. Sale: £12	10	12	05	"PICK UP CARD"			
7	Swipe expired ANSI card for transaction amount above your floor limit. Sale: £8	Not sent on-line	-	-	Locally generated by POS system – "Card Expired" or similar displayed.			
8	Swipe valid ANSI card for refund, value above your floor limit. Refund: £8	Not sent on-line	-	-	Locally generated by POS system by POS system – refund approved.			
9	Swipe valid ANSI card for refund reversal, value above your floor limit. Refund reversal: £8	Not sent on-line	-	-	Locally generated by POS system by POS system – refund reversal approved.			

C2 Script for Attended POS Systems

SWIPED TESTS – ISO CARDS

Test No	Test Details	Request Message	Expected Response Message from Amex	Expected Amex Response Code	Expected Amex Response Text	Actual Text Received	Transaction Sequence Number	Receipt Number	Receipt Date and Time
10	Swipe valid ISO card one for transaction amount below your floor limit. Sale: £4	Not sent on-line	-	-	Locally generated by POS system by POS system – approved.				
11	Swipe valid ISO card one for transaction amount above your floor limit. Sale: £8	10	12	00	"AUTH CODE: NN"				
12	Swipe valid ISO card one for reversal. Reversal: £8	Not sent on-line	-	-	Locally generated by POS system by POS system – reversal approved.				
13	Swipe valid ISO card one for a voice referral. Sale: £10	10	12	02	"CALL AMEX: NNNN" A 4 digit reference which should be quoted when the operator calls the Amex authorisation number 0181 551 1111.				

C2 Script for Attended POS Systems

Test No	Test Details	Request Message	Expected Response Message from Amex	Expected Amex Response Code	Expected Amex Response Text	Actual Text Received	Transaction Sequence Number	Receipt Number	Receipt Date and Time
14	Swipe valid ISO card one for a "deny" response. Sale: £11	10	12	05	"DECLINE"				
15	Swipe valid ISO card one for a "deny and pick up" response. Sale: £12	10	12	05	"PICK UP CARD"				
16	Swipe valid ISO card one for refund, value above your floor limit. Refund: £8	Not sent on-line	-	-	Locally generated by POS system by POS system – refund approved.				
17	Swipe valid ISO card one for refund reversal, value above your floor limit. Refund reversal: £8	Not sent on-line	-	-	Locally generated by POS system by POS system – refund reversal approved.				
18	Swipe valid ISO card two for transaction amount above your floor limit. Sale £8	10	12	00	"AUTH CODE: NN"				
19	Swipe valid ISO card two for reversal. Reversal: £8	Not sent on-line	-	-	Locally generated by POS system by POS system – reversal approved.				

C2 Script for Attended POS Systems

KEYED TESTS – ANSI CARDS

Test No	Test Details	Request Message	Expected Response Message from Amex	Expected Amex Response Code	Expected Amex Response Text	Actual Text Received	Transaction Sequence Number	Receipt Number	Receipt Date and Time
20	Swipe valid ISO card two for refund, value above your floor limit. Refund: £8	Not sent on-line	-	-	Locally generated by POS system by POS system – refund approved.				
21	Key valid ANSI card for transaction amount below your floor limit. Sale: £4	Not sent on-line	-	-	Locally generated by POS system by POS system – approved.				
22	Key valid ANSI card for transaction amount above your floor limit. Sale: £8	20	12	00	"AUTH CODE: NN"				
23	Key valid ANSI card for reversal. Reversal: £8	Not sent on-line	-	-	Locally generated by POS system by POS system – reversal approved.				
24	Key valid ANSI card for a voice referral. Sale: £10	20	12	02	"CALL AMEX: NN"				
25	Key valid ANSI card for a "deny" response. Sale: £11	20	12	05	"DECLINE"				

C2 Script for Attended POS Systems

Test No	Test Details	Request Message	Expected Response Message from Amex	Expected Amex Response Code	Expected Amex Response Text	Actual Text Received	Transaction Sequence Number	Receipt Number	Receipt Date and Time
26	Key valid ANSI card for a "deny and pick up" response. Sale: £12	20	12	05	"Declined. Pick up card"				
27	Key expired ANSI card for transaction amount above your floor limit. Sale: £8	Not sent on-line	-	-	Locally generated by POS system – "Card Expired" or similar displayed.				
28	Key valid ANSI card for refund, value above your floor limit. Refund: £8	Not sent on-line	-	-	Locally generated by POS system by POS system – refund accepted.				
29	Key valid ANSI card for refund reversal, value above your floor limit. Refund reversal: £8	Not sent on-line	-	-	Locally generated by POS system – refund reversal approved.				

C2 Script for Attended POS Systems

RETRY TESTS

The configuration needs to be reset before completing these tests:

PSTN   Primary   Secondary

300 Baud   0800 3844006   0800 3855072
2400 Baud   0800 676233   0800 3855272

NUA - 72

ISDN   Primary   Secondary
               0800 211246   0800 211245

SWIPED RETRY TESTS

30	Sale retry. Swipe ANSI card for £8.00	16	12	00	"AUTH CODE: NN"				
31	Sale retry. Swipe ISO card for £8.00	16	12	00	"AUTH CODE: NN"				

KEYED RETRY TESTS

32	Sale retry. Key ANSI card for £8.00	26	12	00	"AUTH CODE: NN"				

C2 Receipt Checklist for Attended POS Systems

The following details are **mandatory** on every receipt produced at an attended POS system.
Please complete the checklist before returning the test results to American Express.

Please attach your vouchers/receipts to the checklist, marking each receipt/voucher with the number of the test which generated it.

Mandatory requirements	Please tick
American Express Merchant number	
Service Establishment/Outlet name	
Service Establishment/Outlet address	
Transaction type, displayed as "Sale" or "Refund"	
Card scheme name (American Express)	
Cardmember number (PAN)	
Expiry date of the card (MMYY)	
Date of transaction	
Time of transaction	
POS system identifier / Terminal ID	
Transaction number	
Transaction response, e.g. authorisation code	
Value of transaction	
Request for signature	
Space for signature	
Indicator of keyed entry, e.g. "K" or "Keyed"	

Optional information	Please tick
Diagnostic message	
VAT registration number	
Retention reminder	
Courtesy message	
Receipt number	

Tandem Printing Requirements

Many POS systems and electronic imprinters do not print multi-part receipts. They use single-ply paper and print the Service Establishment copy first, and then the Cardmember copy.

The details listed in the previous section must appear on both copies, with the exception of the following which must appear on the Service Establishment's copy but are not required on the Cardmember's copy:

- Request for Cardmember signature
- Space for Cardmember signature.

The retention reminder must appear on the Cardmember's copy but is not required on the Service Establishment's copy.

C3 Script for Unattended POS Systems

Unattended POS system Requirements

Based on agreed UK industry guidelines, American Express requires the following standards to be met in the functionality of unattended POS systems:

- A separate Unattended POS system Agreement must be signed
- Zero floor limit and full on-line authorisation to be used
- The POS system type must be flagged as 'unattended' in the authorisation request
- Motorised card readers with card-capture facility to be used
- Petrol pumps:
  - Pre-authorisation amount £1
  - Maximum transaction amount £50, unless otherwise agreed with American Express
- All other unattended POS system types:
  - Authorise full transaction value up to agreed ceiling
    eg.Self service ticket machines - £300, Car parks - £130.

Procedures identified as Best Practice:

- Velocity checking
- Receipt offered, not mandatory.

The POS system type must be flagged as 'unattended' in the authorisation request message.

C3 Script for Unattended POS Systems

Test No	Test Details	Request Message	Expected Response Message from Amex	Expected Amex Response Code	Expected Amex Response Text	Actual Text Received	Transaction Sequence Number	Receipt Number	Receipt Date and Time
1	Swipe Card 1 for authorisation Transaction value: £1	10	12	00	"AUTH CODE: NN" "Transaction processed" or similar displayed.				
2	Swipe Card 2 for authorisation Transaction value: £1	10	12	00	"AUTH CODE: NN" "Transaction processed" or similar displayed.				
3	Swipe Card 3 for authorisation Transaction value: £1	10	12	05	"AUTH CODE:NN" "Transaction processed", or similar displayed.				
4	Swipe Card 4 for a decline response. Transaction value: £1	10	12	05	"DECLINE" "Please pay at kiosk", or similar message displayed.				
5	Swipe Card 5 for a deny and pick up response. Transaction value: £1	10	12	04	Card retained by POS system. "Card retained" or similar displayed.				
6	Swipe Card 6 – expired card. Transaction value: £1	Non sent on-line	-	-	Locally generated by POS system. "Card Expired" or similar displayed.				
7	Swipe Card 7 for a referral. Transaction value: £1	10	12	02	Transaction referred. "Please pay at kiosk" or similar displayed.				

C3 Receipt Checklist for Unattended POS systems

The following details are mandatory on any receipt produced from an Unattended POS system. Please complete the checklist before returning the test results to American Express. The production of a receipt should be offered to the Cardmember, rather than being automatically produced.

Please attach your vouchers/receipts to the checklist, marking each receipt/voucher with the number of the test which generated it.

Mandatory requirements	Please tick
American Express Merchant number	
Service Establishment/Outlet name	
Service Establishment/Outlet address	
Transaction type, displayed as "Sale" or "Refund"	
Card scheme name (American Express)	
Cardmember number (PAN)	
Expiry date of the card (MMYY)	
Date of transaction	
Time of transaction	
POS system identifier	
Transaction number	
Transaction response, e.g. authorisation code	
Value of transaction	

Optional information	Please tick
VAT registration number	
Retention reminder	
Diagnostic message	

C4 CNP POS systems & Batch Authorisation

This script should be used where an Operator makes single authorisation transactions from a POS system at which the Cardmember is not present (CNP - mail / telephone order, internet).

For these tests, please use a floor limit of £5.00. If your 'live' floor limit is zero you will not need to complete the below floor limit tests. Please indicate this on the test script.

Note: Remember to zero balance all transactions after each test.

Keyed Tests

Since the card is never presented, no swiped tests are required.

Batch Authorisation

This script may also be used to test Batch Authorisation functionality. Please see the instructions at the end of the script.

Test No	Test Details	Request Message	Expected Response Message from Amex	Expected Amex Response Code	Expected Amex Response Text	Actual Text Received	Transaction Sequence Number	Receipt Number	Receipt Date and Time
1	Key valid card details for transaction. Sale: £8	09	12	00	"AUTH CODE: NN"				
2	Key valid card details for reversal. Reversal: £8	Not sent on-line	-	-	Locally generated by POS system – reversal approved.				
3	Key valid card details for a voice referral. Sale: £10	09	12	02	"CALL AMEX: NN"				
4	Key valid card details for a "deny" response. Sale: £11	09	12	05	"DECLINE"				
5	Key valid card details for a "deny and pick up" response. Sale: £12	09	12	05	Message is "PICK UP CARD". POS system should interpret as "Declined"				

6	Key expired card details for transaction. Sale: £8	Not sent on-line	-	-	Locally generated by POS system. "Card Expired" or similar displayed.				
7	Key valid card details for refund. Refund: £8	Not sent on-line.	-	-	Locally generated by POS system – refund approved.				
8	Key valid card details for refund reversal. Refund reversal: £8	Not sent on-line	-	-	Locally generated by POS system – refund reversal approved.				

RETRY TESTS

The configuration needs to be reset before completing these tests:

PSTN	Primary	Secondary
300 Baud	0800 3844006	0800 3855072
2400 Baud	0800 676233	0800 3855272

NUA - 72

ISDN	Primary	Secondary
	0800 3844006	0800 3855422

10	Sale retry Cardmember not present. Key ANSI card for £8.00	45	12	00	"AUTH CODE: NN"				

Batch Authorisation

If you wish to use this script to test Batch Authorisation functionality you may repeat the tests above as many times as you require. Please ensure that your system is configured according to the communications set-up as follows:

PSTN   0800 3855222   NUA = 77772222122

ISDN   0800 3855422   NUA = 77772222122

D   APACS 30 Authorisation Request

APACS Standard 30 v.18 - Authorisation Request Message

- The American Express host will accept authorisation requests in ASCII 7-bit even or ASCII 8-bit no parity characters. However, the response will always be in ASCII 7-bit even parity.
  Note: All POS systems operate in even parity.

- There are no security provisions in APACS Standard 30. Messages are transmitted un-encrypted .

Key:

F = Fixed length field
V = Variable length field
FS = Field Separator character
US = Unit Separator character

Field	Field Name & Description	Size	Format	Requirement
0	**DIAL INDICATOR** - The number of attempts made to establish contact with the American Express host.	1	F	Required
1	**POS SYSTEM IDENTITY** - The unique fixed terminal identity number.	8	F	Required
2	**MESSAGE NUMBER** - The four digit message sequence number generated by the client when the request was sent, starting at 0000, where 9999 + 1 = 0000.	4	F	Required

3	**POS SYSTEM TYPE** - A four digit code defining the POS system attributes:
	Digit 1 - Indicates whether the POS system has a magnetic stripe reader. It is assumed that all POS systems are merchant operated.
	    1 = ICC Chip card reader
	    2 = Magnetic stripe reader
	    3 = Both Magnetic Stripe and ICC readers
	    4 = No card reader
	Digit 2 - The number of 16 character lines to be displayed or printed.
	    1 = One line
	    2 = Two lines
	    3 = Three lines
	    4 = Four lines
	    5 = Five lines
		4	F	Required

D APACS 30 Authorisation Request

Field	Field Name & Description	Size	Format	Requirement
3	Digit 3: Indicates POS ability to process response messages	4	F	Required

Digit	Online Download Of Tel No.	Hold Capability	On line Download Of Date & Floor Limit	AVS Functionality
0	No Special Features			
1	Yes	No	No	No
2	No	Yes	No	No
3	Yes	Yes	No	No
4	No	No	Yes	No
5	Yes	No	Yes	No
6	No	Yes	Yes	No
7	Yes	Yes	Yes	No
8	No	No	No	Yes
9	Yes	No	No	Yes
A	No	Yes	No	Yes
B	Yes	Yes	No	Yes
C	No	No	Yes	Yes

Digit 4: indicates additional device features and capabilities

Value	Unattended Device	PIN Pad available	POS system able to capture cards
0	No additional information available		
1	Yes	No	No
2	No	Yes	No
3	Yes	Yes	No
4	No	No	Yes
5	Yes	No	Yes
6	No	Yes	Yes
7	Yes	Yes	Yes
8	No	No	No

Field	Field Name & Description	Size	Format	Requirement
4	**MESSAGE TYPE** - Two digit indicator of the message type. 10 = Swiped sale first attempt 16 = Swiped sale retry 20 = Keyed sale first attempt 26 = Keyed sale retry 09 = Keyed sale first attempt – Cardmember not present 45 = Keyed sale retry – Cardmember not present A0 = Continuous Authority first attempt A1 = Continuous Authority retry A8 = Sale (E-com) Card first attempt A9 = Sale (E-com) Card retry B2 = Sale (E-com) keyed first attempt B3 = Sale (E-com) keyed retry **There are no special requirements for EMV transactions.**	2	F	Required

D   APACS 30 Authorisation Request

Field	Field Name & Description	Size	Format	Requirement
5	**SERVICE ESTABLISHMENT NUMBER**	15	V	Required
6	FS	1	F	Required
7	**CARD DETAILS** – All characters from the track 2 image on the chip	40	V	Required
8	FS	1	F	Required
9	**AMOUNT** - In pence. Minimum of 2 digits.	11	V	Required
10	**FS**	1	F	Required
11	**DESCRIPTIVE ADDRESS DATA** (please request our CID & AVS addendum to this guide if you use Address and Card Security Code checking)	16	V	Optional
12	FS	1	F	Required
13	Reserved	-	-	-
14	FS	1	F	Required
15	Reserved	-	-	-
16	FS	1	F	Required
17	**CASH AMOUNT**	11	V	Optional
18	FS	1	F	Required
19	**TRANSACTION DATE & TIME (YYMMDDhhmm)**	10	F	Required
20	FS	1	F	Required
21	**EMV TERMINAL TYPE** – Two digit code specified in EMV specifications for EMV terminals and specified in APACS for e-commerce transactions <table><tr><td rowspan="2">Environment</td><td colspan="3">Operational Control provided by:</td></tr><tr><td>Financial Institution</td><td>Merchant</td><td>Cardholder</td></tr><tr><td>Attended</td><td></td><td></td><td></td></tr><tr><td>Online only</td><td>11</td><td>21</td><td>-</td></tr><tr><td>Offline with online capability</td><td>12</td><td>22</td><td>-</td></tr><tr><td>Offline only</td><td>13</td><td>23</td><td>-</td></tr><tr><td>Unattended</td><td></td><td></td><td></td></tr><tr><td>Online only</td><td>14</td><td>24</td><td>34</td></tr><tr><td>Offline with online capability</td><td>15</td><td>25</td><td>35</td></tr><tr><td>Offline only</td><td>16</td><td>26</td><td>36</td></tr></table>	2	F	Required for ICC and e-commerce transactions
22	FS	1	F	Required
23	**TERMINAL COUNTRY CODE:** the ISO code for the country where the transaction originated.	3	F	Required for ICC
24	FS	1	F	Required

D APACS 30 Authorisation Request

Field	Field Name & Description	Size	Format	Requirement
25	**TRANSACTION CURRENCY CODE**: the ISO currency of the authorisation transaction. '826' in the UK only. Request our Multi-currency addendum for other currency codes.	3	F	Required
26	FS	1	F	Required
27	**REASON ON-LINE CODE (EMV)** Used by the acquirer to determine if stand in authorisation would be an appropriate action for the transaction (ie: ICC or Card Accepting Device requiring online authorisation.) Values from ' 00' - '11'	2	F	Required
28	FS	1	F	Required
29	**EMV AUTHORISATION REQUEST DATA**	156	V	Required
29.1	Authorisation request cryptogram (ARQC)	16	F	Required
29.2	Application interchange profile (AIP)	4	F	Required
29.3	Application transaction counter (ATC)	4	F	Required
29.4	Unpredictable number	8	F	Required
29.5	Terminal verification results (TVR)	10	F	Required
29.6	Cryptogram transaction type	2	F	Required
29.7	Issuer application data	64	V	Required
29.8	US	1	F	Required
29.9	Application identifier (AID)	32	V	Required
29.10	US	1	F	Required
29.11	Application version number	4	F	Required
29.12	US	1	F	Required
29.13	Cryptogram information Data	2	F	Required
29.14	US	1	F	Required
29.15	CVM Results	6	F	Required
30	FS	1	F	Required

D   APACS 30 Authorisation Response / Hold

- A response or hold message is given in response to an authorisation request.

Field	Field Name & Description			Size	Format	Requirement
0	DIAL INDICATOR – The number of attempts made to establish contact with the American Express host.			1	F	Required
1	POS SYSTEM IDENTITY – The unique fixed Terminal Identity number (TID).			8	F	Required
2	MESSAGE NUMBER – The four digit message sequence number generated by the client when the request was sent, starting at 0000, where 9999 + 1 = 0000.			4	F	Required
3	MESSAGE TYPE – Two digit indicator of the message type: 12 = Auth response 81 = Hold			2	F	Required
4	ACQUIRER RESPONSE CODE			2	F	Required
	Response Code	Message	Interpretation			
	00	AUTH CODE:nn	The transaction is authorised. American Express responds with a two digit authorisation code.			
	02	HOLD FOR AMEX (for auto-dial POS systems) or PLEASE CALL nnnn (for POS systems without auto-dial)	A voice referral is required. If American Express cannot supply an authorised or declined code within 20 seconds, a referral code is given. If the POS system has an auto-dial facility, it dials American Express. A unit separator (hex 1f) on its own is downloaded to make the POS system dial its internal default number. This should be 0208 551 1111, the number for the American Express Authorisations Centre. If no auto-dial facility is available, American Express sends a four digit code to the POS system. The operator must contact American Express manually and quote the code. If the charge is authorised, American Express gives a code to be manually input into the POS system.			
	05	DECLINE or PICK UP CARD	The transaction is declined. The message text displayed on the POS system may request that the branch retain the card.			
	04	PICK UP CARD (for unattended POS systems only)	The transaction is declined. The POS system retains the card. This will only be used when the POS system has identified itself as 'unattended'.			
	30	EXCEPTION	A voice referral is required, due to invalid or insufficient details.			

D   APACS 30 Authorisation Response / Hold

Field	Field Name & Description	Size	Format	Requirement
5	CONFIRMATION REQUEST	1	F	Required
6	AUTHORISATION CODE	9	V	Optional
7	FIELD SEPARATOR (FS)	1	F	Required
8	AMOUNT – In pence. Minimum of 2 digits.	11	V	Optional
9	FS	1	F	Required
10	MESSAGE – This may include a referral queue number. Includes authorisation code, if given.	80	V	Required
11	FS	1	F	Required
12	REFERRAL TELEPHONE NUMBER – The number that should be called by the Service Establishment in the case of a referral.	16	V	Optional
13	FS	-	F	Optional
14	FLOOR LIMIT - A set amount, above which transactions must go on-line for authorisation. Assigned for each Service Establishment.	3	V	Optional
15	FS	1	F	Optional
16	DATE – In format YYMM.	4	F	Optional
17	FS	1	F	Optional
18	EMV Response Data	83	V	Required
18.1	Issuer Authentication Data	32	V	Required
a	Application Response Cryptogram (ARPC)	16	F	Required
b	Optional Additional Data	16	V	Optional
18.2	US	1	F	Required
18.3	Issuer Script Data	256	V	Optional
19	FS	1	F	Optional
20	Response Additional Data	6	F	Optional
21	FS	1	F	Optional

D   APACS 40 Authorisation Request

APACS Standard 40 v.18 - Authorisation Request Message

- The American Express host will accept authorisation requests in ASCII 7-bit even or ASCII 8-bit no parity characters. However, the response will always be in ASCII 7-bit even parity.
  Note: All POS systems operate in even parity.

Key:

F = Fixed length field
V = Variable length field
FS = Field Separator character
US = Unit Separator character

Field	Field Name & Description	Size	Format	Requirement
0	DIAL INDICATOR - The number of attempts made to establish contact with the American Express host.	1	F	Required
1	POS SYSTEM IDENTITY - The unique fixed terminal identity number.	8	F	Required
2	MESSAGE NUMBER - The four digit message sequence number generated by the client when the request was sent, starting at 0000, where 9999 + 1 = 0000.	4	F	Required

3	POS SYSTEM TYPE - A four digit code defining the POS system attributes:
	Digit 1 - Indicates whether the POS system has a magnetic stripe reader. It is assumed that all POS systems are merchant operated. For information on Cardmember Activated POS systems, please see Section 3.
	    1 = EMV Chip card reader
	    2 = Magnetic stripe reader
	    3 = Both Magnetic Stripe and EMV readers
	    4 = No card reader
	Digit 2 - The number of 16 character lines to be displayed or printed.
	    1 = One line
	    2 = Two lines
	    3 = Three lines
	    4 = Four lines
	    5 = Five lines
		4	F	Required

D   APACS 40 Authorisation Request

Field	Field Name & Description	Size	Format	Requirement
3	Digit 3 - Indicates the POS system's ability to process response messages			
3	Digit 4 - Used to indicate additional features and capabilities of the authorisation device.			
4	MESSAGE TYPE: two digit indicator of the message type – please see APACS 30 format guide.	2	F	Required
5	SERVICE ESTABLISHMENT NUMBER	15	V	Required
6	FIELD SEPARATOR (FS)	1	F	Required
7	CARD DETAILS – All characters from the track 2 image on the chip	40	V	Required
8	FS	1	F	Required
9	AMOUNT - In pence. Minimum of 2 digits.	11	V	Required
10	FS	1	F	Required
11	DESCRIPTIVE ADDRESS DATA	16	V	Required
12	FS	1	F	Required

Field 3 (Digit 3) detail table:

Digit	Online Download Of Tel No.	Hold Capability	On line Download Of Date & Floor Limit	AVS Functionality
0	No Special Features			
1	Yes	No	No	No
2	No	Yes	No	No
3	Yes	Yes	No	No
4	No	No	Yes	No
5	Yes	No	Yes	No
6	No	Yes	Yes	No
7	Yes	Yes	Yes	No
8	No	No	No	Yes
9	Yes	No	No	Yes
A	No	Yes	No	Yes
B	Yes	Yes	No	Yes
C	No	No	Yes	Yes

Field 3 (Digit 4) detail table:

Value	Unattended Device	PIN Pad Available	POS system able to capture cards
0	No additional information available		
1	Yes	No	No
2	No	Yes	No
3	Yes	Yes	No
4	No	No	Yes
5	Yes	No	Yes
6	No	Yes	Yes
7	Yes	Yes	Yes
8	No	No	No

D   APACS 40 Authorisation Request

Field	Field Name & Description	Size	Format	Requirement
13	CONFIRMATION CODE An indication of whether the transaction amount has been accumulated or disregarded by the host subject to certain conditions. Values: 0: confirmed/accumulated, 1: failed to complete/discarded 2: acquirer declined/discarded 3:Cancelled at terminal/discarded 4: Accepted after Voice Referral/Accumulated 5: Declined after voice referral/discarded 6: Voice referral requested by acquirer, cannot complete/discarded. 7:First EFT after initialisation/N/A 8:PIN retry in progress/N/A 9:Void/discarded	1	F	Required
14	BALANCE CODE Indicator of whether transaction totals are in balance between terminal and host. Values: 0: not checked 1: Balance confirmed 2:Out of balance (1st time) 3:Out of balance (subsequent occurrence 4:In balance and totals reset to zero (REC only) 5: Out of balance but totals reset to zero (REC only)	1	F	Required
15	Reserved	-	-	-
16	FS	1	F	Required
17	CASH AMOUNT	11	V	Optional
18	FS	1	F	Required
19	TRANSACTION DATE & TIME (YYMMDDhhmm)	10	F	Required
20	FS	1	F	Required
21	EMV TERMINAL TYPE – Two digit code specified in EMV specifications for EMV terminals and specified in APACS for e-commerce transactions (see table below)	2	F	Required for ICC and e-commerce transactions

Table for Field 21:

Environment	Operational Control provided by:		
	Financial Institution	Merchant	Cardholder
Attended			
Online only	11	21	-
Offline with online capability	12	22	-
Offline only	13	23	-
Unattended			
Online only	14	24	34
Offline with online capability	15	25	35
Offline only	16	26	36

D   APACS 40 Authorisation Request

Field	Field Name & Description	Size	Format	Requirement
22	FS	1	F	Required
23	TERMINAL COUNTRY CODE The ISO code for the country where the transaction was originated.	3	F	Required
24	FS	1	F	Required
25	TRANSACTION CURRENCY CODE The ISO currency of the authorisation transaction. '826' in the UK only .	3	F	Required
26	FS	1	F	Required
27	REASON ON-LINE CODE (EMV) Used by the acquirer to determine if stand-in authorisation would be an appropriate action for the transaction (ie; ICC or CAD requiring online authorisation.) Values from ' 00' - '11'	2	F	Required
28	FS	1	F	Required
29	EMV FINANCIAL TRANSACTION REQUEST DATA	156	V	Required
29.1	Authorisation request cryptogram (ARQC)	16	F	Required
29.2	Application interchange profile (AIP)	4	F	Required
29.3	Application transaction counter (ATC)	4	F	Required
29.4	Unpredictable number	8	F	Required
29.5	Terminal verification results (TVR)	10	F	Required
29.6	Cryptogram transaction type	2	F	Required
29.7	Issuer application data	64	V	Required
29.8	US	1	F	Required
29.9	Application identifier (AID)	32	V	Required
29.10	US	1	F	Required
29.11	Application version number	4	F	Required
29.12	US	1	F	Required
29.13	Cryptogram information Data	2	F	Required
29.14	US	1	F	Required
29.15	CVM Results	6	F	Required
29.16	US	1	F	Required
29.17	Application Usage Control	4	F	Required
29.18	US	1	F	Required
29.19	Issuer Action Codes – Default/Denial/Online	30	F	Required
30	FS	1	F	Required
31	Cipher Block	16	F	Optional
32	MAC Key	8	F	Required

D   APACS 40 Authorisation Response / Hold

- A response or hold message is given in response to an authorisation request.

Field	Field Name & Description	Size	Format	Requirement
0	DIAL INDICATOR	1	F	Required
1	POS SYSTEM IDENTITY	8	F	Required
2	MESSAGE NUMBER	4	F	Required
3	MESSAGE TYPE	2	F	Required
4	ACQUIRER RESPONSE	2	F	Required
5	CONFIRMATION REQUEST	1	F	Required
6	AUTHORISATION CODE	9	V	Optional
7	FIELD SEPARATOR (FS)	1	F	Required
8	AMOUNT – In pence. Minimum of 2 digits.	11	V	Optional
9	FS	1	F	Required
10	MESSAGE	80	V	Required
11	FS	1	F	Required
12	REFERRAL TELEPHONE NUMBER	16	V	Optional
13	FS	-	F	Optional
14	FLOOR LIMIT	3	V	Optional
15	FS	1	F	Optional
16	DATE – In format YYMM.	4	F	Optional
17	FS	1	F	Optional
18	EMV RESPONSE DATA	83	V	Required
18.1	Issuer Authentication Data	32	V	Required
a	Application Response Cryptogram (ARPC)	16	F	Required
b	Optional Additional Data	16	V	Optional
18.2	US	1	F	Required
18.3	Issuer Script Data	256	V	Optional
19	FS	1	F	Optional
20	RESPONSE ADDITIONAL DATA	6	F	Optional
21	FS	1	F	Optional
22	CIPHER BLOCK	16	F	Optional
23	MAC KEY	8	F	Required

E   APACS 29 file format specification

Files must be produced using fixed-length records in either EBCDIC or ASCII. EBCDIC is not suitable for transmissions by FTP.

Label	Contents and function
VOL1 Volume Label	Because of the restriction to EBCDIC character coding, American Express supports two versions of the VOL1 header label for APACS 29 submissions (both 80 characters unblocked): ● Option 1 is the ISO version 3 label. ● Option 2 is the IBM standard label, which differs in the location of the Agent Reference Code and the content of the label standard version.
HDR1 Header Label	HDR1 contains operating system and device-dependent data relating to the submission.
HDR2 Header Label	HDR2 contains other characteristics of the submission.
UHL1 User Header Label	This contains user-specified data used in processing. It identifies American Express as the file recipient.
Submission Records	One record for each transaction (also known as 'Record of Charge').
Net Summary Record	One per batch of transactions (also known as 'Summary of Charge').
Net Claim Record	One per file **unless the file is multi-currency**, in which case one for each Net Summary Record
EOF1 End of File Label	One per file; format similar to the HDR1
EOF2 End of File Label	One per file; format similar to the HDR2
UTL1 User Trailer Label	Control data, such as accumulated totals and record counts, and is used for data reconciliation and file integrity-checking. 80 characters unblocked.

Notes
- Transactions should be batched and summarised by SE number; a batch cannot contain more than one SE number
- If a submission contains one or more records with EMV data then all non-EMV records should be padded with spaces to a record length of 636 bytes
- There must be only one logical file per submission
- Optional fields must be space-filled if not populated

TRANSACTION CODES ('n')

Transaction Record (n1 / n2)
n = J   – 3 Segment record (380 bytes) for magstripe transactions in a magstripe-only batch
n = K   – 3 Segment record (padded to 636 bytes) for magstripe txns in mixed ICC / magstripe batch
n = Q   – 4 Segment record (636 bytes) for all ICC transactions

Net Summary Record (n4 / n5)
n = J – for a batch containing only magstripe data (no ICC data)
n = K – for a batch containing one or more ICC transactions

Net Claim Record (n7 / n8)
n = J – for a claim record summarising only J4 and J5s (magstripe only data)
n = K – for a claim record summarising one or more K4 or K5s (one or more ICC transactions)

FORMAT KEY

N indicates a numeric field that must be Right-justified with leading zeros
A indicates an alphanumeric field that must be Left-justified with trailing spaces
AB indicates a binary field

E   APACS 29 file format specification

The illustrations in this section show only the financial data records and specifically omit any file transmission records and / or character strings associated with the underlying communications protocol(s).

Header Label Specifications

APACS 29 allows for either an IBM or ISO format Volume Header. The format used is dictated by the merchant; typically a mainframe system would use the IBM option, A PC-based solution the ISO option.

Volume Header Label - ISO Option

Position	Size	Format	Field name and description	Requirement
1-4	4	A	LABEL IDENTIFIER - always 'VOL1'	Required
5-10	6	A	VOLUME IDENTIFIER – File Number. Must start with at least one alphabetic character and must increment by one for each new file submitted. Example: A00001, A00002 up to A99999. Do not use 'AMEX' or 'AMX'	Required
11-37	27	space	Space-filled	Optional
38-47	10	A	OWNER IDENTIFICATION or AGENT REFERENCE – unique reference assigned by American Express, eg MERCHANT42	Required
48	1	N	FILE CURRENCY INDICATOR – 0 = Not used 1 = Single currency in file (eg GBP) 2 = More than one currency in the file	Required
49-79	31	space	Space-filled	Optional
80	1	N	LABEL STANDARD VERSION - always '3' for ISO header	Required

Volume Header Label - IBM Option

Position	Size	Format	Field name and description	Requirement
1-4	4	A	LABEL IDENTIFIER – always 'VOL1'	Required
5-10	6	A	VOLUME IDENTIFIER – File Number. Must start with at least one alphabetic character and must increment by one for each new file submitted. Example: A00001, A00002 up to A99999. Do not use 'AMEX' or 'AMX'	Required
11-41	31	space	Space-filled	Optional
42-51	10	A	OWNER IDENTIFICATION or AGENT REFERENCE – unique reference assigned by American Express, eg MERCHANT42	Required
52	1	N	FILE CURRENCY INDICATOR – 0 = Not used 1 = Single currency in file (eg GBP) 2 = More than one currency in the file	Required
53-79	27	space	Space-filled.	Optional
80	1	space	LABEL STANDARD VERSION – Must be blank	Optional

E   APACS 29 file format specification

First File Header Label (HDR1)

HDR1 contains operating system and device-dependent data that relates to the submission.

Position	Size	Format	Field name and description	Requirement
1-4	4	A	LABEL IDENTIFIER – always 'HDR1'	Required
5-14	10	A	SOURCE IDENTIFIER OF ORIGINATOR – 'IBRO' followed by merchant name, abbreviated if necessary eg IBROJONES	Required
15	1	A	RECORD TYPE IDENTIFIER: J if no ICC records in file (fixed length records) Z if one or more ICC records in file (variable length records)	Required
16-17	2	space	Space-filled	Optional
18	1	N	FILE CURRENCY INDICATOR – 0 = Not used 1 = Single currency in file (eg GBP) 2 = More than one currency in the file	Required
19-21	3	space	Space-filled	Optional
22-27	6	A	VOLUME IDENTIFIER – File Number. Must be the same as in VOL1 Header Label positions 5-10 eg A00001 and incrementing	Required
28-31	4	N	FILE SECTION NUMBER - always '0001'	Required
32-35	4	N	FILE SEQUENCE NUMBER - always '0001'	Required
36-42	7	space	Space-filled	Optional
43-47	5	N	CREATION DATE - the year and day (Julian format YYDDD) on which the file was written	Required
48	1	space	Space-filled.	Optional
49-53	5	N	EXPIRY DATE - the year and day (in Julian format YYDDD) after which the file must not be processed. This may be up to 40 days after the creation date, but cannot be before the day on which the file is received for processing.	Required
54	1	space	ACCESSIBILITY – space-filled	Optional
55-60	6	N	BLOCK COUNT – zero-filled	Required
61-73	13	space	SYSTEM CODE – space-filled	Optional
74-80	7	space	Space-filled	Optional

E   APACS 29 file format specification

Second File Header Label (HDR2)

Position	Size	Format	Field name and description	Requirement
1-4	4	A	**LABEL IDENTIFIER** – always 'HDR2'	Required
5	1	A	RECORD FORMAT: F if no ICC records in file (fixed length records) D if one or more ICC records in file (variable length records)	Required
6-10	5	N	BLOCK LENGTH - must be any exact multiple of 380 (magstripe) or 636 (ICC) to a maximum of 31920. We suggest: 03800 for file with no ICC transactions 06360 for file with one or more ICC txns	Required
11-15	5	N	RECORD LENGTH: 00380 = only J records in file (fixed) 00636 = ICC records in file (fixed) 00640 = ICC records in file (variable-blocked)	Required
16-50	35	space	Space-filled	Optional
51-52	2	N	BUFFER OFFSET – zero-filled	Required
53-80	28	space	Space-filled	Optional

User Header Label (UHL1)

UHL1 contains user-specified data used in processing. It identifies American Express as the file recipient.

Position	Size	Format	Field name and description	Requirement
1-4	4	A	LABEL IDENTIFIER – always 'UHL1'	Required
5-10	6	N	PROCESSING DATE format: spaceYYDDD	Optional
11-20	10	N	RECIPIENT IDENTIFIER: always '3700000007'	Required
21-28	8	N	COUNTRY CODE ISO country code followed by zeros eg 82600000 for a UK Submitter	Required for multi-currency
29-37	9	A	WORK CODE - space-filled	Optional
38-40	3	N	FILE NUMBER – space-filled	Optional
41-54	14	space	Space-filled	Optional
55-80	26	space	Space-filled	Optional

E   APACS 29 file format specification

Transaction Record Format

n = J   – 3 Segment record (380 bytes) for magstripe transactions in a magstripe-only batch
n = K   – 3 Segment record (380 bytes) for magstripe transactions in a mixed ICC / magstripe batch
n = Q   – 4 Segment record (636 bytes) for all ICC transactions

Segment 1

Position	Size	Format	Field name and description	Requirement
1-19	19	N	CARDMEMBER NUMBER – 15-digit card account number with 4 leading zeros and no embedded spaces. Must start with either 37 or 34 and have a valid Luhn check digit	Required
20-21	2	A	TRANSACTION CODE: • n1 - debit transaction (purchase) • n2 - credit transaction (refund) – see above for 'n' value	Required
22-32	11	N	SERVICE ESTABLISHMENT NUMBER – your 10-digit Amex Service Establishment number with a leading zero and no embedded spaces	Required
33-36	4	N	CARD EXPIRY DATE – if present, must be valid YYMM or MMYY format	Optional
37-47	11	N	TRANSACTION AMOUNT – must be numeric and non-zero. Do not use + or -	Required
48-53	6	N	TRANSACTION DATE – must be a valid date, in 'spaceYYDDD' or 'YYMMDD' format	Required
54-59	6	N	TRANSACTION TIME – must be valid 'HHMMSS' format, or zero-filled	Required
60-67	8	N	AUTHORISATION CODE – American Express authorisation codes are usually two digits long	Optional
68-79	12	A	ORIGINATOR'S TRANSACTION REF: a reference code whereby American Express can request Service Establishment support for a charge. This reference must be supplied by the merchant or agent and should be an index to the Service Establishment's records so that the original document can be readily retrieved (Terminal ID, EFT Sequence Number etc)	Required
80	1	N	Zero-filled	Required
81	1	N	ATM/POS TYPE Non-Euro transaction currency: 0 – Unspecified terminal capabilities 1 – EMV reader only 2 – Magnetic stripe only 3 – EMV / Magnetic Stripe 4 – No card reader Euro transaction currency: 5 – Unspecified terminal capabilities 6 – EMV reader only 7 – Magnetic stripe only 8 – EMV / Magnetic Stripe 9 – No card reader	Required

E   APACS 29 file format specification

Position	Size	Format	Field name and description	Requirement
82	1	N	CARD SEQUENCE NUMBER - zero-filled	Required
83	1	A	CUSTOMER INSTRUCTIONS: 0 – Signed 1 – Mail / telephone order 2 – Continuous Authority 3 – PIN verified – online 4 – PIN verified – offline 5 – Signed – magnetic stripe captured 6 – Signed – Keyed at POS 7 – Unattended device without PIN 8 – PIN-verified, recovered after sale 9 – Signed voucher, recovered after sale B – Fallback to signature-verified, ICC C – Signature-verified, ICC D – Downgraded ICC transaction (track 2) F – EMV fallback to magnetic stripe	Required
84-90	7	N	SEQUENCE NUMBER – must be a valid number starting with 1 for the first transaction record on the file and incrementing by 1 on subsequent data records, *including Net Summary and Net Claim records*	Required
91-116	26	A	ESTABLISHMENT NAME - must be the name of the Service Establishment where the transaction took place, corresponding to the Service Establishment number in 22-32 above. Please provide text in UPPER CASE. Only the first 25 characters may be used on the Cardmember statement	Required
117-142	26	A	ESTABLISHMENT ADDRESS - abbreviated establishment address. Normally the name of the town is sufficient. Please provide text in UPPER CASE. Only the first 25 characters may be used on the Cardmember statement	Required
143-145	3	A	ESTABLISHMENT TYPE	Optional
146-171	26	A	CARDMEMBER NAME	Optional
172-173	2	N	FORMAT TYPE - must be one of the following, depending on the format of segment 3: 01 - Retail format 04 – General format	Required

E   APACS 29 file format specification

Segment 3 - Retail

This table contains the fields for Retail format i.e. when the format type (positions 172-173) is 01.

Position	Size	Format	Field name and description	Requirement
174-341	168 (28x6) (3) (15) (10)	A N A N	PURCHASE DETAILS for six purchases, including: Purchase quantity Purchase description (UPPER CASE) Purchase amount	Required
342-361	20	A	TAX or DISCOUNT CAPTION - explanation of tax or discount changes to total value. If used, either discount or tax amount may be present, but not both. Must be filled if DISCOUNT or TAX is used. Otherwise space-filled.	Required if DISCOUNT or TAX is present
362-370	9	A	DISCOUNT – discount amount if applicable. Otherwise space-filled.	Required, as before
371-379	9	A	TAX - tax amount if applicable. Otherwise, fill with spaces.	Required, as before
380	1	space	Space-filled	Required

Segment 3 - General

This table contains the fields for General format i.e. when the format type (positions 172-173) is 04.

At least one entry of purchase details is required, for example GOODS or MERCHANDISE. Unused entries are filled with spaces.

Position	Size	Format	Field name and description	Requirement
174-213	40	A	CHARGE DESCRIPTION LINE 1 - the first description line to appear on the Record of Charge.	Required
214-253	40	A	CHARGE DESCRIPTION LINE 2 - the second description line to appear on the Record of Charge.	Optional
254-293	40	A	CHARGE DESCRIPTION LINE 3 - the third description line to appear on the Record of Charge.	Optional
294-333	40	A	CHARGE DESCRIPTION LINE 4 - the fourth description line to appear on the Record of Charge.	Optional
334-373	40	A	CHARGE DESCRIPTION LINE 5 - the fifth description line to appear on the Record of Charge.	Optional
374-380	7	space	Reserved - to be space-filled.	Required

E   APACS 29 file format specification

Segment 4 - ICC Data

Position	Size	Format	Field name and description	Requirement
381-382	2	A	APPLICATION PAN SEQUENCE NUMBER – Identifies and differentiates between Cards with the same PAN (Primary Account Number)	Required
383-384	2	A	AUTHORISATION RESPONSE CODE	Required
385-395	11	N	CRYPTOGRAM TRANSACTION AMOUNT – Amount, Authorised (EMV Tag 9F02) as input to cryptogram generation	Required
396-397	2	N	CRYPTOGRAM TRANSACTION TYPE – Indicates the type of transaction (Debit, Credit) supplied by the POS system as input to the cryptogram generation: Value 00 = Debits 20 = Credits	Required
398-403	6	N	TERMINAL TRANSACTION DATE -(YYMMDD) The date supplied by the POS system as input to the cryptogram generation	Required
404-406	3	N	TRANSACTION CURRENCY CODE The ISO currency code of the transaction as input to the cryptogram generation For example 826 where the transaction is in GBP	Required
407-409	3	N	TERMINAL COUNTRY CODE – The ISO code designating where the POS system is operating. UK will be '826'	Required
410-425	16	AB	TRANSACTION CRYPTOGRAM - Transaction Certificate (TC), Authorisation Request Cryptogram (ARQC) or Application Authentication Cryptogram (AAC)	Required
426-429	4	AB	APPLICATION INTERCHANGE PROFILE (AIP) – Indicates the capabilities of the Card to support specific functions in the application	Required
430-433	4	AB	APPLICATION TRANSACTION COUNTER (ATC) – Counter maintained by the application in the ICC (Incrementing the ATC is managed by the ICC)	Required
434-441	8	AB	UNPREDICTABLE NUMBER – Unpredictable Number input to cryptogram generation	Required
442-451	10	AB	TERMINAL VERIFICATION RESULT (TVR) – Terminal Verification Results input to cryptogram generation	Required
452-515	64	AB	ISSUER APPLICATION DATA (IAD) - Contains proprietary application data for transmission to the user in an on-line transaction. Provided by the card at the time of the Transaction Cryptogram generation.	Required
516-519	4	AB	APPLICATION USAGE CONTROL	Required

E   APACS 29 file format specification

Position	Size	Format	Field name and content	Requirement
520-521	2	AB	CRYPTOGRAM INFORMATION DATA - Indicates the type of cryptogram (TC, ARQC or AAC) returned by the card	Required
522-527	6	AB	CARDMEMBER VERIFICATION METHOD (CVM) RESULTS - Indicates the results of the last CVM performed	Required
528-559	32	AB	APPLICATION IDENTIFIER – (AID) or DF name, whichever is longer.	Required
560-563	4	AB	APPLICATION VERSION NUMBER - Version number associated with the Application Identifier	Required
564-567	4	AB	TRANSACTION STATUS INFORMATION – An indication of the terminal functions performed during the Transaction	Required
568-569	2	AB	EMV TERMINAL TYPE	Required
570-575	6	AB	EMV TERMINAL CAPABILITIES	Required

Position	size	Source (POS or Card)	Format	Field name and content	Requirement
576-577	2	POS system	A	POS ENTRY MODE DIGIT 1 (Card Transaction Info.) 0 = Not used with APACS 50 1 = Swipe 2 = Keyed 3 = EMV 4 = Recovered data, keyed 5 = Recovered data, electronic 6 = Information advice 7 = Downgraded EMV transaction 8 = Swipe EMV failure 9 = Reserved for future use DIGIT 2 (Card member verification, if any) 0 = Not used with APACS 50 1 = Customer present, signature 2 = Customer present, PIN 3 = Customer present, alternate CVM 4 = Customer present, UPT no CVM 5 = Customer present, UPT, PIN 6 = Customer present, UPT, alternate CVM 7 = Customer not present 8 = No verification 9 = Reserved for future use	Required
578-603	26	Card	A	OTHER CARD DATA - All the data from track 2 after and including the field separator, padded with trailing spaces. The card data will be read from the magnetic stripe or the track 2 equivalent on EMV cards and will be padded with trailing spaces if required.	Optional
604-636	33	-	space	Reserved for Future Use. Space-filled	Optional

E   APACS 29 file format specification

Net Summary Record – n4 or n5

n = J – for a batch containing only magstripe data (no ICC data)
n = K – for a batch containing one or more ICC transactions

Position	Size	Format	Field name and content	Requirement
1-19	19	N	Filled with zeros.	Required
20-21	2	A	TRANSACTION CODE: n4 – if value of debits (n1) > credits (n2) n4 – if value of debits (n1) = credits (n2) n5 – if value of credits (n2) > debits (n1) – see above for 'n' value	Required
22-32	11	N	SERVICE ESTABLISHMENT NUMBER – the Service Establishment number for the preceding financial transaction record.	Required
33-35	3	A	CURRENCY INDICATOR – Use ISO Currency Code (eg 826 for £ Sterling)	Required
36	1	space	Space-filled	Required
37-47	11	N	NET AMOUNT - net value of preceding n1 and n2 records. Do not use + or -	Required
48-58	11	N	VALUE OF DEBIT ITEMS Value of preceding n1 records (debits)	Required
59-69	11	N	VALUE OF CREDIT ITEMS Value of preceding n2 records (credits)	Required
70-76	7	N	COUNT OF DEBIT ITEMS Number of preceding n1 records (debits)	Required
77-83	7	N	COUNT OF CREDIT ITEMS Number of preceding n2 records (credits)	Required
84-90	7	N	SEQUENCE NUMBER – must be one more than the sequence number of the preceding financial transaction record	Required
91-93	3	A	SOC REF NO INDICATOR – always 'YES'	Required
94-99	6	N	SOC REFERENCE NUMBER – a number (eg date) that will appear on payment advices or other reporting. Recommended to facilitate payment reconciliation. NB - for third party processors polling offline POS systems, it is requested that transactions are batched by end-of-day function, with the date of the first transaction as the SOC reference.	Required
100-380	281	N	Reserved for future use - zero-filled	Required

E   APACS 29 file format specification

Net Claim Record – n7 or n8

n = J – for a batch containing only magstripe data (no ICC data)
n = K – for a batch containing one or more ICC transactions

If the file is multi-currency (ie contains more than one currency) there must be one Net Claim Record (n7/8) for each Net Summary Record (n4/5).

Position	Size	Format	Field name and content	Requirement
1-6	6	N	SORTING CODE – zero-filled	Required
7-14	8	N	ACCOUNT NUMBER – zero-filled	Required
15	1	N	TYPE OF ACCOUNT CODE – zero-filled	Required
16-19	4	N	Zero-filled	Required
20-21	2	A	TRANSACTION CODE: n8 – if value of debits (n4) > credits (n5) n8 – if value of debits (n4) = credits (n5) n7 – if value of credits (n5) > debits (n4) – see above for 'n' value	Required
22-32	11	N	ACCOUNTING UNIT NUMBER zero-filled	Required
33-35	3	A	CURRENCY INDICATOR - Use ISO Currency Code (eg 826 for £ Sterling)	Required
36	1	Space	Space-filled	Required
37-47	11	N	NET AMOUNT - net value of preceding n4 and n5 records. Do not use + or -	Required
48-58	11	N	VALUE OF DEBIT ITEMS - value of preceding n4 records (debit summaries)	Required
59-69	11	N	VALUE OF CREDIT ITEMS - value of preceding n5 records (credit summaries)	Required
70-76	7	N	COUNT OF DEBIT ITEMS - number of preceding n4 records (debit summaries)	Required
77-83	7	N	COUNT OF CREDIT ITEMS - number of preceding n5 records (credit summaries)	Required
84-90	7	N	SEQUENCE NUMBER – must be one greater than the sequence number of the preceding net summary record.	Required
91-380	290	N	Zero-filled	Required

E   APACS 29 file format specification

Trailer Label Specifications

First End of File Label (EOF1)

Position	Size	Format	Field name and content	Requirement
1-4	4	A	LABEL IDENTIFIER - always 'EOF1'	Required
5-14	10	A	SOURCE IDENTIFIER OF ORIGINATOR - same as HDR1 label positions 5-14. 'IBRO' followed by merchant name, abbreviated if necessary eg IBROJONES	Required
15	1	A	RECORD TYPE IDENTIFIER – same as HDR1 label position 15. J - if no ICC records in the file (fixed length records) Z - if one or more ICC records in the file (variable length records)	Required
16-21	6		Space-filled	Required
22-27	6	A	VOLUME IDENTIFIER – File Number. Must be the same as in VOL1 Header Label positions 5-10 eg A00001 and incrementing	Required
28-31	4	N	FILE SECTION NUMBER - always '0001'	Required
32-35	4	N	FILE SEQUENCE NUMBER – always '0001'	Required
36-42	7	space	Space-filled	Required
43-47	5	A	CREATION DATE - same as HDR1 label	Required
48	1	space	Space-filled	Required
49-53	5	A	EXPIRY DATE - same as HDR1 label	Required
54	1	space	Space-filled	Required
55-60	6	N	Zero-filled	Required
61-80	20	space	Space-filled.	Required

Second End of File Label (EOF2)

Position	Size	Format	Field name and content	Requirement
1-4	4	A	LABEL IDENTIFIER - always 'EOF2'	Required
5	1	A	RECORD FORMAT – same as HDR2 label	Required
6-10	5	N	BLOCK LENGTH - same as HDR2 label	Required
11-15	5	N	RECORD LENGTH – same as HDR2 label	Required
16-50	35	N	Zero-filled	Required
51-52	2	N	Zero-filled	Required
53-80	28	N	Zero-filled	Required

E APACS 29 file format specification

User Trailer Label (UTL1)

Position	Size	Format	Field name and content	Requirement
1-4	4	A	LABEL IDENTIFIER – always 'UTL1'	Required
5-17	13	N	VALUE OF DEBIT ITEMS – total value of preceding n8 records (debit claims)	Required
18-30	13	N	VALUE OF CREDIT ITEMS – total value of preceding n7 records (credit claims)	Required
31-37	7	N	COUNT OF DEBIT ITEMS - number of preceding n8 records (debit claims)	Required
38-44	7	N	COUNT OF CREDIT ITEMS - number of preceding n7 records (credit claims)	Required
45-54	10	N	RECORD COUNT – the number of data records on the file. This *excludes* VOL1, HDR1, HDR2, EOF1, EOF2, and UTL1. Must be the same as the sequence number of the last Net Claim Record (n7 or n8)	Required
55-80	26	space	Space-filled	Required

F   Card Numbers for Submissions testing

The following Card numbers should be used for sending test transactions to American Express. Please note those in the table below must be used for Submission file testing only.

Please use a minimum of 15 transactions per batch in your test file. You may use the same card number or a variety of card numbers. Please use a mixture of debit and credit transactions.

These Card numbers can be used under any test merchant number.

• 3741 010121 80018	• 3742 510309 00010
• 3742 510187 20018	• 3742 510332 70007
• 3742 510210 90003	• 3745 810632 70000
• 3742 510243 60015	• 3741 010087 22013
• 3742 510276 30000	• 3741 010110 92008
• 3742 510298 12002	• 3741 010143 62010
• 3742 510321 82013	• 3742 510176 32008
• 3742 510354 52009	• 3742 510209 02018
• 3742 810410 92002	• 3742 510232 72005
• 3745 810565 42019	• 3742 510265 42016
• 3745 810598 12005	• 3742 510298 12002
• 3745 810621 82016	• 3742 510310 91009
• 3745 810654 52002	• 3742 510343 61011
• 3741 010076 31009	• 3742 910465 41010
• 3741 010132 71006	• 3742 910521 81016
• 3742 510165 41010	• 3745 810587 21017
• 3742 510221 81017	• 3745 810610 91002
• 3742 510287 21014	• 3745 810643 61014

EMV testing

If you are testing for EMV accreditation you will have been issued the following card number by our EMV Certification Unit:

3742 454554 xxxxx (for security it is shown here truncated).

This card number should be used in EMV submission file testing.

G   Test Service Establishment numbers

The following test Service Establishment (SE) numbers may be used for sending UK Sterling * test transactions to American Express; those in the table must be used for Submission file testing only.

Please submit a minimum of two batches.

• 942 469 0485 • 942 469 0493 • 942 469 0501 • 942 469 0519 • 942 469 0527 • 942 469 0535 • 942 249 9392 • 942 249 9459 • 942 249 9517	• 942 249 9574 • 942 488 8253 • 942 488 8261 • 942 488 8279 • 942 488 8287 • 942 249 9152 • 942 249 9210 • 942 249 9277 • 942 249 9335

If you have previously completed authorisation testing for EMV or magstripe, you will have been issued the following test Service Establishment number:

942 582 1733

This number can be used for EMV and magstripe submission file testing in addition to those listed above.

In certain circumstances it may be appropriate to use you live SE number for testing; please contact us for further information.

* If you wish to certify for currencies other than GBP please ask us for the Multicurrency addendum to this guide.

H   Validating Card and SE numbers

American Express **Cardmember numbers** are always 15 digits long, starting with "34" or "37".

All Cardmember numbers use the LUHN formula for the modulus 10 check digit. The check digit is the last (fifteenth) digit of the card number, and is validated as described in the table below.

In this illustration the following card number is validated: **3742 5103 2182 013**

Column No.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Cardmember No.	3	7	4	2	5	1	0	3	2	1	8	2	0	1	3
Multiply each **even** column by two.		**14**		4		2		6		2		4		2	
If result is >9, add the two digits. (e.g. 7x2=14, 1+4=5)		**5**		4		2		6		2		4		2	
Carry down each digit in the odd-numbered columns.	3	5	4	4	5	2	0	6	2	2	8	4	0	2	3
Add all digits together.	3 + 5 + 4 + 4 + 5 + 2 + 0 + 6 + 2 + 2 + 8 + 4 + 0 + 2 + 3 = 50													
If the result is a multiple of 10, the Cardmember number is valid.	50 divided by 10 = 5. Cardmember number is valid.													

American Express **Service Establishment (SE) numbers** are 10 digits long, starting with "9".

All Cardmember numbers use the LUHN formula for the modulus 10 check digit. The check digit is the last (tenth) digit of the card number, and is validated as described in the table below.

In this illustration the following Service Establishment number is validated: **942 469 048 5**

Column No.	1	2	3	4	5	6	7	8	9	10
Service Establishment No.	9	4	2	4	6	9	0	4	8	5
Ensure first digit is "9" then disregard.	9									
Carry down digits in the odd columns.			2		6		0		8	
Multiply each odd column by two.			4		**12**		0		16	
If result is >9, add the two digits together. (e.g. 6x2=12, 1+2=3)					**3**				7	
Carry down all of the digits.		4	4	4	3	9	0	4	7	5
Add all of the digits together.	4 + 4 + 4 + 3 + 9 + 0 + 4 + 7 + 5 = 40								
If the result is a multiple of 10, the Service Establishment number is valid.	40 / 10 = 4. Service Establishment number is valid.								

I   Magnetic Stripe Layout – ISO and ANSI

Magnetic Stripe Layout

This Appendix documents the two different magnetic stripe layouts, American National Standards Institute (ANSI) and International Standards Organisation (ISO), that are encoded on American Express cards.

These two formats can be distinguished by using the track 2 length. For ANSI-formatted cards the length is 32 digits whilst for ISO-formatted cards the length is 40 digits.

Implications for card acceptance and testing

If you request cards for testing you will automatically be provided with both ISO and ANSI standard test cards. Tests using these cards form part of our required scripts for APACS Standard 30 authorisation testing.

Position 22 on the magnetic stripe track 2 identifies different information depending on format. On an ANSI card it is the start date whilst on an ISO card it is the interchange designator, which identifies whether the card has a chip on it. We have to ensure that American Express Cards issued in both formats can be recognised by POS terminals and processed accordingly.

Please note that the start date is no longer embossed on the front of American Express cards and for this reason Start (effective) date checking must be switched off.

I Magnetic Stripe Layout – ANSI

The ANSI format for the magnetic stripe is as follows:

Field name	Length	Position
TRACK 1		
Start sentinel	1	1
Format code = B	1	2
Cardmember number	17	3
Field separator	1	20
Cardmember name	26	21
Field separator	1	47
Expiration date (YYMM)	4	48
Effective date (YYMM)	4	52
Security code	5	56
End sentinel	1	61
LRC 1	1	62
TRACK 2		
Start sentinel	1	1
Cardmember number	15	2
Field separator	1	17
Expiration date (YYMM)	4	18
Effective date (YYMM)	4	22
Security code	5	26
End sentinel	1	31
LRC	1	32

I Magnetic Stripe Layout – ISO

The ISO 7813 format for the magnetic stripe is as follows*:

Field name	Length	Position
TRACK 1		
Start sentinel	1	1
Format code = B	1	2
Cardmember number	17	3
Field separator	1	20
Cardmember name	26	21
Field separator	1	47
Expiration date (YYMM)	4	48
Interchange designator	**1**	**52**
Service code	**2**	**53**
Effective date (YYMM)	4	55
Security code	5	59
Zeros	**12**	**64**
Language code	**2**	**76**
End sentinel	1	78
LRC 1	1	79
TRACK 2		
Start sentinel	1	1
Cardmember number	15	2
Field separator	1	17
Expiration date (YYMM)	4	18
Interchange designator	**1**	**22**
Service code	**2**	**23**
Effective date (YYMM)	4	25
Security code	5	29
Zeros	**3**	**34**
Language code	**2**	**37**
End sentinel	1	39
LRC	1	40

(* The differences between ISO and the ANSI format are highlighted in bold)

J   Submissions Management and Error Handling

Once you start submitting to American Express in the 'live' environment your submissions are monitored by our Submissions Management team. We ask that you provide us with a point of contact so that we can inform you if we are unable to process any of the data that you submit.

Data Errors

File processing errors are classified into three types:

- **Charge errors**, affecting a single financial transaction eg. an invalid Cardmember number, a zero amount
- **Batch errors**, affecting all transactions for a given branch eg. an invalid Service Establishment number, an out-of-balance net summary record
- **Submission errors,** affecting the whole file eg. invalid headers or trailers

Full or Partial File Rejection

If Charge or Batch errors are encountered either (1) the valid transactions can be processed or (2) the entire submission can be rejected (this is the default setting). You may request a change to your rejection settings by contacting Submissions Management.

A submission error results in the entire submission being rejected.

Notification of Data Errors

If we are unable to process any data that you send to us Submissions Management will contact you to advise on the corrective action required.

Data Recovery and re-submission

Your system must be capable of storing and/or re-creating files sent to American Express. If a submission contains errors which prevent processing, you should correct or remove the errors and resubmit the file. If any valid transactions have already been processed, to avoid duplication these valid transactions must be removed from the file before it is re-submitted.

Data Duplication

American Express checks submission files for duplicate batches and may take action to reverse these transactions. **If you think you have submitted duplicate batches / transactions please do not attempt to cancel these out by submitting refund transactions without first contacting Submissions Management.**

Contact

You may contact Submissions Management at submissionsmanagementeurope@aexp.com.

The submitter is responsible for re-creating and re-submitting any file that fails to reach American Express or proves to be unreadable for any reason.

American Express cannot be held responsible for any delays in payment resulting from the failure of a Service Establishment to submit a file in a readable condition nor can American Express undertake to process charges submitted in any manner other than on the Record of Charge forms, listings, or in files conforming to the specifications defined in this Guide.

K   EMV Receipt Requirements

Element	Mandatory / Optional
Retailer name	M
Retailer address	M
Retail identification / location	M
VAT registration number	O
Cardscheme name	M
Date (DDMMYY) and time (HHMM- 24hr)	M (date only)
Receipt number	O
Terminal identifier (TID)	M
Transaction type (purchase, refund)	M
Transaction amount	M
EFT sequence number (transaction number)	M
Authorisation code	M
Indication of whether ICC, magstripe or PKE transaction	O
Goods amount	O (with currency symbol)
Goods description	O
VAT rate	O
PAN (masked on cardmember copy)	M
Expiry date (magstripe-read and PKE only)	M
AID (Application ID)	M
Application effective date	O
Application expiration date	M
Application PAN sequence number	M
Space for cardmember signature	M where applicable
Cardmember declaration wording (variable)	M
Thank you message (variable)	O
Cardmember PIN-verified / signature-verified message	M where applicable
Cryptogram type and value	O
Merchant ID	M
Customer copy / store copy text (retention reminder)	M
Request for signature	M where applicable

L   Sample APACS 29 file layout

Please note only positions 1 to 60 are shown

a) Non-ICC file containing two transactions; one debit of £105.35, one credit of £5.11, ISO header, General Format.

```
 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0

 V O L 1 J N S B 0 1                                         J O N E S B R O 0 1 1
 H R D 1 I B R O J O N E S B J       1         J N S B 0 1 0 0 0 1 0 0 0 1                 9 9 2 5 1       9 9 2 7 1     0 0 0 0 0
 H D R 2 F 0 1 9 0 0 0 0 0 3 8 0                                                                                     0 0
 U H L 1 9 9 9 2 5 1 3 7 0 0 0 0 0 0 0 0 7 8 2 6 0 0 0 0 0                             0 0 0
 0 0 0 0 3 7 4 2 4 5 4 5 2 2 0 0 0 0 1 J 1 0 9 4 2 5 8 2 1 7 3 3 0 1 1 2 0 0 0 0 0 0 0 1 0 5 3 5     9 9 2 4 9 1 0 3 7 5 4 0
 0 0 0 0 3 7 4 1 2 3 4 5 6 7 0 0 0 0 3 J 2 0 9 4 2 5 8 2 1 7 3 3 0 2 1 1 0 0 0 0 0 0 0 0 5 1 1     9 9 2 4 9 1 0 5 2 3 4 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 J 4 0 9 4 2 5 8 2 1 7 3 3 8 2 6   0 0 0 0 0 0 1 0 0 2 4 0 0 0 0 0 0 1 0 5 3 5 0 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 J 8 0 0 0 0 0 0 0 0 0 0 0 0 8 2 6   0 0 0 0 0 0 1 0 0 2 4 0 0 0 0 0 0 1 0 5 3 5 0 0
 E O F 1 I B R O J O N E S B J           J N S B 0 1 0 0 0 1 0 0 0 1                 9 9 2 5 1       9 9 2 7 1     0 0 0 0 0
 E O F 2 F 0 1 9 0 0 0 0 0 3 8 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 U T L 1 0 0 0 0 0 0 0 0 0 1 0 5 3 5 0 0 0 0 0 0 0 0 0 0 5 1 1 0 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 4
```

b) ICC file containing two transactions; one debit of £105.35, one credit of £5.11, ISO header, General Format (ICC-specific data highlighted in red)

```
 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0

 V O L 1 J N S B 0 1                                         J O N E S B R O 0 1 1
 H R D 1 I B R O J O N E S B Z       1         J N S B 0 1 0 0 0 1 0 0 0 1                 9 9 2 5 1       9 9 2 7 1     0 0 0 0 0
 H D R 2 D 0 1 9 0 0 0 0 0 6 4 0                                                                                     0 0
 U H L 1 9 9 9 2 5 1 3 7 0 0 0 0 0 0 0 0 7 8 2 6 0 0 0 0 0                             0 0 0
 0 0 0 0 3 7 4 2 4 5 4 5 2 2 0 0 0 0 1 Q 1 0 9 4 2 5 8 2 1 7 3 3 0 1 1 2 0 0 0 0 0 0 0 1 0 5 3 5     9 9 2 4 9 1 0 3 7 5 4 0
 0 0 0 0 3 7 4 1 2 3 4 5 6 7 0 0 0 0 3 Q 2 0 9 4 2 5 8 2 1 7 3 3 0 2 1 1 0 0 0 0 0 0 0 0 5 1 1     9 9 2 4 9 1 0 5 2 3 4 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 K 4 0 9 4 2 5 8 2 1 7 3 3 8 2 6   0 0 0 0 0 0 1 0 0 2 4 0 0 0 0 0 0 1 0 5 3 5 0 0
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 K 8 0 0 0 0 0 0 0 0 0 0 0 0 8 2 6   0 0 0 0 0 0 1 0 0 2 4 0 0 0 0 0 0 1 0 5 3 5 0 0
 E O F 1 I B R O J O N E S B Z           J N S B 0 1 0 0 0 1 0 0 0 1                 9 9 2 5 1       9 9 2 7 1     0 0 0 0 0
 E O F 2 D 0 1 9 0 0 0 0 0 6 4 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 U T L 1 0 0 0 0 0 0 0 0 0 1 0 5 3 5 0 0 0 0 0 0 0 0 0 0 5 1 1 0 0 0 0 0 0 1 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 4
```

procedure guide

For a smoother operation

barclaycard

welcome

This procedure guide forms part of your Agreement with Barclaycard and replaces all previous editions of the procedure guide with immediate effect. These procedures must be followed so that your business can enjoy the full benefit of accepting payment by cards, including prompt payment to your bank account.

Your procedure guide should be kept in a safe place, easily accessible to your employees, but out of reach of your customers. Speed, efficiency and security are essential to credit and debit card acceptance today. To help you and your staff gain the maximum benefit from processing with us, your procedure guide contains all the information you need for your business to accept payments by card, whether by a PDQ terminal owned by Barclaycard and leased to you, or by your own terminals.

Change of business type

You will need to notify us if you significantly change the type of goods or services that your original Merchant Agreement applies to (for example if you start trading on the internet or if you start accepting mail or telephone order transactions and you previously advised us that you only accept face-to-face transactions in your retail outlet) or if you change the nature of your business (for example from a partnership to a limited company) or if you change the actual name of your business.

Telephone contacts

You will be advised in various sections of this guide to contact one or more departments. There's a full list of the telephone numbers in Section 7.

Barclaycard outlet number

For ease when you contact Barclaycard, please have your Merchant number ready. You can keep a record of it here:

contents

1. things you need to know before you accept card payments

1.1 Card recognition

It is important to point out that card details and procedures do vary depending on the card type. We have set out a clear guide to each card type, to help you and your staff to become familiar with card recognition practices and acceptance procedures.

The following pages provide a quick reference guide for security checks. For Chip and PIN transactions you are not required to perform visual checks of the card, as the cardholder may retain control of the card while the transaction is performed, however for other transaction types it is important to remember to check each card carefully to ensure it is genuine. Carrying out these visual checks each time will help to minimise card fraud.

Please remember: With PDQ terminals or your own electronic point of sale equipment, always ensure that the cardholder number presented matches the number printed on the receipt. If it does not, ring Authorisation on 0844 822 2000.* Once connected to the automated Authorisation system, advise that you have a Code 10 call (or press 9) at the transaction type prompt. Your call will then be transferred to a customer service advisor and you should tell them, "I have a card number mismatch."

Please be aware that Maestro and V PAY are an exception to this, as the number printed on the front of the card may in fact be the bank account number.

1.1.1 Visa Credit

Acceptable for electronic and paper fallback transactions.

If you are suspicious about a card, a card presenter or the circumstances surrounding a card transaction, please call Authorisation on **0870 24 24 240.***

Card pictured is a sample issued by Barclaycard.

Chip
Most cards carry an embedded microchip.

Card Validity Dates
Cards should not be accepted if they are not in date.

Cardholder Name
Name of cardholder is embossed. Title may also be embossed.

Cardholder Number
16-digit account number with first 4 digits printed below.

Card Type Identification
Letter 'V' tilted to the right after the expiry date is now an optional feature.

Symbol/Logo
Gold and blue 'Visa' on white background.

Contactless Acceptance Mark
Card is capable of undertaking contactless transactions. This is optional.

Magnetic Stripe

Signature Strip
'Visa' repeated in pattern.

Cardholder Signature
Card must be signed.

Hologram
Plain, silver or gold background. Dove appears to fly and change colour when tilted.

1.1.2 New Visa card design

Acceptable for electronic and paper fallback transactions.

If you are suspicious about a card, a card presenter or the circumstances surrounding a card transaction, please call Authorisation on **0844 822 2000**.*

Cards shown for visual purposes only – not actual cards.

Some cards may contain Visa holographic magnetic stripe (a single dove or a series of doves in flight) and some will contain the traditional magnetic stripe.

Signature Panel
Design can be customised.

CVV2
Can also be found within the signature panel.

Optional Chip
Printed first 4 digits of account number.

Embossed or printed account number.

Cardholder name or identifier.

BANK IDENTIFICATION AREA

4000 0012 3456 7899

GOOD THRU 12/10

CARDHOLDER NAME

VISA

Expiry date.

Visa Brand Mark

'V' UV Element

In addition, newer cards will carry a hologram of a single dove on the front or a mini hologram on the reverse.

New Visa card design variations. The new Visa card designs allow issuers to display the card information in a variety of ways (see below).

1.1.3 MasterCard

Acceptable for electronic transactions. Paper fallback is acceptable for embossed cards only.

If you are suspicious about a card, a card presenter or the circumstances surrounding a card transaction, please call Authorisation on **0844 822 2000.***

Card pictured is a sample issued by Barclaycard.

Card Validity Dates
Retailers can accept an expired/prevalid card provided they seek and obtain online authorisation from the issuer and the authorisation message carries the correct expiry date on the card. Cards with an unembossed cardholder number will have an unembossed validity date.

Chip
Most cards carry an embedded microchip.

Card Type Identification
Letters 'MC' tilted to the right after the expiry date is now an optional feature.

Symbol/Logo
Linked circles in red and orange with 'MasterCard' printed across the centre of the symbol.

Cardholder Number
16-digit account number with first 4 digits printed below. This may or may not be embossed.

Cardholder Name
Name of cardholder is embossed. Title may also be embossed.

Magnetic Stripe
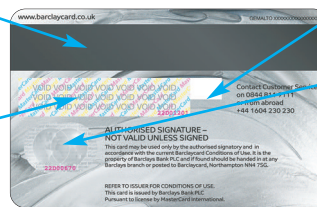
Signature Strip
'MasterCard' repeated in pattern.

Cardholder Signature
Card must be signed.

Hologram
'MasterCard' repeated across background with picture of globe in front. This can appear anywhere on the card back as long as that placement does not impact any other design element or the chip. Hologram changes colour when card is tilted.

1.1.4 Alternative MasterCard

Acceptable for electronic and paper fallback transactions.

If you are suspicious about a card, a card presenter or the circumstances surrounding a card transaction, please call Authorisation on **0844 822 2000.***

The 'MC' security character is no longer permitted on newly issued cards (effective June 1st 2006) but may continue to appear on old cards until June 2010.

Account Number
The account number must be clear and uniform in size and spacing and must appear on one line. This may or may not be embossed.

The 16-digit account number must start with 5, and the first four digits must be the same as the ones printed directly below.

Chip may be present on card.

An additional line of unembossed information may be imprinted directly beneath the cardholder name. This will be the same typeface, size and colour as the cardholder name.

Brand Mark Areas
These must include a hologram unless the hologram or HoloMag tape appears on the back of the card.

Brand Mark
Cards must include a full-colour MasterCard brand mark, which may be below or above the global or debit hologram.

Expiry Date
The card must include a valid expiry date. Cards with an unembossed cardholder number will have an unembossed expiry date.

HoloMag Tape
May be used in place of the traditional magnetic tape.

Debit Hologram
This can appear anywhere on the card back as long as that placement does not impact any other design element or the chip.
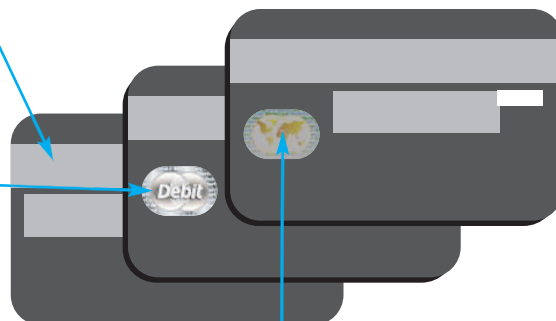
Global Hologram
On back next to the signature panel.

First four digits of the account number must be the same digits as those printed directly below.

Card Design
and MasterCard brand mark may be orientated vertically.

Brand Mark Area
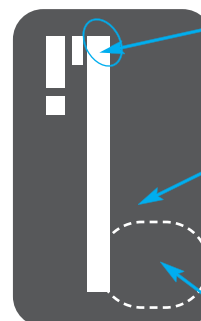
New MasterCard unembossed card design variations. The new MasterCard designs allow issuers to display the card information in a variety of ways.

Issuer Identification
5412 3456 7890 1234
5412
01/00-12/04
LEE M CARDHOLDER
MasterCard
ELECTRONIC USE ONLY

Issuer Identification
5412 3456 7890 1234
5412
01/00-12/04
LEE M CARDHOLDER
MasterCard
ELECTRONIC USE ONLY

1.1.5 New V PAY card

V PAY is a new European chip only card acceptable for electronic transactions.

If you are suspicious about a card, a card presenter or the circumstances surrounding a card transaction, please call Authorisation on **0844 822 2000**.*

Cards shown for visual purposes only – not actual cards.

Chip
A chip must appear on the front of the card.

Ultraviolet "V" element
When placed under an ultraviolet light, a "V" printed in ultraviolet ink will be visible over the V PAY logo.

Magnetic Stripe
Use of the Visa holographic magnetic stripe with doves in flight is optional. You may see this magnetic stripe or a traditional one on a V PAY card.
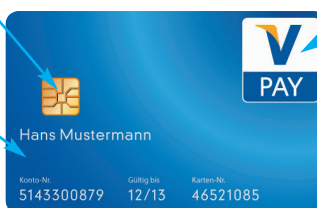
V PAY logo
The V PAY logo appears on the front of the card. Alternative logo placement options and vertical orientation of the card and logo are possible.
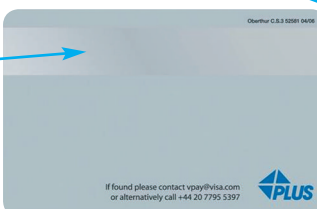
Unembossed Card
Unlike other Visa cards, the cardholder name, account number and expiry date may be printed on either the front or back of the card, not embossed.

Hans Mustermann
Konto-Nr. 5143300879
Gültig bis 12/13
Karten-Nr. 46521085

If found please contact vpay@visa.com or alternatively call +44 20 7795 5397
PLUS

1.1.6 Visa Debit

Acceptable for electronic and paper fallback transactions.

If you are suspicious about a card, a card presenter or the circumstances surrounding a card transaction, please call Authorisation on **0844 822 2000**.*

Cards shown for visual purposes only – not actual cards.

Chip
Most cards carry an embedded microchip.

Cardholder Number
16-digit account number with first 4 digits of the account number printed below.

Cardholder Name
Name of cardholder is embossed. Title may also be embossed.

Visa Brand Mark
This could be displayed top right or top left as well.

Card Validity Dates
Cards should not be accepted if they are not in date.

Visa Debit
4000 1234 5678 9010
4000
12/12
CARDHOLDER NAME
VISA DEBIT

Magnetic Stripe

Signature Strip
The reverse of some Visa debit cards may look similar or identical to the reverse of a Visa credit card.
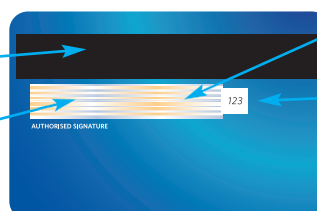
Cardholder Signature
Card must be signed.

CVV2 Mark
Some card issuers may include an optional 'link' logo and/or a 'cheque guarantee' hologram.

123
AUTHORISED SIGNATURE

1.1.7 Visa Electron

Acceptable for electronic transactions only. Please remember: The full card number, cardholder name and 'valid from' date may not appear on the front of all cards. The three-digit Card Security Code, which can be found on the signature panel, will only be present if the full card number appears on the front of the card.

Cards shown for visual purposes only – not actual cards.

Cardholder Number
16-digit account number with first 4 digits of the account number printed below. Full account number may not appear on all cards.

Cardholder Name
Printed or embossed, shows front or back. Title may also show. Cardholder name may not appear on all cards.

Hologram
Dove appears to fly and change colour when card is tilted (optional). May appear on front or back of the card.

Card Validity Dates
Cards should not be accepted if they are not in date.

Symbol/Logo
Visa logo and the word 'Electron'.

Card Type Identification
'Electronic use only' may appear on some cards.

Magnetic Stripe

Signature Strip
The reverse of some Visa debit cards may look similar or identical to the reverse of a Visa credit card.

Cardholder Signature
Card must be signed.
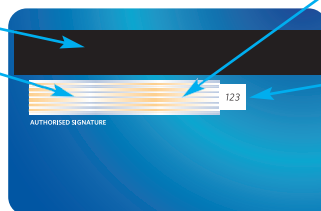
CVV2 Mark
In addition, card could carry a hologram on the reverse.

1.1.8 Solo

Acceptable for electronic transactions only.

Cards shown for visual purposes only – not actual cards.

Chip
Card may carry a chip.

Cardholder Name
Name of cardholder is embossed.

Card Identification
Issue number: this will not appear on all cards.

Card Validity Dates
Cards should not be accepted if they are not in date.

Symbol/Logo
Solo logo on either front or back.

Hologram
Most cards carry a hologram.

Magnetic Stripe

Cardholder Signature
Card must be signed.

1.1.9 Maestro

Acceptable for electronic transactions only.

Cards shown for visual purposes only – not actual cards.

Chip
Some cards carry an embedded microchip.

Cardholder Number
May not appear on all cards. Cards may have a 12 – 19-digit account number printed or embossed. This may be the bank account number not the card number.

Cardholder Name
The cardholder's name may not always appear on the card.
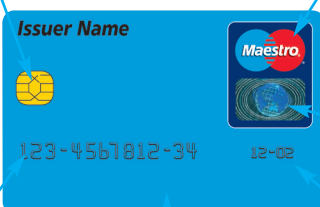
Symbol/Logo
Blue and red interlocking circles with 'Maestro' printed across centre of symbol in white.

Hologram
May not appear on all cards.

Card Validity Dates
Cards should not be accepted if they are not in date. The expiry date may not appear on the card, however, if it does, the card should not be accepted if it has expired.

Magnetic Stripe
This will include the Maestro card account number which will be printed on the transaction receipt. This may differ from the embossed card number on the front of the card.

Cardholder Signature
Card must be signed.

Signature Strip
May have the word 'Maestro' repeated in pattern.

1.1.10 JCB

Acceptable for both electronic and paper fallback transactions.

Cards shown for visual purposes only – not actual cards.

Cardholder Number
Embossed 15 or 16-digit number, with first 4 digits printed above or below.

Card Validity Dates
Cards should not be accepted if they are not in date.

Cardholder Name
Name of cardholder is embossed. Title may also be embossed.

Symbol/Logo
JCB logo appears in right-hand corner.

Hologram
A sun, moon and JCB characters appear when card is tilted.

Card Type Identification
'JCB' embossed after expiry date. A gold card will show 'JCB G'.

Magnetic Stripe

Cardholder Signature
Card must be signed.

1.1.11 Holograms

Check that the hologram moves as you tilt the card back and forth. Many counterfeit cards use poor reproductions and even with a quick glance you can spot a fake. Holograms will contain the following designs:

- Visa – a flying dove
- MasterCard – a globe which will change colour
- JCB – a globe and rising sun
- UK Maestro – own logo
- Visa Electron – a flying dove
- Cheque Guarantee – own logo
- Solo – own logo.

Visa – flying dove optional for Visa Electron

MasterCard

JCB

UK Maestro

Solo

Cheque Guarantee

See Section 1.4.1.3 Holograms for more details.

1.1.12 Ultraviolet motifs

If the ultraviolet motifs do not appear when checked under a UV detector, the card may be forged. A dove will appear on an old style Visa card, while the letters 'MC' will appear on a MasterCard. UK Maestro and Solo cards will show their respective symbols. Take care, as some Electron cards do not have a UV motif.

New Design Cards

Visa and Visa Electron – the Visa brand mark will appear more sleek in design than the current standard card Visa brand mark. There will be an ultraviolet 'V' visible over the Visa brand mark when placed under an ultraviolet light.

V PAY – a 'V' printed in ultraviolet ink will be visible over the V PAY logo.

MasterCard – MasterCard UV markings will remain the same.

Maestro – The word 'Maestro' appears on the bottom left-hand side of the card.

You can obtain a UV detector from the following supplier, who will give a price upon request:

LMN Office Furnishings Limited,
Telephone: **01642 468587**,
Fax: **0870 264 1721**,
email: lmnoffice@supanet.com

PLEASE BE AWARE THAT THIS IS NOT AN ALTERNATIVE NUMBER TO CALL FOR NAME AND ADDRESS CHECKS OR CODE 10 CALLS.

American Express

Visa
(On newly issued cards, the letter 'V' on the Visa logo will appear as an ultraviolet mark.)

MasterCard

Solo

Maestro

1.2 Additional card recognition

1.2.1 Visa Credit and MasterCard

- Many cards will carry a shortened signature strip
- The last 4 digits of the card number, together with a 3-digit Card Security Code will appear on the left-hand side. On the new design Visa cards, the 3-digit Card Security Code will appear on the signature panel or in a white box beside the signature panel. MasterCard have now mandated the 3-digit Card Security Code to appear in a white box adjacent to the signature panel
- Some older cards in circulation may show the whole account number with the 3-digit Card Security Code
- Some foreign cards may carry a message on the signature strip and will not be signed. Please ask for identification such as a passport or driving licence, and carry out a Code 10 call (Authorisation). Refer to Authorisation and Code 10 calls (Section 2.1.9).

1.2.2 Visa Debit

- The last 4 digits of the account number, plus a 3-digit Card Security Code, will appear on the signature strip. The new Visa Debit cards will carry the 3-digit Card Security Code in a white box beside the signature panel
- Some older cards in circulation may show the whole account number with the 3-digit Card Security Code.

1.2.3 Visa Electron

- The last 4 digits of the account number, plus a 3-digit Card Security Code, will appear on all UK-issued cards, but may not be on some foreign cards. The new Visa Electron cards will carry the 3-digit Card Security Code in a white box beside the signature panel
- Some older cards in circulation may show the whole account number with the 3-digit Card Security Code
- Some Visa Electron cards are for use in their own country only. If the card is marked with this information, do not accept the card.

1.2.4 UK Maestro and Solo

- The cardholder number and the 3-digit Card Security Code will appear on the signature strip. Most cards carry a pattern showing the word 'signature' in red
- Some UK Maestro and Solo cards serve additional functions. They may carry cheque guarantee details or branding for an ATM network. The branding may be on the front or the back of the card.

1.2.5 Maestro

- A cardholder photograph and signature may appear on the front of the card.

1.2.6 JCB

- The signature strip will show the 3-digit Card Security Code
- Some cards will carry a microchip.

1.2.7 Visa and Visa Electron mini cards with mini dove design hologram

These are a miniaturised version of a Visa or Visa Electron card.

Mini card design elements

Visa brand mark. The Visa brand mark is the stylised word 'Visa'. On cards the Visa brand mark appears in Visa Blue and Visa Gold and is shown on a standardised white background.

Visa brand mark with the ELECTRON identifier. The Visa brand mark with the ELECTRON identifier is the stylised word 'Visa' in Visa Blue and Visa Gold shown on a standardised white background with the word 'ELECTRON' underneath.

For a Visa or Visa Electron mini card, reduced sizes of the Visa brand mark and the Visa brand mark with the ELECTRON identifier have been created. The mark appears in the upper- or lower-right position.

Use of the mini dove design hologram on a Visa mini card is required. Use of the mini dove design hologram on a mini Visa Electron card is optional. Issuers have the option of placing either a mini dove design hologram on the front of the card or on the back of the card.

Signature panel

A signature panel will appear on the back of the card.

Magnetic stripe

The magnetic stripe will appear on the back of the card.

Card Security Code

A 3-digit Card Security Code number will be indent-printed or laser-engraved on the back of the card in a standardised location, either the white area next to the signature panel, or directly onto the signature panel.

Cardholder photograph and signature

A photograph of the cardholder may appear on either the front or back of the card.
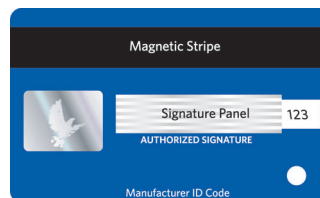
1.3 Commercial cards

There are 3 main types of card available:

Business card

- Gives small businesses a business payment method, an expense control mechanism and a cash management tool
- Ideal for paying for everything a small business needs – travel and entertainment, office supplies, stationery, computers etc
- Available as charge and credit cards.

Corporate card

- For travel and entertainment for mid-sized to large multi-national companies
- Allows streamlined administration of all expenses, saving time and money by reducing cash advances and paper-based payment methods
- Management information is available, making it easier to control expenditure and to manage and develop expense policies.

Purchasing card

- Used by large businesses, Government departments and public sector bodies
- Enables monitoring and control of expenditure and the provision of information to help to improve cost efficiency
- Allows VAT reclamation
- Removes paper-based processes, through electronic invoicing with detailed breakdowns of expenditure
- Card can be used face-to-face, online, by phone or embedded into customer ordering systems.

Barclaycard Hotel Tracker

- Is a Corporate card account where no plastic cards are issued, aimed at hoteliers and hotel booking agents (see Section 2.2 Card-not-present transactions for further details).

For more information and for other card types, go to **www.mastercard.co.uk** or **www.visa.com**

Benefits you can help to deliver to your customers

Monitor and control spending

Card Issuers are able to provide your customers with management information relating to their purchasing spend which can include summary level reports or detailed breakdowns of expenditure which is then analysed or used with accounting packages.

Claiming back VAT

If you accept purchasing cards and you are equipped to support electronic VAT invoices, then your customers will be able to reclaim the VAT on expenditure using the 'Evidence for VAT Deductions' report which is accredited by HM Revenue and Customs.

Contact Barclaycard Customer Services Department on 0844 811 6666* for help with accepting these cards and providing your customers with the appropriate information to help them to run their businesses.

For information or help with taxation we suggest you contact Her Majesty's Revenue and Customs or seek specialist tax advice.

1.4 Fighting fraud

We have focussed on areas of fraud prevention that our customers seek advice on. We have also included information on how we can work together to minimise the risks.

Authorisation only confirms that the issuer of the card agrees there are enough funds to pay for the goods and to confirm the card has not been reported lost or stolen. Authorisation does not guarantee payment.

1.4.1 Preventing and detecting fraudulent card-present transactions

To prevent fraudulent transactions being charged back at a later date, any chip and PIN-enabled cards should be used with a chip and PIN-enabled POS terminal. Likewise, you must ensure you obtain Authorisation on any transaction where the card details are not captured using the chip (eg when presented with a magnetic stripe card transaction) to avoid the risk of loss to card fraud.

If your terminal is chip and PIN-enabled you could be presented with a number of different scenarios, all of which you can accept:

- magnetic stripe and signature verification (eg from an overseas customer where the country has yet to upgrade to chip and PIN technology)
- chip and signature verification (eg from a disabled customer who is unable to use PIN technology)
- chip and PIN verification.

If your terminal has contactless reader, you will also be able to accept contactless transactions with no verification (Section 2.1.6).

In addition, you may wish to undertake occasional mail or telephone order transactions. We strongly recommend you read Card-not-present transactions (Section 2.2) and Chargebacks and retrieval requests (Section 4). If the majority of the transactions you are accepting are mail, telephone or internet transactions, it is essential that you advise us that you are doing so, as we have a range of products and services that may help you to reduce the risk of transactions being charged back at a later date.

If your customer does not remember their PIN, the transaction must be authorised by the issuer. If you rent a PDQ terminal from Barclaycard, the terminal will automatically do this for you. Please ensure you carefully follow the terminal prompts and refer to your Terminal Operating guide if necessary. Please be aware that it may be declined and therefore you may need to ask your customer for payment by other means. If you use your own or a third party supplier's terminal, it is your own responsibility to ensure your terminal seeks Authorisation when required to do so.

In these instances, provided your terminal is chip and PIN-capable, you will be protected against potential counterfeit, lost and stolen, and intercepted card fraud.

Card fraud statistics show there is increased fraud with non-PIN cards. Be aware of the security checks you should make to minimise card deception:

- Keep hold of the card at all times
- Keep the goods out of reach of the customer
- Check the card against any warning notices you have received from us
- Check the 'valid from' date. If the card is newly issued, be extra vigilant
- Watch out for hesitancy when the customer signs and make sure that the signature they give matches the signature on the card
- Be careful not to be distracted during a transaction. Fraudsters may try to hurry you, or draw your attention away from making card checks
- Check the name on the card and compare against the presenter
- Be sure not to process transactions on behalf of anyone else. This is a breach of your Merchant Agreement and could lead to transactions being charged back to you.

1.4.1.1 Counterfeit cards

Due to the increase in quality of fraudulent cards being produced recently, changes in design for both Visa and MasterCard have been introduced. This is the first significant change in nearly 30 years.

The new designs along with the current design will both be in circulation over the next four years. The current designs will be phased out by 2010.

When checking the card, current card designs have several features that may not be present on a Visa or MasterCard:
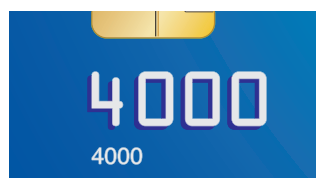
- On current design Visa cards it is now only optional to carry an embossed 'V' tilted to the right, next to the expiry date (see New Visa card design in Section 1.1.2)

- On current design MasterCard it is now only optional to carry the embossed letters 'MC' tilted to the right to form an unusual 'M' next to the expiry date (see MasterCard in Section 1.1.3)

- The first 4 digits of the embossed card number should be printed below the card number. Check that the numbers match.

1.4.1.2 New card designs for Visa and MasterCard

The repeat of the first 4 embossed digits printed below the card number will remain on the new designs.

However, you need to be aware that on the new designed cards for both Visa and MasterCard the unique embossed symbols 'V' or 'MC' will be removed. Since many fraudsters have mastered the art of copying this feature it is considered less secure than when first introduced.

If you are suspicious about a card, a card presenter or the circumstances surrounding a card transaction, please call Authorisation on **0844 822 2000**.*

1.4.1.3 Holograms

Current card design

Check that the hologram moves as you tilt the card back and forth. Many counterfeit cards use poor reproductions and even with a quick glance you can spot a fake. Holograms will contain the following designs:

- Visa – a flying dove
- MasterCard – a globe which will change colour
- JCB – a globe and rising sun
- UK Maestro – Globe or APACS cheque guarantee symbol
- Visa Electron – flying dove is optional.

Also see Section 1.1.10 for more details.

New card design

With the new design cards both Visa and MasterCard will allow the hologram to appear on the front or the back of the card.

Visa – the dove hologram will appear on the front of the card. Or a mini dove hologram may be on the back of the card.

MasterCard – the redesigned MasterCard globe hologram is integrated with the magnetic stripe as a hologram stripe or will show the standard hologram symbol, on the front or back of the card.

1.4.1.4 Ultraviolet motifs

Current card design

If the ultraviolet motifs do not appear when checked under a UV detector, the card may be forged. A dove will appear on a Visa card, while the letters 'MC' will appear on a MasterCard. Maestro and Solo cards will show their respective symbols. Take care, as some Electron cards do not have a UV motif. Also see Section 1.1.6 for more details.

New design cards

Visa and Electron – the Visa brand mark will appear more sleek in design than the current standard card Visa brand mark. There will be an ultraviolet 'V' visible over the Visa brand mark when placed under an ultraviolet light.

V PAY – a 'V' printed in ultraviolet ink will be visible over the V PAY logo.

MasterCard – MasterCard UV markings will remain the same.

Maestro – The word 'Maestro' appears on the bottom left-hand side of the card.

You can obtain a UV detector from the following supplier, who will give a price upon request:

LMN Office Furnishings Limited,
Telephone: **01642 468587**,
Fax: **0870 264 1721**,
email: lmnoffice@supanet.com

PLEASE BE AWARE THAT THIS IS NOT AN ALTERNATIVE NUMBER TO CALL FOR NAME AND ADDRESS CHECKS OR CODE 10 CALLS.

1.4.1.5 Card chip-read/swipe failure

The following information will help you and your company reduce losses through counterfeit fraud. The vast majority of your card transactions are chip-read or swiped through your electronic Point of Sale (POS) terminal with no problems. However, on occasions when your terminal is unable to read the chip or magnetic stripe on the card, your staff need to manually enter the card number embossed on the front of the card using the terminal keys.

If you have a chip-enabled terminal you should find chip cards will not usually fail to dip. You may find, if you key enter or revert to the magnetic stripe swipe on a chip card, that the issuer may decline the card. This is for increased security. If this is the case, follow the terminal prompts, which may include you having to speak to our Authorisation Department. Please ensure you follow their instructions. Only give the card back to the customer if you are not asked to retain the card.

When a card transaction is processed in this way a number of very important security checks, usually undertaken by the electronic terminal, are bypassed. It is evident that some fraudsters are aware of this situation and are exploiting the opportunities. Under Visa and MasterCard Card Scheme Regulations, a Card Issuer has the right to request sight of an imprinted verification voucher signed by the cardholder. Failure to provide this gives the Card Issuer the right to charge the transaction back to you.

To protect your business from losses and reduce the risk of chargebacks when a card fails to be read by your electronic processing equipment, you should:

- enter the card number embossed on the front of the card using the terminal keys and seek Authorisation
- in addition to manually entering the card number into the terminal, imprint a sales voucher and fully complete the verification voucher. This must be signed by the customer. The words 'For verification only – this voucher is not for banking' should be written on the voucher. Pass the customer copy to the customer along with the terminal receipt. If you need a supply of preprinted verification vouchers please call **0845 600 6766***
- please do not bank the verification (or sales) voucher, as your terminal will still process the transaction in the usual way
- banking the verification or sales voucher will cause the cardholder's account to be debited twice. The voucher is simply your proof that the card was present at the point of sale. It can be used to prove the validity of the transaction if the customer subsequently disputes it

- the merchant copy of the terminal receipt and the verification (or sales) voucher should be kept together in case of any future query. Failure to provide copies in the event of a query from a Card Issuer could result in a chargeback and losses to your business. Your verification vouchers should be fully completed including full details of the goods/services purchased. Do not write just 'Goods'. Ensure you write the Authorisation code provided by the Authorisation Department.

1.4.1.6 UK Maestro and Solo cards

If a UK Maestro or Solo card fails to swipe through your terminal you should carry out all of the actions as detailed above as well as contacting Authorisation for a Code 10. In order to defend this type of chargeback we MUST have a record of a Code 10 being approved by the Card Issuer.

1.4.1.7 Maestro cards (issued outside the UK)

Maestro transactions must be captured by swiping the magnetic stripe or reading the chip. There is no manual key entry permitted. If a card fails to chip-read or swipe through, you should ask your customer for another form of payment as there is no chargeback defence in the event of a card swipe failure.

1.4.1.8 Visa Electron cards

The majority of Visa Electron cards and all V PAY cards are not embossed and therefore Visa Electron transactions MUST be processed electronically. If a card fails to chip-read or swipe through your terminal you should ask your customer for another form of payment as there is no chargeback defence in the event of card-swipe failure.

1.4.1.9 Returning wanted or recovered cards

If our Authorisation operator asks you to destroy a card and return it to us, please follow the procedure described below. You should politely inform your customer of the decision, without putting any other customers or yourself at risk.

1. To preserve fingerprints and other forensic evidence, handle the card as little as possible and only by the edges.
2. With the card facing you, cut off only the bottom left-hand corner.
3. Make sure the signature strip, magnetic stripe, chip and hologram are intact.
4. You will find your first recovered card form in your welcome pack.

Further recovered card forms may be obtained by calling our Customer Services Department on **0844 811 6666.***

- The form must be completed in full and the cut-off slip of the completed form should be retained in your files
- The top section of the form and both pieces of the card should be sent to:

  Recovered Card Services, Barclaycard, Department RC, Northampton NN4 7SG.

If you are returning a Visa Electron card, please also enclose a copy of the terminal declined receipt.

1.4.1.10 Reward scheme

A £50 reward may be paid to your business for the return of a wanted card and it is at the discretion of the business owner whether reward payments are passed on to the person recovering the card.

In the event of the police needing to retain a wanted card or sales voucher for investigation (for example, if a stolen card is presented) you will need to keep certain details in the event of a query. Please ensure you have a copy of the sales voucher (a good photocopy will be acceptable) as well as the following information:

- the card number
- the expiry date
- the name embossed on the card
- UK Maestro/Solo card issue number (if applicable)
- date card recovered
- the crime reference number
- details of the officer and police station dealing with the case.

A reward can still be claimed if the police take the card for evidence.

1.4.1.11 Cheque guarantee

For 24-hour-a-day validation of a Barclays Bank cheque, guaranteed by a Barclays Connect card, Barclaycard Visa card or a Barclays Premier card, call **0800 515 788.***

Please remember: Company cheques cannot be guaranteed by any card.

If you are suspicious of the cheque, the cheque guarantee card or the presenter, you need to inform the Authorisation operator on **0800 515 788*** (and follow their instructions). Start your conversation by saying, "This is a Code 10 call."

1.4.1.12 Fraud prevention advice

Transaction laundering
If you are approached with a proposal to buy card transactions or process other business transactions through your number, please contact us on **01604 252773.*** This is called laundering and is contrary to the terms of your Agreement.

Bogus/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 should be wary. 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.

Be aware some fraudsters may make attempts to mirror your website to gain genuine information from cardholders.

To report any of these instances contact **internetsecurity@barclays.com**

1.4.2 Preventing and detecting fraudulent card-not-present transactions

Card-not-present (CNP) fraud takes place because neither the cardholder nor the card are present at the point of sale when a transaction is made. Examples of CNP transactions are orders made over the internet or by phone, mail order or fax. Such transactions mean that:

- you are unable to physically check that the card being used for payment is genuine

- it is not possible to verify whether the identity given by the individual is correct

- a PIN is unable to be entered or checked to ensure the card is authentic.

Card-not-present (CNP) fraud is a growing problem in the UK and elsewhere as criminals turn their attention to CNP fraud.

Extra care needs to be taken when taking transactions online, over the phone, or by mail order and fax. You need to consider the risks before accepting payment:

- A CNP transaction means that a cardholder and a card are not present. Unlike a normal face-to-face situation a retailer is unable to check that the card is genuine – and that the 'customer' is not just using a stolen card number. In these situations, the genuine cardholder may not be aware that their card number has been compromised eg a fraudster has taken the card details from a customer's discarded receipt

- Only online transactions can be authenticated by the cardholder to prove they are a genuine customer, when you use Verified by Visa and MasterCard SecureCode – this is comparative to PIN at point of sale. If a retailer is unable to prove that the cardholder is genuine they are unable to guarantee that the card information provided relates to the genuine cardholder

- Authorisation only confirms the issuer of the card agrees there are enough funds to pay for the goods and to confirm the card has not been reported lost or stolen. **Authorisation does not guarantee payment**

- Never release goods to a third party. Always ensure that goods are sent to the named person on the card

- If a cardholder comes to collect the goods in person, cancel the CNP payment and process as a card-present transaction.

Questions you need to ask yourself before accepting the transactions:

- Why has this customer come to me?

- Is the sale too easy, is the customer uninterested in the price or details of the goods and are they a new customer?

- Are the goods high value or easily resaleable?

- Is the transaction out of character compared to your usual orders or is the customer ordering many different items and do they seem unlike your usual customer?

- Is the customer reluctant to give a landline phone number or only prepared to give a mobile number?

- Does the address provided seem suspicious or has the delivery address been used before with different customer details?

- Is the customer being prompted by a third party whilst on the phone?

- Is the customer attempting to use more than one card in order to split the value of the sale?

- Does the customer seem to lack knowledge of their account? Are they providing details of someone else's card (eg that of a client or family member)?

- Does the customer seem to have a problem remembering their home address or phone number or do they sound as if they are referring to their notes?

Use fraud monitoring tools recommended by the card schemes. The most common examples of these tools are: Card Security Code and Address Verification Service (CSC/AVS) fraud screening.

1.4.2.1 Velocity checking and fraud screening

Use of Rule Based and Neural Networks as additional tools can be beneficial and help to check the validity of transactions. A system which enables you to crosscheck the name, address, telephone numbers, card details, email address, IP address with past and daily records could help you to reduce risk to your business.

Crosschecking this type of information continually will identify any duplication of information which may indicate other attempts to use similar details by a possible fraudster.

For example they may quote different card numbers but use the same name or address or may quote entirely different details but still be seen to come from the same IP address.

Any such instance of duplication should be rejected and checked further before accepting the order or request.

There are a series of third party solutions providers available to provide this additional tool and assist with checking the authenticity of customer information:

Further advice for internet transactions

To add to existing velocity checks:

- check for sequential card numbers
- review orders made using non-UK issued cards
- review orders where IP address does not match delivery address (country)
- review orders going to/coming from same customer – name/address/card number
- review/decline all/new orders going to a different delivery address
- review/decline duplicate purchases
- review/decline if postal code does not match
- decline if CSC does not match
- decline new orders with an invalid expiry date.

Use the 'chargeback data' you receive to:

- highlight potential problem names/addresses/ IP addresses
- always ensure that you respond promptly to 'request for information letters'; you may be able to prevent the chargeback
- also use Internet Authentication (3D Secure) and CSC/AVS for added security.

Check **www.cardwatch.co.uk** and **www.barclaycard.co.uk/paymentacceptance** for additional information. Fraud Literature for staff awareness and training is also available.

1.4.2.2 Card Security Code and Address Verification Service (CSC/AVS)

Barclaycard and the UK card industry have worked together to develop a service to reduce card-not-present fraud, simply by requesting a small amount of additional information from the cardholder. This information is comprised of:

- the Card Security Code (the last 3 numbers on the signature strip on the card or the 3 digits in a white box adjacent to the signature panel)
- the numbers in the cardholder's postcode
- up to the first 5 numbers of the cardholder's full statement address.

The Card Security Code must not be stored after the transaction has been authorised.

This service is available for customers processing transactions via our PDQ and ePDQ products. Please contact us on **0844 811 6666*** for further information.

If you are processing transactions through your own electronic point of sale equipment, you can take action now by contacting your electronic point of sale equipment supplier for information about development requirements and the timescales needed to implement the service.

1.4.2.3 Authentication or 3D Secure

Authentication is an industry-wide initiative to help combat fraud and protect businesses trading over the internet. Visa, Maestro and MasterCard cardholders buying online can verify their identity with a password that automatically authenticates the cardholder, so you can safely accept their order.

Benefits for you

- **Increased sales and profits** – customers prefer to buy from websites that offer the reassurance of Authentication
- **Greater security** – increased protection against fraud
- **Cost savings** – thanks to the reduced risk of transactions being charged back
- **Convenience** – Authentication is quick and easy for your staff to use
- **Time savings** – spend less time on dealing with transactions that have been charged back.

Benefits for your customers

- **Peace of mind** – because if their card is stolen it's more difficult for the fraudster to use it on websites that include Authentication
- **Convenience** – it's quick and easy for your customers to enter their password, and their payment will be authorised in seconds
- **Reassurance** – customers will know you have invested in these safeguards, so they can safely trust you with their card details.

How Internet Authentication makes online transactions safer

1. A customer browsing on the internet decides to buy from you with a Visa, MasterCard or Maestro*.
2. Your payment pages eg ePDQ Card Payment Interface (CPI), communicate with the Visa/MasterCard Directory, which then contacts the Card Issuer.
3. The Card Issuer confirms whether the customer has registered for Internet Authentication.
4. If the Card Issuer supports Internet Authentication, a 'pop-up' or 'in-line' web window appears on the customer's screen. If not, the transaction proceeds to Authorisation detailed in point 7 below.
5. The Card Issuer asks for the customer's Internet Authentication password and accepts or rejects it.
6. If the password is correct, the payment process continues (if incorrect, the transaction may be stopped).
7. Your payment software eg ePDQ, authorises the payment details and passes them to the acquirers eg Barclaycard, for settlement.

*Provided your internet site supports Verified by Visa and MasterCard SecureCode.

Which cards are covered?

- All standard issued Visa, Maestro and MasterCard cards are included for Authentication except internationally issued commercial cards which are only covered if the transaction is fully authenticated ie the cardholder successfully inputs the correct password. Visa cash cards are excluded.

Visa and MasterCard regularly review and amend the types of card and regions of the world that are covered by Internet Authentication. Please refer to the current version of the Internet Authentication Procedure guide for full details.

How Authentication works with various systems and providers
Authentication is available with our ePDQ service or stand-alone with other software.

If you have the ePDQ Cardholder Payment Interface (CPI)
Authentication works best with our cost-effective ePDQ CPI. It's straightforward to use, and whenever new software or security measures become available we'll upgrade you automatically – saving you time, technical resources and money. The ePDQ CPI includes a co-branded payment page, to reassure your customers that they're dealing with a trusted brand.

If you have the ePDQ Merchant Payment Interface (MPI)
You can also benefit from Authentication, as it will work with your own website and can be integrated using our software development kit. You should allow several days for installation – time you could save by upgrading to our CPI.

If you use a payment service provider other than ePDQ
They may not offer Authentication. However, they could install it with our software development kit, but they may charge you for this service.

If you have your own software for internet transactions
You can install Authentication with our software development kit.

If Barclaycard processes your transactions and you are using Authentication from another provider
It must be approved by us and registered by Barclaycard with Visa and MasterCard.

If you are using Authentication from another provider
It must be approved by us and registered by Barclaycard with Visa and MasterCard.

For more information about Authentication, please visit **www.barclaycard.co.uk/paymentacceptance** or call **0844 811 6666**.*

1.5 Card scheme requirements

As a member of the card schemes we require you to comply with the Payment Card Industry Data Security Standard (PCI DSS) and a Maestro Mandate which dictates how you accept Maestro cards. This section sets out the obligations you must comply with to achieve these standards.

1.5.1 Payment Card Industry Data Security Standard (PCI DSS)

What is PCI DSS?
It is an auditable set of standards designed to ensure that certain card data is stored securely by your company and any third party which stores, transmits or processes such card data on your behalf.

What information must be securely stored?
Any information that is necessary to process card transactions correctly including any information which is recorded electromechanically or otherwise on any payment card and includes, although is not limited to, the following:

- any information that is used to authenticate a card payment including but not limited to the card number, expiry date, issue number, passwords, pass phrases and any other unique data supplied as part of the card payment

- any information that could identify individual cardholders and their purchases. This includes name, address, purchase description, amount and other details of the card payment.

This shall be referred to as Cardholder Data in the rest of this section.

What information must not be stored at any time?
You must not store any of the following information at any time:

- the contents of the magnetic stripe also known as Track 2 Data

- the Card Verification Value or CVV contained in the magnetic stripe

- the Card Verification Value contained in the magnetic stripe image in a chip known as the iCVV

- the Card Security Code also known as CVV2 printed on the back of the card in or next to the signature panel

- the PIN Verification Value or PVV which is contained in the magnetic stripe.

What must you do to comply with PCI DSS?

PCI DSS sets out a number of requirements which you must comply with to ensure that Cardholder Data is securely stored. You must:

1 install and maintain a firewall configuration to protect data

2 not use vendor-supplied defaults for password or other security parameters

3 protect stored Cardholder Data

4 encrypt the transmissions of Cardholder Data and sensitive information across public networks

5 use and regularly update anti-virus software

6 develop and maintain secure systems and applications

7 restrict access to Cardholder Data by business need-to-know

8 assign a unique ID to each person with computer access

9 restrict physical access to network resources and Cardholder Data

10 track and monitor all access to network resources and Cardholder Data

11 regularly test security systems and processes

12 maintain a policy that addresses information security.

In complying with the requirements as set out above you must meet the standards as specified by the PCI Standard Security Council (PCI SSC) and mandated by the Card Schemes. The current standards that you must adhere to in meeting the above requirements are as set out in 'The Payment Card Industry (PCI) Data Security Standards', version 1.2, October 2008.

This is available for download from the PCI Security Standards Council website and can be currently downloaded from the following website address: **https://www.pcisecuritystandards.org**

For more information and useful tools to help you on your journey towards compliance, please access the Barclaycard PCI DSS website at: **http://www.barclaycardbusiness.co.uk/pcidss/**

If you are unable to access the standards for any reason whatsoever you must contact us and we will advise you how you can obtain a copy of these documents.

Demonstrating compliance with PCI DSS

We need you to demonstrate that you are complying with PCI DSS and the method by which we require you to do this will differ depending upon the type and volume of card transactions that we process on your behalf. To decide which obligations you must comply with you must first determine what type of Merchant you are (Merchant Level).

For the purposes of PCI DSS, Merchants are classified as follows:

Merchant Level	Definition
Level One Merchant	• A Merchant which processes more than 6 million card transactions per year for any Card Scheme (for example more than 6 million Visa card transactions per year or more than 6 million MasterCard transactions per year); • or a Merchant that has suffered a compromise. (see details below regarding data compromises).
Level Two Merchant	A Merchant which processes between 1 million and 6 million card transactions per year for any Card Scheme (for example 2 million Visa card transactions per year).
Level Three Merchant	A Merchant which processes between 20,000 and 1 million e-commerce card transactions per year for any Card Scheme (for example 35,000 e-commerce MasterCard card transactions per year).
Level Four Merchant	• Any merchant processing less than 20,000 Visa or MasterCard e-commerce transactions per year, • and all other merchants processing up to 1 million Visa or MasterCard transactions per year.

We may from time to time audit your type and volume of card transactions. We may as a result of such audit, or if we are instructed to do so by a Card Scheme, notify you which type of Merchant you are for the purposes of PCI DSS and you agree that you will comply with the obligations of that level of Merchant as detailed below.

What you must do to demonstrate compliance with PCI DSS

When you have determined which type of Merchant you are for the purposes of PCI DSS, you will need to comply with the following obligations depending upon your Merchant Level:

Merchant Level	What you must do
Level One Merchant	If you are a Level One Merchant you must: • engage a Card Scheme Approved Qualified Security Assessor (see below for details) to complete an annual on-site audit; • provide us with a copy of the Qualified Security Assessor (QSA) Report On Compliance (executive summary only). This must be less than 12 months old; • if you have any card payment systems connected to the Internet, either directly or indirectly, contract the services of a Card Scheme Approved Scan Vendor (see below for details) to conduct quarterly network vulnerability scans; AND • provide us with a copy of the latest scan report (summary only). This must be less than 3 months old.
Level Two Merchant	If you are a Level Two Merchant you must: • engage a Card Scheme Approved Qualified Security Assessor (see below for details) to complete an annual on-site audit; • provide us with a copy of the Qualified Security Assessor (QSA) Report On Compliance (executive summary only). This must be less than 12 months old; • if you have any card payment systems connected to the Internet, either directly or indirectly, contract the services of a Card Scheme Approved Scan Vendor (see below for details) to conduct quarterly network vulnerability scans; AND • provide us with a copy of the latest scan report (summary only). This must be less than 3 months old.

Merchant Level	What you must do
Level Three Merchant	If you are a Level Three Merchant you must: • complete and provide us with an annual Card Scheme Approved Self-assessment Questionnaire and signed Attestation of Compliance, which demonstrates that you comply with PCI DSS. This must be less than 12 months old; you may want to contract the services of a Card Scheme Approved Qualified Security Assessor (see below for details) to validate this exercise; AND • if you have any card payment systems connected to the Internet, either directly or indirectly, contract the services of a Card Scheme Approved Scan Vendor (see below for details) to conduct quarterly network vulnerability scans and provide us with a copy of the latest scan report (summary only). This must be less than 3 months old.
Level Four Merchant	If you are a Level Four Merchant you must: • complete and provide us with an annual Card Scheme Approved Self-assessment Questionnaire and signed Attestation of Compliance, which demonstrates that you comply with PCI DSS. This must be less than 12 months old; you may want to contract the services of a Card Scheme Approved Qualified Security Assessor (see below for details) to validate this exercise; AND • if you have any card payment systems connected to the Internet, either directly or indirectly, contract the services of a Card Scheme Approved Scan Vendor (see below for details) to conduct quarterly network vulnerability scans and provide us with a copy of the latest scan report (summary only). This must be less than 3 months old.

Copies of all reports required to be provided as specified in the table above should be sent to:

The PCI DSS Compliance Manager
Barclaycard
Payment Acceptance
1234 Pavilion Drive
Northampton
NN4 7SG

Card Scheme Approved Qualified Security Assessor
The specialist organisations which are qualified to conduct on-site annual audits of a Merchant compliance with PCI DSS are those advised by the card schemes from time to time. Details of the current card scheme approved specialist organisations can be found at:
https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf

If you are unable to access the list for any reason whatsoever, you must contact us and we will advise you how you can obtain a copy.

Card Scheme Approved Scan Vendors
The specialist organisations which are qualified to conduct network vulnerability scans are those advised by the card schemes from time to time. Details of the current card scheme approved specialist organisations can be found at:
https://www.pcisecuritystandards.org/pdfs/asv_report.html

If you are unable to access the list for any reason whatsoever, you must contact us and we will advise you how you can obtain a copy.

Self-assessment Questionnaire
The PCI Standard Security Council has published a set of Self Assessment Questionnaires (A, B, C or D) depending on your type of business. You can find Instructions for completing a Self Assessment Questionnaire (version 1.2) on the PCI Standard Security Council website at
https://www.pcisecuritystandards.org/saq/index.shtml

If you are unable to access any of these documents for any reason whatsoever, you must contact us and we will advise you how you can obtain a copy.

Further action you may need to take
We may, as a consequence of considering any report that you must submit to demonstrate compliance with PCI DSS (as set out above):

• notify you that you are a different Merchant Level (for example a Level One Merchant rather than a Level Two Merchant) and you agree that you will comply with the obligations of that Merchant Level going forwards, or

• require that you take additional security measures to ensure compliance with PCI DSS within an agreed period of time. Barclaycard are not unique in requiring their merchants to become PCI DSS compliant; all card acquirers have the same responsibility to the Card Schemes (eg Visa and MasterCard).

Data compromises

If any unauthorised person obtains access to any Cardholder Data, or Cardholder Data is lost, or you suspect that either has happened, you must immediately notify us of this data compromise.

Consequences of a data compromise

If we are notified that you have suffered any data compromise or suspected data comprise (whether you notify us or any Card Scheme) you will be required to instruct a Qualified Forensics Investigator (QFI) to undertake a forensic investigation at your company in relation to the data compromise. The QFI will review the whole end-to-end process of handling Cardholder Data and will deliver a report on their findings, and set out recommendations for a remedial action.

Should you suffer a data compromise you will be required to pay the costs of the QFI engaged as a result of any data compromise.

If you suffer a data compromise we may notify you that you are to be reclassified as a Level One Merchant and that you will comply with the obligations of such Merchant Level.

You can find a list of QFIs at **http://www.visaeurope.com/aboutvisa/security/ais/ resourcesanddownloads.jsp**

If customer data, which you or your third parties have handled, is proven to have been compromised, stolen, used fraudulently etc. and your business is non compliant with PCI DSS, you may incur potentially substantial associated costs (eg forensic investigations, Card Scheme compromise fines, issuer losses, reputational damage). The Card Schemes may decide to levy further fines for non-compliance and storage of sensitive authentication data.

Third Parties that store, transmit or process your Cardholder Data

The PCI DSS standard applies to all merchants and their third parties that store, process or transmit cardholder data. The standard applies equally to manual processing and storage of cardholder information (eg PDQ terminals and imprinters) as well as to electronic methods of storage (eg EPOS, PC).

PCI DSS compliance applies to a merchant's overall environment, including any third parties used by the merchant that would store, process or transmit cardholder data. A merchant can only reach compliance if its affected third parties are also compliant and PCI DSS compliance must be re-validated annually.

Third Parties include, but are not limited to:

- Resellers
- Till vendors
- EPOS vendors
- Software Application Providers
- Payment Service Providers
- Payment Processing Bureaux
- Data Storage Providers
- Web Hosting Providers
- Shopping Cart Providers
- Software Vendors

Barclaycard requires merchants to notify them of the third parties they use that store, process or transmit cardholder data.

1.5.2 Maestro mandate – compulsory changes to the way you accept Maestro card payment

What is the Maestro mandate?

An industry-wide Maestro mandate came into force from 1st July 2007, requiring compulsory changes to the way Maestro cards are accepted. All of your businesses which accept Maestro as a form of payment are impacted by this mandatory change. It is important for you to ensure that all businesses under your control are aware of the requirements. If you do not comply with these mandatory changes, you may be liable to Card Scheme fines.

The compulsory changes

Unless otherwise informed in writing by your Acquirer, from 1st July 2007 if you want to continue accepting Maestro as payment you must:

- Remove all Switch branding from all points of sale and replace with Maestro logos. The 'What must you do to comply with the Maestro mandate' section tells you where you can get the new logos from
- Recognise and accept all Maestro cards – UK and international
- Implement SecureCode for all Maestro e-commerce transactions. This will help your business to defend against rising online fraud and to avoid potential card scheme fines of up to $25,000 US per month.

Whether or not you are already using Authentication for Visa or MasterCard, to avoid potential scheme non-compliance fines, it is important that you make the Maestro developments listed in the 'What must you do to comply with the Maestro mandate' section.

Why is it important to be compliant?

- To allow your business to maximise income by accepting a wider range of cards
- To make all your online transactions even more secure, reducing fraud losses and providing additional confidence to your customers
- To help you avoid heavy scheme fines of up to $25,000 per month being issued.

What must you do to comply with the Maestro mandate?

The Maestro mandate sets out a number of requirements which you must comply with when accepting Maestro card payments. It is important that you comply with each of the following requirements:

1. If a third party is used to facilitate e-commerce payments, such as a Payment Service Provider, if you have not done so already, you must contact them immediately and instruct them to:

- Extend the use of or implement SecureCode to cover Maestro e-commerce transactions
- Remove any Switch logos from your point of sale and web payment pages and replace them with the Maestro logo. The Maestro logo can be downloaded from the Information Zone at **www.barclaycard.co.uk/paymentacceptance**

2. If your business hosts their own internet service or front pages for accepting card payments, you will need to make the above technical and branding changes listed in point 1 yourself. As normal, once you have completed the changes, your solution will need an updated accreditation from Barclaycard.

1.5.3 If you fail to comply with PCI DSS or the Maestro mandate

If you fail to comply with PCI DSS or the Maestro mandate, or any of the obligations as set out in section 1 of the Operating Instructions and Procedures guide, you will be in breach of your Agreement with us and:

- we have the right to recover any penalties, fees or fines imposed by any Card Scheme in accordance with our Agreement with you (of which this Operating Instructions and Procedures guide forms part); and/or
- this will be considered a material breach of your Agreement and we may exercise all rights at our disposal in accordance with our Agreement with you;
- we may suspend your Acquiring facilities until such time as you can prove compliance with PCI DSS or the Maestro mandate to our reasonable satisfaction.

1.6 Protecting cardholder information

In addition to complying with PCI DSS in accordance with Section 1.5.1 above, you must comply with the following requirements to safeguard cardholder information.

1.6.1 Thermal paper

If you are using thermal paper to process transactions, extra care is needed when storing transaction copies to ensure they do not fade.

- Do not store in direct sunlight. Wrap transaction copies in paper or store in brown envelopes
- Do not store close to heaters
- Store in a cool, dark and dry environment
- Maintain an even temperature and humidity. Ideally these are a temperature of 20-23 degrees and a relative humidity of 45-55 per cent. Do not store in PVC wallets.

For a supply of our pre-paid envelopes, call our Customer Services Department on **0844 811 6666**.*

1.6.2 Storing your records

Original retailer copies of transactions must be retained in an accessible place for a minimum period of 6 months. We also advise you to keep copies of transactions for a further 12 months from that date, although this can be on microfilm or similar media. In the event that a cardholder disputes a transaction, or another query arises, you may be required to provide the necessary documentation. This can happen up to 6 years after the date of the transaction.

If we need to send a retrieval request we will give you the cardholder's name wherever possible. However, the Card Issuer does not have to give us this information so we may be unable to tell you. Transactions should therefore be stored by card number or transaction date and not by cardholder name. It is important that all copy vouchers and till rolls are kept in a secure place, to prevent any fraudulent use of the information.

2. accepting card payments

2.1 Card-present transactions

2.1.1 Installation

Most PDQ terminals are easily installed by our customers, who then follow simple instructions to activate the system. However, our Customer Services Department will be able to help you in the unlikely event of any queries. Please call **0844 811 6666**.*

2.1.2 Insurance

The value of each Barclaycard PDQ terminal is approximately £400 and it is your responsibility to meet the costs of any necessary repair work unless the fault is of a technical nature which has not been caused by you or your employees. It is your responsibility to insure the PDQ terminal(s) under your business policy, with cover for accidental damage, fire and loss.

2.1.3 Care of your bank-owned PDQ terminal(s)

The information in the Operating guide supplied with your PDQ terminal should be followed by all members of your staff. It is important to look after your PDQ terminal(s). Please ensure that liquids, including cleaning agents and water, are not spilt on the PDQ terminal. This could cause damage and, as a result, you would not be able to use your PDQ terminal until it has been repaired. This may also have an adverse impact on your business.

2.1.4 Using your own or third party-supplied terminal

Whilst you may use your own terminal or one supplied by a third party, you are responsible for maintaining the terminal and ensuring all transaction receipts produced are clear and legible.

Please remember to change your till rolls when they are running low as we may sometimes need you to supply a clear and legible copy of the transaction receipt. If you are unable to do so, this may result in a transaction being charged back to you. Please refer to Storing your records (Section 1.6.2) for further information. When photocopies of the vouchers are taken that have the red reminder strip present, they are often illegible.

2.1.5 Using your point of sale terminal

This section is relevant if you are using a PDQ terminal, your own terminal, or one supplied by a third party supplier.

1. Follow the procedure set out in your PDQ terminal Operating guide.

2. If the card carries a chip and you are using a chip-enabled terminal you will be able to process the transaction via the chip card reader. If the terminal rejects a chip card, please take extra care when dealing with the transaction (refer to Section 1.4.1.5). If the terminal is unable to read the chip, you may process the transaction by swiping the magnetic stripe through your terminal and ensuring Authorisation is obtained. If Authorisation is declined, do not proceed with the transaction, ask for an alternative method of payment. Do not key-enter the card details.

3. If the card does not carry a chip or your terminal is not a chip-enabled terminal, you will need to swipe the card through the terminal magnetic stripe reader. As an additional security check, the terminal may prompt you to key in the last 4 digits of the embossed card number. Please note that if you are not using a chip-enabled terminal and the card has a chip, you will be liable for any subsequent chargeback should the transaction later turn out to be fraudulent (refer to Section 4 of this guide).

4. Ensure that the card is valid and in date by referring to the recognition guide in Section 1.1 of this guide. Remember to rub your thumb over the signature strip (it should be smooth and flush with the surface of the card) and also check that no part of the card has been damaged or tampered with.

5. If you have an online terminal, your terminal will automatically go online and obtain an Authorisation code. If you have an offline terminal, your terminal will automatically check the Hot Card Warning Notice. For retailer-owned terminals, you may need to check the Hot Card Warning Notice manually. Please refer to your terminal user instructions.

6. If the cardholder is instructed to sign the transaction receipt, check that the cardholder's signature matches that shown on the back of the card. If the cardholder is requested to enter a PIN, ensure that they enter a PIN without hesitation.

7. Check that the cardholder number printed on the receipt matches the number embossed on the front of the card. If it does not, you must ring Authorisation and say, "I have a card number mismatch." If you are unable to speak freely, just say, "I have a Code 10 call."

8. Check that the spelling of the signature (if legible) corresponds with that of the name embossed on the card and that the title of the cardholder matches the presenter (if it appears on the card). If a title is shown on the card, ensure that the presenter of the card matches the title eg if 'Mr' is printed, ensure the presenter is male.

9. When you have completed the transaction, hand the goods to the customer together with the cardholder's copy of the receipt and the card.

10. You must retain original copies of all transactions for a minimum of 6 months. Please refer to Section 1.6.2 for further advice and guidance.

11. All unembossed Visa Electron, VPay, Mastercard and Maestro (issued outside the UK) transactions must be processed electronically and must be authorised. In the event of terminal failure, or if the card reader does not read the required details, return the card to the customer and ask for an alternative method of payment.

12. Remember that an Electron card number must never be key-entered for a sale transaction.

2.1.6 Contactless transactions
2.1.6.1 What is a contactless transaction?

A contactless transaction is a transaction that is processed utilising wireless technology, where the payment instructions are securely exchanged between a chip card and a specially adapted card point of sale terminal. The value of any single transaction is limited to a certain amount (currently £10 – as at April 2009). Any change in this amount would be communicated separately.

2.1.6.2 Accepting contactless card payments

Sales – a single contactless transaction is permitted only for an amount under a predefined limit (as at April 2009, set to £10). Any change in this amount will be communicated to you.

Refunds – these are prohibited. All refunds should be undertaken as chip and PIN transactions.

Fallback transactions – any transaction unable to be processed as a contactless transaction should be processed as a normal contact transaction (ie chip and PIN).

Fall up transactions – as part of security measures, on a periodic basis a contactless transaction may be requested to be processed as a chip and PIN transaction. This is to ensure that the correct user is in possession of the correct card.

Receipts – cardholder copies of receipts are optional. Barclaycard contactless terminals have been configured not to print a copy of the receipt. For further information please refer to your Terminal Operating guide.

2.1.7 Manual entry for card-present transactions (card swipe failure)

Please remember: You cannot carry out manual key entry for Visa Electron and Maestro (issued outside the UK) transactions.

Please follow the Operating guide for your terminal for full instructions on how to process a transaction if a chip card fails to read or a magnetic stripe card fails to swipe. In addition, please ensure:

- If the card presented for payment has a chip and the chip does not read: You may swipe the magnetic stripe through your terminal. Your terminal will automatically prompt you to confirm that the chip cannot be read and then to go online to seek Authorisation. We strongly recommend that you do not progress with the transaction if Authorisation is not obtained, as we will not be able to defend you if the transaction is charged back at a later date;

- If the card presented for payment has a magnetic stripe and fails to swipe through your terminal, please ensure you follow the procedure as detailed in Card chip-read/swipe failure in Section 1.4.1.5 of this guide. Your copies of the terminal receipt and the voucher should then be stored together in case of future query. The voucher should not be banked, as your bank account will be credited via your terminal.

Please remember: A Code 10 Authorisation call must be obtained for Solo and UK Maestro card transactions in all circumstances where the card fails to be accepted by your electronic terminal.

Manual key entry should also be used when a card fails to chip-read or swipe during a refund transaction.

For all **failed electronic transactions**, you must take an imprint of the card on a verification voucher to prove that the card was present at the time of the transaction. Failure to provide an imprinted voucher at a later date could result in the transaction being charged back to your business. An imprinted voucher, however, does not protect you from a chargeback for UK Maestro and Solo transactions. If a transaction fails to swipe, you should make a Code 10 call as an anti-fraud measure. A record of an approved Code 10 Authorisation will protect you from chargebacks.

2.1.8 Fallback paper voucher processing

Processing transactions using an imprinter

If your terminal is not functioning correctly, or if you have a power or telephone network failure, you may have to use your imprinter as a backup and complete the transaction using a sales voucher. If you rent a PDQ terminal from us, you must report all faults to our Customer Services Department on **0844 811 6666**.*

Please remember: An unembossed Visa Electron, VPay, MasterCard and Maestro (issued outside the UK) card transaction can only be processed electronically and must not be taken on paper vouchers.

UK Maestro and Solo transactions can only be processed using an imprinter if the terminal is not functioning correctly. Vouchers should be stored for at least 6 months. Please see Section 1.6.2 for further information.

2.1.8.1 Making a transaction when the customer is present

1. Carry out all normal checks of the card. Please refer to the card recognition section of this guide.
2. Place the card face up on the imprinter.
3. Place the sales voucher, face up, over the card and operate the imprinter.
4. Remove the sales voucher and card from the imprinter.
5. Using a ballpoint pen and writing clearly, please note the following necessary details:
   - the date
   - the amount of each item
   - the transaction total
   - details of what was purchased. Please do not just write 'Goods' as this is not acceptable.

If the customer is using a purchasing card, they may require a customer reference number to be recorded in the relevant boxes on the sales voucher. If you are selling fuel, use the 'For Merchant Use Only' boxes on the sales voucher to record the vehicle registration number.

Please remember: Altered vouchers are not acceptable. If you make a mistake when entering the details of a transaction, you must destroy the incorrect voucher and start again. It is essential that vouchers are not pinned, stapled, folded or damaged as this may cause processing problems.

6. Ask the cardholder to sign the sales voucher in the box indicated. Hold the card and watch while the voucher is being signed. Rub your thumb lightly over the signature strip on the card – it should be smooth and flush with the surface of the card.
7. Check that the signature on the sales voucher matches the signature on the reverse of the card.

8. Check that the spelling of the signature (if legible) corresponds with that of the name embossed on the card and check that the card is in date. If a title is shown on the card, ensure that the presenter of the card matches the title eg if 'Mr' is printed, ensure the presenter is male.
9. Check the signature strip to ensure that no attempt has been made to disguise the original signature.

Please remember: If you are suspicious of the card, the presenter or the circumstances of the transaction, you must follow the Code 10 procedure.

10. You must seek voice Authorisation by calling Authorisations on **0844 822 2000**.* You must not split a sale. Split sales are at your own risk and could be charged back if disputed. Please refer to Section 3.2.3 for further information on split sales.
11. You will be prompted for the following information when calling for Authorisation:
    - your outlet number
    - transaction type – you should say "Standard Authorisation"
    - the card number embossed on the customer's card
    - the expiry date of the card
    - the issue number if applicable (UK Maestro and Solo cards only)
    - the amount of the transaction (whole pounds only).
12. If the transaction is authorised, you will be given an Authorisation code by a voice response service, which may include numbers and letters. Write the code in the appropriate box on the sales voucher. Detach the cardholder copy of the sales voucher and hand it to the customer with their card and goods.
13. If the request is refused, no reason will be given and you should return the card to the customer – unless instructed otherwise by the operator – and ask for payment by other means.
14. If the transaction is referred to an operator, you should follow their instructions. Be prepared – the operator may in fact wish to speak to the cardholder.
15. Once the procedure has been completed to your satisfaction and all the required checks have been carried out, you must ensure that the necessary details of the transaction have been clearly recorded on all copies of the sales voucher. You should then detach the cardholder copy of the voucher and hand it to the customer with his or her card and their goods.
16. Key in the transaction when your terminal is working again. Take care when keying the card details to ensure that they are correct. If at a later date, the transaction is charged back due to invalid details being input, your company may be debited with a chargeback.
17. If the transaction is accepted, file the sales voucher in case of a subsequent dispute. Do not bank the voucher as your bank account will be credited via your terminal.

18. If, when key-entering the transaction, you receive a 'Declined Authorisation' message, bank the sales voucher for processing. Refer to Sales and refund vouchers, Section 3.1.2. Transactions may be honoured as long as you have obtained Authorisation where required (ie at the time the transaction was undertaken with the cardholder present, followed all the procedures correctly and reported the fault to us, so that it shows on our log reports).

19. Pay the vouchers into your bank account within 2 days (refer to Sales and refund vouchers, Section 3.1.2).

2.1.9 Authorisation and Code 10 calls

2.1.9.1 Definition of Authorisation

When you seek Authorisation for a card payment, we check with the Card Issuer whether they will approve payment. **Authorisation from the Card Issuer is not a guarantee of payment** nor does it confirm that the person who presents the card is the genuine cardholder. The Card Issuer can charge the card payment back to you even if it has been authorised – particularly where the correct procedures have not been followed.

If you are undertaking a transaction where the cardholder is not present, our Authorisation Department is unable to check whether the presenter of the card is the genuine cardholder or not.

2.1.9.2 Referrals

On occasions, when processing transactions, the card issuing company may generate a referral and you will be prompted by your terminal to call for Authorisation.

A referral occurs when the Card Issuer requests Barclaycard to contact them before releasing a decision. Examples of why referrals are generated are an unusual pattern of spending, or a large transaction value which has triggered the fraud detection methods which are in operation. Our aim is to process the referral in a quick and efficient manner to minimise the time spent processing the transaction.

On most occasions we will ask you to put the cardholder on the phone. Simply follow our customer service advisor's instructions, and once we have spoken to the presenter of the card and the Card Issuer, we will give you a decision.

2.1.9.3 Automated Authorisation System

Our Authorisation department operates an automated Authorisation facility, which is designed to speed up your transaction processing by answering your call within one ring, avoiding unnecessary delays at your point of sale.

The system is easy to use and offers you straightforward menu options to ensure your calls are processed correctly. The system incorporates voice recognition and touch tone technology, to allow you to input the information in the way that suits you best. To allow you to speed up your transaction processing, the system incorporates a barge-in facility. For example, you can wait for the system to ask for the 'transaction type' and respond with 'mail order'.

You do not have to wait for the system to list the available options if you know what your input will be.

If the system has not understood your input, you will be asked to repeat your information. If you continue to experience difficulties, your call will be routed to a customer service advisor who will handle your enquiry.

When the system has captured all the transaction data, you will be advised of the decision. If the transaction is a referral, your call, along with the transaction data, will be transferred to a customer service advisor.

Please ensure you have the following information to hand before calling:

- your outlet number
- card number
- expiry date
- amount
- issue number (if applicable).

2.1.9.4 Code 10 calls for card-present transactions

- If you or your staff are in any way suspicious of a card, its presenter or the circumstances surrounding a transaction, you must call Authorisation on **0844 822 2000***
- You will be prompted for your Merchant number and then for the transaction type. If you are suspicious and unable to speak freely, you will be given the option to say, "This is a Code 10 call" or press 9 to avoid possible confrontation
- You will be asked for the card number, followed by the expiry date and the issue number (if applicable) and will be given options to choose from depending on the type of call you are making
- After this, you will be connected to an operator who will ask a series of questions which require a yes or no answer
- Remember to keep the card and the goods out of reach of the customer
- Activate any surveillance equipment you may have
- If the operator asks you to keep the card, inform the customer politely, again without putting others or yourself at risk.

Please note: Code 10 is only available for card-present transactions where we may ask to speak to the cardholder. It is not available for transactions where the cardholder is not present such as mail, telephone and internet transactions. In such circumstances we are unable to guarantee that the person undertaking the transaction is the genuine cardholder.

2.2 Card-not-present transactions (terminal or ePDQ-Lite)

2.2.1 Definition of card-not-present

A card-not-present transaction is when the card is not at the point of sale. Mail order, telephone order, internet and recurring transactions are examples of card-not-present transactions. You must advise Barclaycard if the majority of your transactions are card-not-present.

Please note: International Maestro cards cannot be accepted for mail or telephone orders.

Please note: Card-not-present transactions are prone to fraud and therefore may be charged back to your business if at a later date the genuine cardholder denies participating in the transaction. You are not obliged to accept card-not-present transactions, but in doing so you must accept the risks involved. Barclaycard will be unable to defend you from disputed card-not-present transactions, refer to Preventing and detecting fraudulent card-not-present orders (Section 1.4.2).

2.2.2 Advertising

If you advertise the availability of mail, telephone or internet ordering services, your advertising should comply with the requirements of the British Codes of Advertising and Sales Promotion. Contact the Committee of Advertising Practice Copy Advisory Team by calling **0207 580 4100** or by fax on **0207 580 4072** for further information, or visit **www.cap.org.uk**

2.2.3 Processing card-not-present orders

For a card-not-present transaction to be processed you must obtain the following details:

- the card number
- the card expiry date
- Card Security Code
- the cardholder's full name and address, as held by the Card Issuer, including the postcode and telephone number
- the gross amount (including postage and packaging) of the transaction
- for UK Maestro or Solo cards, issue number or start date*
- for mail orders, the signature
- for telephone orders, an immediate written record of all the above including date/time of conversation
- for mail and telephone orders, the delivery address and name of the recipient if different from that of the cardholder
- the customer reference number (if quoted) for a Visa purchasing card transaction.
- **Authorisation does not guarantee payment**. It merely confirms that there are sufficient funds available on the account and that the card has not been reported lost or stolen. We are unable to guarantee that the person presenting the card details is the genuine cardholder

- There are increased risks of chargebacks for card-not-present transactions, because the customer and card are not present
- You must not release goods to a third party or anyone claiming to have been sent by the cardholder (eg a taxi driver) to collect the goods
- Where a cardholder places a mail or telephone order and collects the goods later, you should cancel the card-not-present transaction and perform a new card-present transaction. Ensure you also carry out the full card-present procedures. Refer to Using your own or third party-supplied terminal (Section 2.1.4)
- Beware of unusual one-off high-value transactions, especially if you do not normally operate in this manner.

Then follow the procedures set out in your Terminal Operating guide.

*Please remember: Some UK Maestro and Solo cards do not carry an issue number. If they do not, take details of the start date when making a transaction.

2.2.4 Pre-authorisation

Visa and MasterCard permit Pre-authorisation for hotel, car rental, internet and mail order/telephone order retailers only. Please refer to Section 5 for details of how and when you can perform Pre-authorisation for car rental and hotel accommodation bookings.

2.2.5 Visa authorisation rules for MOTO and internet

For goods to be shipped, a mail/telephone order or an Electronic Commerce Merchant may obtain Authorisation on any day up to 7 calendar days prior to the transaction date. The transaction date is the date the merchandise is shipped. This Authorisation is valid if the transaction amount is within 15% of the authorised amount, provided that the additional amount represents shipping costs.

2.2.6 MasterCard authorisation rules for MOTO and internet

For goods to be shipped, a mail order or Electronic Commerce Merchant should obtain Authorisation on the day the cardholder contacts them to place the order. When the goods/services are ready to be delivered, they should process the transaction. This should not be for more than the original Authorisation amount.

The date the merchant ships the goods or renders the service is considered the transaction date. Solo and Maestro do not allow Pre-authorisation for MOTO, internet, hotels or car rental transactions.

If shipping goods more than 7 days after the original authorisation request, we recommend you obtain a second authorisation. When presenting the transaction for processing please quote the original authorisation code, but keep the second one for dispute resolution purposes.

2.2.7 Recurring transactions

A recurring transaction is one for which a cardholder grants permission, through writing or electronically, to a merchant to periodically bill their account for recurring goods or services delivered over a period of time (not to exceed one year between transactions). Examples of this are vehicle recovery services, insurance, memberships and subscriptions.

If you wish to accept this type of transaction, please contact our Sales Centre on **0800 61 61 61*** quoting your existing outlet or chain number. We may allocate you an additional outlet number and will advise you of the procedures you will need to follow. However, please remember that this type of transaction must not be undertaken with UK Maestro, Maestro or Solo cards.

2.2.8 What about chargebacks?

In the event of a dispute involving a card-not-present transaction we will do all we can to prevent the transaction being debited back to you (known as a 'chargeback'). A chargeback usually occurs when a cardholder disputes a transaction shown on their statement or you process a transaction outside the terms of your Merchant Agreement. The cardholder may claim that the goods were never received or were defective, or that the card number had been used fraudulently. It is your responsibility to investigate the matter and recover the goods or the payment by some other means. Please refer to Chargebacks and retrieval requests (Section 4).

Barclaycard has a dedicated Chargeback Education Team that can provide you with bespoke advice on the steps you can take to reduce the risk of transactions being charged back. If you wish to receive free advice, please contact our dedicated team on **01604 614012**.*

2.2.9 Telephone orders

- Please keep a record of the cardholder's name and address in case of any future query
- It is your responsibility to check the card upon collection or delivery. You should make sure that the card number and the expiry date quoted agree with the card presented
- It is also your responsibility to obtain a signature and ensure the signature on the card matches that obtained from your customer
- If an order is to be collected, you must cancel the original transaction and start a new one as a card-present transaction. Refer to the card-not-present procedures and how to minimise chargebacks in Section 1.4.2.

Please remember: A customer must still be supplied with a transaction receipt. We recommend that the cardholder copy must display only the last four digits of the card number. For MasterCard transactions the expiry date must not be quoted.

2.2.10 Barclaycard Hotel Tracker

Barclaycard Hotel Tracker is a Visa corporate charge card account where no plastic cards are issued. As such the booking agent will not be able to provide photocopies of the front and back of the card. It has been developed as a simple payment method for companies who are booking and paying for hotel accommodation on behalf of their employees, particularly where companies do not provide individuals with their own company card. It removes the need for hotels to operate manual invoicing/bill back procedures and provides swift payment to the hotel on guest departure. The Visa card number quoted in the reservation should be charged by carrying out a card-not-present transaction. The booking agent stores the Barclaycard Hotel Tracker account details in an audited approved computer system which means that the card details are totally secure and are only revealed to the hotel/property that has been instructed to charge them. On check-out the Visa account is charged and the management information and transactional charges are combined and sent to the customer to create a detailed monthly statement.

2.3 Internet transactions

2.3.1 E-commerce

Our ePDQ service provides quick and secure transaction processing. Your customers simply browse your website, select their order(s) and enter their card details as directed.

2.3.2 Options

ePDQ Cardholder Payment Interface (CPI) is our end-to-end solution for accepting card payments online. A world-class, secure service for card payment Authorisation and settlement that lets you trade online, fast, easily and safely. It's flexible, reliable and straightforward to integrate.

If you prefer to control the whole card capture process and host your own payment pages, opt for our ePDQ Merchant Payment Interface (MPI). You can integrate the MPI, which enables you to take full responsibility for collecting cardholder details and allows your website to communicate with our ePDQ payment engine.

2.3.3 e-PDQ

ePDQ is a secure online service from Barclaycard for card payment Authorisation and settlement. It enables you to accept and process card transactions from your website 24 hours a day, 365 days a year. Please contact our Sales Centre on **0800 61 61 61*** or visit **www.barclaycard.co.uk/paymentacceptance** for further information. When you use the ePDQ CPI you can rely on us to meet and maintain all security and transaction processing software standards, including full compliance with the new Payment Card Industry Data Security Standard (PCI DSS).

If you choose not to use a Barclays-owned submission product, you must correctly flag every transaction by using the correct level of APACS software. You must maintain the level of software in accordance with APACS standards. If you fail to adhere to this condition, you will be liable for any Card Scheme fines or penalties, which may result from non-compliance.

2.3.4 Requirements for merchants not using the ePDQ CPI

Security and custody of card data

You must adopt minimum security measures before processing card transactions from an internet site.

These requirements apply regardless of whether the site is:

- maintained solely by our merchant customer
- maintained solely by a third party provider, which is receiving and processing card payment transactions on behalf of our merchant customer
- a combination of the two above.

Minimum security measures

1. All transactions containing card information should be transmitted over the internet in an encrypted form using either:

   - the Secure Socket Layer (SSL) protocol, currently with a minimum effective symmetric key length of 128 bits

   or

   - a protocol employing similar encryption algorithms and key lengths which provide similar or greater strength to SSL.

Measures should be adopted not only when the transaction details are being passed from the cardholder to the web-server, but also from the web-server to the merchant if this takes place directly over the internet.

2. Any servers involved in processing transactions containing card information and originating from the internet should not be exposed directly to the internet.

   - These servers should be placed in a secure domain by means of internal network partitioning with connectivity to the internet protected by firewall technology.

3. Additional internal network partitioning should be provided:

   - between the server(s) involved in processing transactions containing card information and connectivity to the Barclaycard host, where automated settlement and/or Authorisation transactions are to be generated.

You are responsible for protecting card data and may be liable for card scheme fines or penalties which result from breach of your security.

2.3.5 Internet Payment Service Providers (PSPs)

We can accept your internet card payments from a recognised third party Payment Service Provider (PSP). However, you must ensure that the PSP meets the minimum security measures detailed in this procedure guide and that they can offer the necessary communication links to Barclaycard. It is important to stress that you have the responsibility for complying with the Internet Merchant Procedures within this procedure guide for internet card payment transaction acceptance as Barclaycard will not enter into any contract with the PSP on your behalf.

2.3.6 Modulus 10 Check

The payment page should be designed to incorporate a Modulus 10 Check Digit Algorithm for verifying the card number. To obtain copies of the Modulus 10 Check Digit Algorithm, card scheme or Barclaycard logos, via the business online section of our website at **www.barclaycard.co.uk/paymentacceptance**

2.3.7 Website information

Your website must contain the following details:

- your company name, address, telephone number, fax number and email address
- your company registration number and VAT number (where applicable)
- a complete description and price of all goods and services, clearly stated, including all additional costs such as taxes, delivery costs and export restrictions
- Your purchase terms and conditions, displayed 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
- clear information on your company's delivery, refund and cancellation policies
- A 'click to accept' button, or other acknowledgement, evidencing that the cardholder has accepted the delivery, refund and cancellation policies
- a statement to describe the type of transaction security that is supported
- a privacy statement
- transaction currency
- disclosure of the merchant outlet country at the time of presenting payment options to the cardholder
- the scheme logos of the cards you accept
- your delivery policy
- export restrictions.

The Barclaycard name and logo may not be displayed on your internet site without prior registration and agreement from us.

2.3.8 Transaction receipts

Your customers must be supplied with a transaction receipt as part of an order confirmation notice at the time of the purchase. The receipt must include:

- an instruction to print or keep the receipt for any future query
- your company name, address and telephone number to enable customer contact
- your website address
- the total cost of the purchase and the currency
- transaction date and type (sale or refund)
- a unique transaction order reference number
- the name of the purchaser
- the Authorisation code
- a complete description of all goods and services purchased
- clear information on Terms and Conditions, cancellation, return and refund policy (if restricted)
- exact date any free trial period ends, if offered.

Please remember: The receipt must only include the last four digits and not the full card number. For MasterCard transactions the expiry date must not be quoted.

3. general procedures and banking

3.1 Everyday procedures

3.1.1 Banking procedures

Please ensure that you follow the end-of-day banking procedure (as detailed in your Terminal Operating guide) to ensure you receive payment for all transactions. It is essential that all transactions are submitted for payment within 2 working days of being accepted. Please note that if a transaction is submitted after 2 working days, the card issuer may reject the transaction resulting in it being charged back. Barclaycard will be unable to defend you from such chargebacks.

If your terminal is not working, please ensure that you follow the procedure in Section 2.1.7 in order to receive payment. To bank any voucher that cannot be processed by your terminal, please follow the procedures below:

- Complete the three-part Merchant Voucher Summary (MVS) before handing the bank copy of your sales and refund vouchers into any branch of Barclays Bank

- Each batch of vouchers must be accompanied by part three (the white copy) of the completed MVS. No more than 20 vouchers should accompany each MVS.

3.1.2 Sales and refund vouchers

In the event of your terminal not working, please ensure you follow the procedure in Section 2.1.7.

These vouchers provide 3 copies of the sale or refund details, one for your own use, one for the bank to process and one for the cardholder.

- **Merchant copy** – The top copy of the completed sales or refund voucher is your record of the transaction

- **Bank processing copy** – The middle copy of the sales or refund voucher should be handed in to your local branch of Barclays Bank. Vouchers should be handed in on the day of the transaction and no more than 2 banking days afterwards

- **Cardholder copy** – The bottom copy must be given to the cardholder for his or her records or, in the case of a mail or telephone order, it must be posted to the cardholder.

3.1.3 Completing your Merchant Voucher Summary (MVS)

- Write your Merchant name and number (this is normally shown on the top line of your imprinter plate) clearly on the MVS, with the paying-in date

- List the value of each sales voucher and refund voucher on the reverse of the MVS in the boxes indicated

- Write the total of each column in the boxes at the bottom

- Write the total number and value of both sales vouchers and refund vouchers on the front of the MVS

- If possible, vouchers should be deposited on the day of the transaction and no more than 2 banking days afterwards

- Any queries about the credit to your bank account should be made by calling our Customer Services Department on **0844 811 6666**.*

3.1.4 Posting vouchers

If you are located in a remote area and are unable to get to a branch of Barclays Bank, you may post your vouchers to us for processing. The MVS bank processing copies of your sales and refund vouchers should be sent to:

Barclaycard Financial Exceptions, Dept FX, Barclaycard House, 1234 Pavilion Drive, Brackmills, Northampton NN4 7SG.

For a supply of our pre-paid envelopes, call our Customer Services Department on **0844 811 6666**.*

3.1.5 Monthly statements

3.1.5.1 Understanding your monthly statement

Your Merchant invoice/statement explains the status of your account, including transactions, other charges where applicable, and the total amount due.

barclaycard

Registered in London, England, Reg No 1026167
Reg. Office: 1 Churchill Place, London E14 5HP

MERCHANT INVOICE/STATEMENT
Barclaycard Payment services (Dept CSD) Northampton NN4 7SG
If you have any queries please call Customer Services
Department 0844 811 6666

			Outlet No.	Invoice No.	Account
Period	Sample Name PLC Sample Street Sample Town Sampleshire ZZ9 1AA				
				VAT Reg. No.	Tax Point

INVOICE THIS PERIOD		Charge £	VAT £	Total £
£189.80	42 Visa Credit	4.75		
£190.70	39 Visa Premium Credit & All Others	4.76		
£7758.46	1717 MasterCard Credit	170.69		
£5522.00	1522 Mastercard Premium Credit & All Others	121.84		
£80.80	11 JCB	1.78		
£2807.00	455 UK Visa Delta	113.75		
£3244.00	375 UK Visa Electron	93.75		
£245.50	56 International Visa Debit	5.40		
£1245	96 UK MasterCard Debit	27.39		
£100.40	3 International MasterCard Debit	2.20		
£8986.00	11025 UK Maestro	256.25		
£5348.00	876 UK Solo	219.00		
£567.00	42 International Maestro	10.50		
£326.70	14 Visa Commercial	8.16		
£845.65	26 MasterCard Commercial	18.60		
£350.75 cr	12 Refund Transactions	6.00		
£37807.76	**Sub Total**	1064.82		1064.82

Other Charges
(Standard Rate VAT 17.5%)

1 epdq Management fee		25.00		
1 pdq Classic contactless		10.00		
	Sub Total	35.00	6.12	41.12
	INVOICE TOTAL	1099.82	6.12	1105.94

STATEMENT OF ACCOUNT

Balance brought forward from last period		31.38
Payment – Thank You		31.38 cr
Invoice Total (from above)		1105.94
TOTAL AMOUNT DUE		**1105.94**

This amount will be debited to:
Bank Account 11-11-11 12345678 on or after 01 January 2008

Pre Pay Details

£80.00	cr	4	Pre Pay T-Mobile @ 3.45%	2.76 cr
£60.00	cr	4	Pre Pay Orange @ 3.45%	2.07 cr
£50.00	cr	4	Pre Pay O2 @ 3.45%	1.72 cr
£30.00	cr	4	Pre Pay Vodafone @ 3.45%	1.03 cr
£30.00	cr	4	Pre Pay Virgin Mobile @ 3.45%	1.03 cr
£250.00			**Total 1**	**4.67 cr**

Summary of your credit/debit card transaction details listed for all outlets

Summary of your account

Summary of your E-Top Up commission earned

Your E-Top Up commission inclusive of VAT

barclaycard

Registered in London, England, Reg No 1026167
Reg. Office: 1 Churchill Place, London E14 5HP

SERVICE CHARGE DETAIL ADVICE
This is not a VAT Invoice
Barclaycard (Dept CSD) Northampton NN4 7SG
If you have any queries call Customer Services
Department 0870 600 600
8.00-20.00 Mon/Sat or 08.00 – 18.00 Sun.
Please quote your Chain No.

Sample Name PLC
Sample Street
Sample Town
Sampleshire
ZZ9 1AA

		Your Ref	VAT Reg No.	Tax Point
LONDON	Charge £	VAT £	Total £	
Ref: 1234567 020				
Transaction Charges				
(Vat Exempt)				
£95.00	12 JCB @ 3%	2.85		
£95.00	12 MasterCard Credit @ 2.75%	2.61		
£95.00	12 Visa Credit @ 2.75%	2.61		
£285.00	Sub Total	**8.07**		8.07
Commission				
(Commission Rates Shown net of VAT 17.5%)				
£50.00 cr 2	Pre Pay T-Mobile @ 5%	2.50 cr		
£10.00 cr 2	Pre Pay Orange @ 5%	0.50 cr		
£30.00 cr 2	Pre Pay O2 @ 5%	1.50 cr		
£20.00 cr 2	Pre Pay Vodafone @ 5%	1.00 cr		
£20.00 cr 2	Virgin Mobile @ 5%	1.00 cr		
	Sub Total	6.50 cr	1.13 cr	7.63 cr
	OUTLET TOTAL	1.57	1.13 cr	0.44
MILTON KEYNES				
Ref: 2223333 010				
Transaction Charges				
(VAT Exempt)				
£95.00	12 JCB @ 3%	2.85		
£95.00	12 MasterCard Credit @ 2.75%	2.61		
£95.00	12 Visa Credit @ 2.75 %	2.61		
£285.00	Sub Total	**8.07**		8.07
Commission				
(Commission Rates Shown net of VAT 17.5%)				
£30.00 cr 2	Pre Pay T-Mobile @ 5%	1.50 cr		
£50.00 cr 2	Pre Pay Orange @ 5%	2.50 cr		
£20.00 cr 2	Pre Pay O2 @ 5%	1.00 cr		
£10.00 cr 2	Pre Pay Vodafone @ 5%	0.50 cr		
£10.00 cr 2	Virgin Mobile @ 5%	0.50 cr		
	Sub Total	6.00 cr	1.05 cr	7.05
	OUTLET TOTAL	2.07		1.02

This figure is the credit/debit card transaction charges less the E-Top Up commission earned

Total VAT payable on E-Top Up commission listed by outlet

3.1.5.2 What you will receive

If you have requested statements to be sent to your head office, your outlets will usually receive nothing. Your head office will receive:

- Merchant invoice/statement
- Transaction payment advice
- Service charge detail advice.

If you are a single outlet, or you have requested that we send separate statements to each outlet, you will receive:

- Merchant invoice/statement
- Transaction payment advice.

3.1.5.3 Queries

If you have a query about a Merchant invoice/statement you have received, please contact our Customer Services Department on **0844 811 6666**,* quoting your Outlet or Chain Head Office number. Remember to check that all transactions have been processed and show on both your Merchant and bank statements. You are required to reconcile your monthly Service charge statement against your bank statement on a regular basis. If you do not do this, you may be liable for subsequent chargebacks for late presentation of transactions.

Any queries should be directed to our Customer Services Department on **0844 811 6666**.*

3.1.5.4 Merchant invoice/statement

This is both a VAT invoice and a statement. Each page number and the total number of pages are shown in the top right-hand corner. There are 3 main headings:

- Transactions and other charges where applicable
- Statement of account (including any adjustments)
- Total amount due.

3.1.5.5 Transaction payment advice

Provides itemised details of payments made to you with the dates the transactions were processed by us and the payment reference.

3.1.5.6 Periodic settlement

If you have chosen to be paid periodically (for example weekly, or twice weekly) please remember that the figure, Total payments this period, may not agree with the transaction charges on page 1 of your statement, as they cover different accounting periods. Payment for any dates not showing will appear on your next statement.

3.1.5.7 Service charge detail advice

This shows a breakdown of the invoice for each outlet and includes customer reference. PDQ terminal rental charges are shown, detailing the number of PDQ terminals per outlet and the total charge. This page will only be sent to chain head offices.

3.2 Exceptional procedures
3.2.1 Can I pass charges to my customer?

In the United Kingdom, you are entitled to add a surcharge to any transaction made by card. However, if you decide to do so, there are several procedures you must follow and a number of legal requirements that apply. These are the Payment Services Regulations 2009 and the Price Indications (Method of Payment) Regulations 1991 (if you sell motor spirit, the relevant regulations are contained in the Price Marking (Petrol) (Amendment) Order 1991). Breach of some of these requirements is an offence. (Please note if you accept payments outside the United Kingdom, other legal requirements may apply. You must check these yourself.)

The combined effects of these requirements are that you must make certain that your customers are informed of any surcharges before the initiation of the transaction.

- *For all payments*, you must ensure that your advertising makes clear that any prices you state are for payments other than by card.

- *For all payments made in store or by phone*, you must inform the customer the amount of the charge before he or she authorises the card payment.

- *For payments in store*, you must clearly display information regarding your surcharges at the entrance to your premises and, at the point of payment, display how much extra you charge for payment by card.

- *For payments made by mail, telephone or online*, you must display information regarding your surcharges in your catalogues, advertisements and the order form itself.

Copies of the Payment Services Regulations 2009, the Price Indications (Method of Payment) Regulations 1991 and the Price Marking (Petrol) (Amendment) Order 1991 and other applicable regulations are not available from Barclaycard Business. Please contact your local Trading Standards Office or equivalent body if you need further information.

In other countries, you must charge the customer the same price as if he or she were paying cash unless you are accepting Cards in any country where you are entitled to charge customers for using a Card under national legislation. You must comply with any relevant legal requirements limiting the amount you can charge and what you must tell customers about the charge. It is your responsibility to check these requirements yourself.

3.2.2 Minimum charging

You may not set any minimum limit on credit and debit card transactions – purchases by card must be treated in exactly the same way as cash purchases.

3.2.3 Split sales

Sometimes, a cardholder will ask to split the payment of a purchase between several cards, or between a card and cash or a cheque.

It is important that you follow the instructions below to ensure you understand when you can and when you cannot split a transaction as instructions vary by each possible scenario.

1. If several cardholders request you split a transaction amount into smaller amounts in order that they all pay a proportion of a bill, this is permitted. For example, in a group booking in a restaurant, each person requests to pay either their own bill or a proportion of the total bill: you are permitted to split the total bill between each cardholder. To prevent future disputes, always ensure each cardholder agrees the amount they will pay by ensuring that you process separate transactions for each card. Each transaction must be verified by the cardholder's PIN/signature as prompted by your terminal. Please ensure each cardholder receives a copy of the transaction receipt applicable to the agreed amount which may or may not include a gratuity as agreed by the cardholder.

2. If one cardholder asks you to split a transaction amount between several cards (possibly issued by different Card Issuers) you may proceed as follows:

• Only proceed if you are not suspicious of the transaction/presenter of the card

• Ensure each card is issued in the same cardholder name (if the name appears on each card)

• Follow normal card acceptance procedures as detailed in Section 2 of this guide.

This may typically occur when accepting large value transactions where the cardholder may not have sufficient credit available on one card. The cardholder may request to pay part of the total amount by cash and/or cheque. Ensure any cheque payment is also issued in the cardholder's name. We recommend you only permit a cardholder to split a transaction over more than one card when:

• the cardholder and card are present. We strongly recommend you do not split a sale on several cards for any telephone, mail order or internet transaction

• you ensure that each card presented is either issued by a different bank or is a different card type from the same bank. It is unlikely that a cardholder will have more than one card issued by the same bank and be the same card type (eg it is unlikely that a cardholder will have two Visa credit cards issued by Barclaycard but may have a Visa credit card and a Visa debit card issued by Barclays Bank)

• each transaction is processed as either chip-read or magnetic stripe (as per the terminal prompts). Refer to Section 2 on how to accept card payments

• each transaction is verified by PIN or signature (as requested by the terminal)

• each transaction is authorised (regardless of any floor limit you may operate)

• the cardholder clearly agrees to what amount is charged to each card and is given a copy of each transaction receipt that clearly shows what has been charged to each card.

3. Do not split transaction amounts for the same cardholder into smaller amounts eg if Authorisation is declined on a transaction do not split the transaction into smaller amounts in an attempt to get Authorisation. The purchase of more than one item in any one day must be totalled as one amount and Authorisation sought for the total only. If you attempt to split a sale, any transaction may be charged back. Barclaycard will be unable to defend you from such chargebacks.

3.2.4 Double charges

• Please take extra care when a bill is split between your customers

• Ensure that the correct amounts are charged to the appropriate cards to avoid queries at a later date.

3.2.5 Alteration of amounts

• Please do not adjust a transaction amount without the cardholder's consent

• If you have the gratuity facility on your terminal, ensure that the cardholder has signed for any gratuity added to the bill.

3.2.6 Exchanges

• No additional procedure is required if a cardholder exchanges a purchase for goods of the same value

• When the value of the new purchase is less than that of the original, complete a refund transaction for the difference of the cost. Refunds should be processed on the same card as the original sale. If the original card has been lost/stolen the refund can be applied to the new account. For any other type of card closure you must still refund to the card number used in the original transaction.

• When the value of the new purchase exceeds that of the original, complete a sale for the difference in cost, seeking Authorisation even if the amount is below your floor limit.

Please remember: Refunds cannot be made by cash or cheque.

4. chargebacks and retrieval requests

4.1 Retrieval requests

A retrieval request or Request for Information (RFI) is when a cardholder asks for a copy of the transaction details. This is usually because they don't recognise a transaction on their statement or need more details for their records (eg an expenses claim or tax return).

One of the main reasons cardholders ask for a copy of the transaction receipt is because the description shown on their statement does not match the name of your company. So, if you seem to be getting a lot of retrievals, check what is being shown on the cardholder statements. You can change the description by contacting our Customer Services Department on **0844 811 6666.***

It is a requirement of Visa and MasterCard that, if you are predominantly undertaking mail or telephone order transactions, a contact number rather than location should be included within the description: for instance, 'The E Shop, London', should be shown as 'The E Shop, 01207 123 4568'. This encourages people simply to call you to identify their transaction, rather than disputing this with their Card Issuer. Likewise, if you are undertaking internet transactions, you are required to display your internet website address and/or email address on cardholders' statements so that customers can contact you.

As you are simply providing information, there is no loss to your business. However, if you don't supply a clear and legible copy of the transaction within the time requested (usually 14 days), the Card Issuer may charge the transaction back to us. We will then pass the cost on to you in the form of a chargeback.

If a transaction is charged back this will result in you being debited and therefore becomes a loss to your business.

Chargebacks can cause you hassle and cost your business time and money. Following the correct procedures in this guide will help you avoid chargebacks, so you can gain the full sales benefits of accepting payments by card.

4.2 Why chargebacks occur

Chargebacks result when a transaction is deemed invalid – for example, where a cardholder queries a transaction shown on their statement and the Card Issuer, after investigation, agrees to refund the amount. Chargebacks also occur for technical issues such as duplications and no Authorisation.

The most common reasons for chargebacks are:

- a fraudulent mail, telephone or internet transaction. Please refer to Section 1.4.2 for further information and guidance on how to avoid these types of chargebacks
- you did not respond in time to a request for a copy of a transaction (retrieval request)
- the card was not valid when the transaction was made ie the transaction was made before the valid from date or after the expiry date

- you accepted a card payment where the card is subject to a Hot Card Warning Notice/Card Recovery Bulletin and your terminal either did not seek Authorisation or the terminal did not check the card against the Hot Card Warning Notice/Card Recovery Bulletin
- the amount of the sale exceeds your floor limit and Authorisation was not sought, for whatever reason
- the signature on the terminal receipt or sales voucher does not match the signature shown on the card itself
- a transaction was taken on a card that should only be used in an Automated Teller Machine (ATM)
- you accepted a card that should have been verified by the PIN after being initiated by the chip; however, you do not have a terminal capable of undertaking these checks
- if two or more card transactions have been completed for one sale over the floor limit (split sale) and Authorisation was not obtained
- the goods or services provided were defective, not as described, or not received
- a transaction was processed on behalf of a third party who could not process the transaction themselves. This is called laundering and is a breach of your Merchant Agreement.

Since the 1st January 2005, if you take a card-present transaction and your point of sale terminal is not chip and PIN-enabled, you will be liable for any fraudulent transactions and these will be charged back to you. Please note that all Barclaycard contactless terminals are chip and PIN-enabled.

Please remember: You may also receive a chargeback if any of the terms of the Agreement between you and Barclaycard, including any of the instructions in this Procedure guide, have not been followed.

4.3 Responding to retrieval requests and chargeback letters

- Please ensure we receive a reply by the date quoted, either by fax or by post, as not responding within these timescales will usually result in a chargeback
- Please remember to send all relevant documentation that supports the transaction ie Terms and Conditions and details of Authorisation codes, dates and times, where appropriate
- Remember, transaction copies and all details provided need to be clear, as chargebacks can also occur when transaction copies are illegible
- Please ask for details of our Faxlink service, which provides a quick and simple way of dealing with retrieval and chargeback letters via a fax machine (see Section 4.4)
- If you are already registered and using the Faxlink service, templates are available for you to use. To request a copy of the template relevant to your business, please contact **01604 614 012.***

4.4 Faxlink service

This service lets you send and receive all chargeback and retrieval information by fax, avoiding postal delays and speeding up the process. There are no extra charges for utilising this service.

Should you have any queries about chargebacks, retrievals or Faxlink, please call our dedicated team on **01604 614 012**.*

4.5 To help reduce the risk of chargebacks

- Use a chip and PIN-enabled terminal to help protect your business against fraud. Using chip and PIN helps establish that a card is genuine and that the person using it is the true owner. The chip makes it difficult to counterfeit or copy the card while the PIN makes it harder for a criminal to use a lost or stolen card. And because, instead of signing, the customer authorises the transaction by keying in a 4-digit PIN known only to them, the risk from forgery is reduced. For contactless transactions, provided you process transactions in accordance to card scheme regulations and follow the procedures laid out in this guide, we will offer you the same level of protection.

- Ensure that all transactions are correctly processed according to card type

- Ensure you only accept cards which you have an Agreement to process, as some cards perform several functions

- Do not accept mail, telephone or internet transactions unless you are aware of the possible risks surrounding this type of transaction. If you see an increase in this type of transaction, please notify us to ensure you have the correct Agreement in place

- Follow your instincts – if something about a card, card presenter or the transaction itself does not seem genuine, make a Code 10 call to our Authorisation Department. **Please remember that Authorisation is not a guarantee of payment and Code 10 calls are only for card-present transactions**

- Retain copies of all transaction records. In order to settle any dispute, you may be asked to provide evidence of a transaction. Failure to do so may result in a chargeback to your business. You must keep all receipts for a minimum of 6 months

- Remember to display a limited returns policy on your receipts and at the point of sale, to avoid disputes which could lead to a chargeback.

4.6 Timescales to chargebacks

A disputed transaction is normally charged back because either:

- the cardholder does not recognise the transaction (eg they claim their card details have been used fraudulently) or

- the transaction has been processed outside of your Merchant Agreement (eg Authorisation was not obtained when required).

The vast majority of disputes are raised because the genuine cardholder disputes the transaction on their statement. As cardholders are only sent card statements once a month, it can be up to one month before a cardholder will receive their statement and therefore dispute the transaction with their Card Issuer (eg MBNA, Capital One, NatWest, Barclaycard etc.).

In cases where the cardholder claims neither to have participated in nor authorised a transaction, the Card Issuer will ask the cardholder to complete and sign a 'disclaimer'. This is a legal document whereby the cardholder declares they did not undertake the transaction. Typically the cardholder will be given 14 days to complete and return this documentation.

The Card Issuer does not notify Barclaycard of the dispute until it has received all necessary documentation from the cardholder. Visa and MasterCard have strict time limits in which Card Issuers must notify us of any dispute along with rules for what documentation must be provided. Barclaycard will automatically protect you from a dispute if the correct documentation is supplied or if the correct time limits are adhered to.

As soon as Barclaycard receives notification of the disputed transaction, we will notify you. Analysis has shown that the typical disputed transaction is notified to us approximately 50 days after the date the transaction was undertaken. Sometimes it may be less but often it can be more, especially in cases where the cardholder is based outside of the UK. Actual time limits vary depending on the reason for dispute and what part of the world the card was issued in (cards issued overseas have longer time limits to allow for postal delays). The maximum time allowed is 120 days from the date of the transaction. For transactions relating to delayed travel (eg holidays), the time limit is calculated from the date of travel and not the date of the transaction.

Notification of the chargebacks will either be by letter or, if you have signed up to our Faxlink service, by fax. For disputes where it is likely that you will have additional information that may enable us to defend the dispute, you will have 14 days after receipt of this notification to supply the information. For disputes where it is unlikely you will be able to defend the dispute eg if Authorisation was not obtained, then you may be debited at this time. If you disagree with the dispute it is important that you notify us with your reasons in writing within 14 days. If you fail to respond within the 14 days, or your reply is unclear or illegible, then we may not be able to defend you from the chargeback.

Our Chargeback Education Team can provide bespoke advice as to when you should be replying and with what. They can also provide general advice on all matters relating to chargebacks. For tailored advice for your own business, please call us on **01604 614 012*** (available 9.00am – 5.00pm Monday to Friday. Closed Bank Holidays). Or email us at **chargeback.education@barclaycardbusiness.co.uk** and we will get back to you within 48 hours. Please provide your contact details and Barclaycard Merchant number (found on your statement).

5. vehicle rental reservation service

5.1 Vehicle rental companies

Best Practice for minimising chargebacks
At Barclaycard we understand that chargebacks are an ongoing concern. We know that certain types of chargebacks occur more frequently amongst vehicle rental providers. To support you we have created this Best Practice guide to detail the correct procedures to deal with chargebacks and provide advice on how to reduce the cost to your business.

Although it is in your best interests to authorise every transaction, please remember that AUTHORISATION DOES NOT GUARANTEE PAYMENT – it only confirms that:

1. the card has not been reported lost or stolen at the time of the transaction
2. there are sufficient funds available at the time of the transaction.

Except for contactless transactions, you will still be liable for any transactions if the genuine cardholder later states that they did not participate in or authorise a transaction.

Card-not-present transactions are particularly prone to chargebacks at a later date.

Please remember: Any transactions processed without the card being present may result in a chargeback should they be disputed at a later date. It is in your own interests, where possible, to process transactions with the card present and ensure the cardholder is verified by their PIN or a signature is obtained (if the card is not PIN-enabled).

5.1.1 Tips on taking telephone reservations

As telephone reservations are card-not-present transactions, we recommend you take the precaution of asking for as many details as possible in order to verify the authenticity of the unseen cardholder:

- the name of the caller
- their direct dial telephone number (NOT a mobile telephone number)
- the name of the person(s) requiring the vehicle (if not the caller)
- their expected collection date and time
- the number of days they are expected to hire the vehicle
- the card number of the card to be used for the charges
- the card valid from date
- the card expiry date
- the cardholder's name
- the cardholder's billing address
- the Card Security Code (the last 3 digits on the signature strip on the back of the card or the 3 digits in the box adjacent to the signature panel).†

†If your vehicle reservation system allows you to check the Card Security Code given at the time of the reservation then it should be entered. However, if you are using a POS terminal that is unable to check the Card Security Code then it should still be asked for as this may deter potential fraudsters. However, you must not keep or store the CSC code.

Additionally, you should discuss and agree the hire rate and obtain the caller's consent to your cancellation policy. The cancellation policy must be clearly explained to the customer. Once you have confirmed acceptance of their order, please ensure you send a copy of your Terms and Conditions together with the cancellation policy to the cardholder.

5.1.2 Taking reservations by fax or mail

Like the tips on telephone reservations, we recommend requesting as many details as possible from the unseen cardholder – as listed above. And when taking orders from company cardholders, we advise you to check that the fax or letter looks genuine eg that it's on genuine company headed paper. Obvious questions to ask are:

- Does it contain a company logo?
- Does it contain the correct corporate colours?
- Does it show a switchboard telephone number? Check by calling the sender; the switchboard operator would normally announce the company
- Does it contain a registered address for 'Ltd' and 'PLC' companies?
- Is it signed by someone in authority?

Faxes and mail bookings should contain the same details required for telephone reservations – except for the Card Security Code. It should also confirm acceptance of your cancellation policy. And we recommend calling the sender for confirmation of the reservation, the card details and the Card Security Code.

Ideally you would also reply with your acceptance of the reservation in writing (fax or mail), together with a copy of your Terms and Conditions, including your cancellation policy.

5.1.3 Taking reservations over the internet

Transactions via the internet are effectively card-not-present transactions and are prone to being disputed and charged back. It is in your own interests to process transactions with the card present wherever possible.

When taking bookings over the internet we advise that you take the same procedures and precautions as those taken by telephone. This includes ensuring that cardholders can confirm acceptance of your Terms and Conditions eg in a tick box.

We strongly recommend that your website uses 'Internet Authentication'. (Refer to Authentication Section 1.4.2.3 for further details.) Available from Barclaycard, this service allows you to confirm that reservations are being made by genuine cardholders. We can provide this service as part of your existing website or you can use our own ePDQ product as your Payment Service Provider (PSP). For more details on ePDQ, simply click onto our website at **www.barclaycard.co.uk/paymentacceptance**

5.1.4 Extra tips for verifying genuine customers

- Set up your reservation system (or a stand-alone PC solution) to check the billing and company address by comparing it to the Royal Mail address. See **www.royalmail.com** or call Royal Mail Postcode Products on **0845 603 9038**. Alternatively, you can invest in PC software that uses a postcode address to verify addresses. Find out more at these websites:
  - **www.streetmap.co.uk**
  - **http://uk2.multimap.com**
- Check the electoral roll. Companies like Equifax do this, and will charge for the service (**0845 600 1772** or **www.equifax.co.uk**). Alternatively, you can buy and install electoral roll software
- Check the Yellow Pages or BT Telephone Directory for the customer's listing. Then call and ask for the person who sent the fax
- Barclaycard provides an ePDQ product, with inbuilt velocity checking, with parameters that you can determine. The fraud screening options are controlled and set by you.

5.1.5 Your cancellation policy

Please note that whilst you may have a cancellation policy within your Terms and Conditions (which must be clearly communicated to your customer), you may not charge any cancellation fee to the card used for reservation. If you do make a charge to the card, Barclaycard will be unable to defend you from any subsequent chargeback.

5.1.6 No show

If a cardholder doesn't turn up, having failed to cancel their hire vehicle, your Terms and Conditions may entitle you to charge the customer. However, you must not charge the No show amount to the card used for reservation. If you do charge the card, then Barclaycard will be unable to defend you from any subsequent chargeback.

5.1.7 Vehicle collection

Ask to see the customer's card and ask them to read your Terms and Conditions and sign the Rental Agreement. Then carry out the usual visual checks to ensure the card is genuine eg the hologram, and that the signature strip has not been tampered with.

You must not ask the cardholder to sign a blank transaction receipt in case there are any additional or delayed charges. The cardholder must give their expressed consent to be charged additional or delayed charges.

If possible obtain payment by processing a card-present transaction (refer to Section 2.1). If payment has already been obtained, ensure an imprint of the card is obtained on the Car Rental Agreement as proof that the cardholder consented to pay by card.

If a specialised vehicle was requested (ie a vehicle that forms less than 10% of your fleet or one that you have obtained specifically for the customer to hire) and it then becomes unavailable, you must provide the following services at no extra charge:

- a comparable vehicle at another car rental establishment for the reservation period
- transportation to the alternative outlet.

5.1.8 Estimated Authorisation

Estimated Authorisation lets you estimate the final transaction amount, get Authorisation and reserve the payment while the vehicle is still on hire. Base your estimate on:

- the cardholder's intended rental period
- the rental rate and applicable tax
- mileage rates.

You cannot use Estimated Authorisation with UK Maestro, Maestro or Solo cards, and it does not apply to potential vehicle damage or other insurance-deductible amounts.

Estimated Authorisations are valid for the length of the rental. However, for extended hire we recommend you close the customer's account after 14 days and bill them fortnightly.

The Operating guide for your terminal includes instructions for Estimated Authorisations, including chip and PIN card transactions, when the hirer will need to enter their PIN number to confirm they are the genuine cardholder.

You can update estimates as often as you need, up to and including the date the vehicle is returned. When you issue a new estimate, make sure it does not include amounts which have already been authorised.

5.1.9 Estimated Authorisation – useful tips

- Make sure your transaction receipt always includes the details of the Authorisation code, the dates and the amount(s)

- Always tell the hirer how much you have estimated, as it will reduce the funds available on their card. Explain that they have not yet been charged, and that their final bill is unlikely to be exactly the same as the estimate

- If your customer unexpectedly decides to reduce the hire period, simply provide the appropriate refund. Refunds must always be applied to the same card used for the original payment.

5.1.10 Estimated Authorisation – end of hire

If the final bill is within 15% of the estimated amount, you can use the code provided during Estimated Authorisation. However, you will need a final Authorisation code if:

- the final transaction amount is above your floor limit and you have not obtained a previous Authorisation

- there is more than 15% difference between the final bill and the Pre-authorisation amount

- the hirer is paying by Visa Electron and the final bill is more than the sum of all the Estimated Authorisations you've already obtained for their hire period.

5.1.11 Handling Pre-authorisation

Pre-authorisation allows you to estimate the final transaction amount and receive Authorisation before the vehicle is returned – allowing you to reserve the funds on the card while the vehicle is still on hire. However, this is not supported on UK Maestro, Maestro or Solo cards. Instead we recommend you obtain full payment upon vehicle collection, for the expected hire value. If the customer unexpectedly decides to reduce the length of hire, you can then simply provide the appropriate refund.

The value should be based on the cardholder's intended rental period, the rental rate with applicable tax and the mileage rates. You can update the estimates as often as you need, up to and including the date the vehicle is returned. Each additional Pre-authorisation request must not include previously authorised amounts. And you may not attempt to gain Pre-authorisation for potential vehicle damages or the insurance deductible amount.

The Authorisation remains valid for the length of the rental. However, we recommend that you close the customer's account after two weeks and bill the customer every two weeks.

- The Operating guide for your terminal contains instructions for performing Pre-authorisation. This can include undertaking a Pre-authorisation using a chip and PIN-compliant card. The cardholder will be required to input their PIN number at the time of the Pre-authorisation to confirm they are the genuine cardholder

- Estimate the final amount and obtain Authorisation

- Do advise the hirer how much you have pre-authorised, as this will reduce the funds they have available on the card. Explain to the hirer that no charge has actually been made at this point, and that it is unlikely that the final bill will be exactly the same as the pre-authorised amount.

5.1.12 Pre-authorisation – end of hire

If the final bill is within 15% of the pre-authorised amount, you can process the transaction by using the code provided during Pre-authorisation.

If there is a difference of more than 15% between the final bill and the pre-authorised amount, please call **0870 24 24 240*** and ask for another Authorisation code for the difference.

> **Tip**
>
> Make sure you keep accurate records of the hirer's charges, including dates and amounts.

5.1.13 Accident or collision

In the event of an accident/collision, you may charge Visa cardholders for the damage to the vehicle. An estimate of the cost must also be obtained from an organisation which can legally provide such services. Alternatively, an itemised repair bill may be produced. Either of these should always be forwarded to the cardholder where a charge for damage is made. The following conditions also apply:

- The cardholder must have consented in writing to pay such charges by Visa card (this consent should make up part of your Rental Agreement). It is critical that your Car Rental Agreement clearly states that any additional or collision charges will be charged to the Visa card used for payment to hire the car. The cardholder must sign to agree that they accept this Term and Condition. The cardholder's signature must be on the same page of the Car Rental Agreement as the condition. If the cardholder's signature is on a separate page we may be unable to defend you from a subsequent chargeback should the cardholder claim that they never agreed to their Visa card being charged for any additional charges

- The charge must be submitted within 90 calendar days of the date of the transaction

- There is a bigger risk of chargeback if the cardholder is not notified.

Note about MasterCard: To apply additional charges to a MasterCard, a separate cardholder signed authority must be obtained by processing a card-present transaction (refer to Section 2.1). If the charge is disputed later, this will be required as proof that the cardholder authorised the additional charge.

5.1.14 Procedure for transacting delayed charges

In order for you to process a delayed charge (such as damage, fuel, insurance fee, parking tickets, excessive mileage, additional rental etc.) the cardholder must have consented by signing the Rental Agreement and agreeing to the Terms and Conditions. These state their liability for late charges to be debited to the card number used in the original transaction. The cardholder's signature must be on the same page of the Car Rental Agreement as the Term and Condition that allows you to charge for delayed charges. If the cardholder's signature is on a separate page, we may be unable to defend you from a subsequent chargeback should the cardholder claim that they never agreed to their card being charged for any delayed charges.

Any such charges must be processed within 90 days of the original transaction date – and you must obtain further Authorisation. The charge must be submitted as a separate transaction, with the words 'Signature on file' clearly visible. You are required to notify the cardholder in writing of any delayed charges – sent to the address on the Rental Agreement.

Also, you must supply them with any additional documentation to support the charge eg if the customer was responsible for a traffic violation, send them:

- a copy of the rental agreement
- documentation of the violation
- the licence number of the rental vehicle
- the statute/law violated and (if applicable) a copy of the Civil Authority's accident report
- notice of the amount to be charged.

5.1.15 Accepting split sales

Occasionally, customers ask to split payments between cards, cash or cheques, sometimes in order to share costs between partners. Although these transactions are acceptable, a high number of chargebacks result from them. So Authorisation must always be obtained regardless of your floor limit – and always inform the Authorisation Operator at the start of the call that the transaction is part of a split sale. Process only one transaction per card.

5.1.16 Your refund policy

If you operate a No Refund policy this must be made clear to the cardholder at reservation.

If you do agree to refunds, beware of any opportunities for fraudsters. All refunds must be credited to the same card used to make the booking. Where a charge is made to a card in error, the reversal must be applied to the card within 30 calendar days. Under no circumstances refund by cash, cheque or other payment means as this is likely to result in chargebacks.

Contactless refunds are prohibited. All refunds for contactless transactions should be undertaken as chip and PIN transactions on the same card.

5.1.17 Extended hire

We strongly recommend that you do not allow your customer to hire the vehicle for more than two weeks without settling their bill. Ask hirers wishing to extend the lease for more than two weeks to pay the current total due – ideally by the cardholder in person. Failing that, by using the card details provided at the original booking (although there is a risk that this amount could be disputed at a later date if no signature or PIN is obtained). If the current bill is more than 15% over the pre-authorised amount obtained at the original transaction, you need to get a further Pre-authorisation code for the remainder of the rental period.

5.1.18 Disputed transactions

If a transaction is later disputed, it is vital to show that the card was present and authorised (where required). Except for contactless transactions, if no signature or PIN was obtained or if Authorisation was not given then we will be unable to defend you from a chargeback. Where possible and except for contactless transactions, it is in your interest to process transactions with the card present and obtain a signature or PIN.

The most common reasons why disputed transactions are charged back for vehicle rental are:

1. **Hire reservations made using a card obtained by a fraudster who never arrives**. Often this is because the fraudster is only using your reservation system to check that the card is valid and funds are available. They will then use the card to obtain goods from other establishments fraudulently. The first time the genuine cardholder will be aware that their card has been used fraudulently is when they receive their card statement and they see they have been charged your No show charge.

> ### Tip
>
> To try to prevent taking reservations from fraudsters we strongly recommend the best practices detailed in this Procedure guide.

2. **Not replying to requests for information**. Under card scheme rules, the Card Issuer is entitled to request details of any transaction. In most instances, they only need a copy of the final transaction receipt, showing the card was present at the transaction and, except for contactless transactions, was authenticated by the cardholder – either by a signature or PIN. Sometimes, however, the Card Issuer may require a full breakdown of the charge. The Request for Information from Barclaycard will give details of what is required. Please ensure you reply within 14 days – failure may result in the Card Issuer making a chargeback.

For more information on preventing chargebacks, please go to our website at **www.barclaycard.co.uk/information zone/chargebacks**

Or alternatively call our dedicated Chargeback Telephone Team on **01604 614 012*** and ask to speak to our Chargeback Education Team.

5.1.19 Sample retrieval letter – internet transactions

This is an example of a letter you might receive from us asking for details of a queried online transaction. You simply need to check the transaction details are correct, find the sales voucher and send it back to us with the letter.

payment acceptance   **barclaycard**

1234 Pavilion Drive,
Northampton, NN4 7SG
www.barclaycard.co.uk/paymentacceptance

Retrieval
Barclaycard, Dept FX
1234 Pavilion Drive
Northampton
NN4 7SG

Date:

Dear Sir/Madam,

rental agreement details request – internet booking

The Card Issuing Company has requested details of the transaction below. Since this item relates to an INTERNET transaction, we are able to supply the following details of the transaction:

CASE ID:
CARD NUMBER:
EXPIRY DATE:
CARDHOLDER NAME:
CARDHOLDER ADDRESS:
RENTAL AGREEMENT NUMBER:
RENTAL AND RETURN LOCATION:
RENTAL AND RETURN DATES:
VEHICLE TYPE:
AUTHORISATION CODE (if any):
A COPY OF THE TERMS AND CONDITIONS:
TOTAL TRANSACTION AMOUNT:
This amount must be the same as the case ID.
Please show breakdown of what the total amount is made up of eg damage waiver, excess mileage, refuelling etc.

DATE AND AMOUNT OF REFUND (if applicable)

Yours faithfully,

Contact Name
Contact Telephone/Fax Number

Barclays Bank PLC.
Barclays Bank PLC is authorised and regulated
by the Financial Services Authority.
Registered in England. Registered No: 1026167.
Registered Office: 1 Churchill Place, London E14 5HP.

5.1.19 Sample retrieval letter – telephone and mail order transactions

This is an example of a letter you might receive from us asking for details of a queried telephone or mail order transaction. You simply need to check the transaction details are correct, find the sales voucher and send it back to us with the letter.

payment acceptance   **barclaycard**

1234 Pavilion Drive,
Northampton, NN4 7SG
www.barclaycard.co.uk/paymentacceptance

Retrieval
Barclaycard, Dept FX
1234 Pavilion Drive
Northampton
NN4 7SG

Date:

Dear Sir/Madam,

rental agreement details request – car rental

The Card Issuing Company has requested details of the transaction below. Since this item relates to a Car Rental transaction, we are able to supply the following details of the transaction, together with a copy of the Agreement/Terms and Conditions.

CASE ID:
CARD NUMBER:
EXPIRY DATE:
AMOUNT:
CARDHOLDER NAME:
CARDHOLDER ADDRESS:
RENTAL AGREEMENT NUMBER:
RENTAL AND RETURN LOCATION:
RENTAL AND RETURN DATES:
VEHICLE TYPE:
AUTHORISATION CODE (if any):
A COPY OF THE TERMS AND CONDITIONS:
TOTAL TRANSACTION AMOUNT:
This amount must be the same as the case ID.
Please show breakdown of what the total amount is made up of eg damage waiver, excess mileage, refuelling etc.

DATE AND AMOUNT OF REFUND (if applicable)

Yours faithfully,

Contact Name
Contact Telephone/Fax Number

Barclays Bank PLC.
Barclays Bank PLC is authorised and regulated
by the Financial Services Authority.
Registered in England. Registered No: 1026167.
Registered Office: 1 Churchill Place, London E14 5HP.

5.2 Additional rules for the Visa Vehicle Rental Reservation Service

Visa Vehicle Rental

A Vehicle Rental Company or its third-party booking agent that accepts European issued Visa Cards or Visa Electron Cards must offer a guaranteed car rental reservation and adhere to the following requirements.

In return you may optionally charge a No show fee where a Visa Europe cardholder has not cancelled a reservation in accordance with your terms and conditions.

1 You or your third-party booking agent must obtain the cardholder name, account number and expiration date as displayed on the Visa Card or Visa Electron Card

2 You or your third-party booking must communicate your cancellation policy and procedures to the cardholder when making the reservation.

3 You or your third-party booking agent must inform the cardholder, in writing, of all the following:

- Reserved car rental rate
- Currency of the transaction
- Exact name and physical address of the location from where the car is to be collected.

4. You or your third-party booking agent must provide written confirmation of the reservation to the cardholder by mail, fax or e-mail.

5. You or your third-party booking agent must inform the cardholder that a No-show Transaction up to the value of one day's rental at the reserved car rental rate will be billed if the cardholder has neither:

- Collected the vehicle within the 24 hours of the collection time nor
- Properly cancelled the reservation in accordance with your communicated cancellation policy.

6. If you wish to bill a No-show Transaction, you or your third-party booking agent must confirm, in writing, as part of the reservation confirmation, the value and currency of the fee that will be billed to the cardholder.

7. You or your third-party booking agent must also provide written confirmation containing the following information:

- Cardholder name, account number (truncated to only display four digits) and card expiration date as displayed on the Visa Card or Visa Electron Card.
- Confirmation code which the cardholder must retain in the event of a dispute.
- Exact physical address of the location from where the car is to be collected.
- Hours of operation of the collection and return outlet.
- Cancellation policy procedures.

8. You or your third-party booking agent must not require cancellation notification of more than 72 hours prior to the schedule collection time of the booking without penalty.

9. If the cardholder makes a reservation within 72 hours of the scheduled pick up date, the cancellation deadline must be no earlier than 18:00 at the physical location of the vehicle rental company on the scheduled pick up date.

10. You or your third-party booking agent must provide to the cardholder with cancellation code (if the reservation is properly cancelled in accordance with the communicated cancellation policy that relates to the Vehicle Rental Reservation Services) and advise the cardholder to retain it in case of dispute.

11. You or your third-party booking agent must send written confirmation of the cancellation to the cardholder within 5 business*days of the cancellation date.

12. If a cardholder has not claimed or cancelled the car rental by the specified time, you or your third-party booking agent must keep the car available according to the reservation for 24 hours from the collection time. If the car remains unclaimed by the cardholder, you may process a No-show Transaction.

13. If the Vehicle Reservation Service guaranteed vehicle is unavailable, you must provide the cardholder with an equivalent or higher group car at no extra charge.

14. You must ensure that the cardholder is advised at the time of making the reservation that a confirmation receipt is available during the hours of operation of the outlet on return of the rented vehicle. This confirmation receipt confirms the mutually agreed condition of the rented car upon return.

15. You must provide the cardholder with written confirmation of the cardholder decision of whether or not to request a confirmation receipt as part of the reservation confirmation.

16. You must provide the cardholder with written confirmation of all of the following:

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

17. If the cardholder returns the car using an express drop-off facility, the written confirmation receipt must be sent to the cardholder within 5 business days of the return date of the rented car. You should advise the cardholder to retain the confirmation receipt in case of a dispute.

18. You may only process a delayed or amended charge transaction if the cardholder has given their prior consent to incur such delayed or amended charge transaction.

19. For delayed or amended charge transactions related to damages, you must provide a written confirmation containing the details of the damage, the cost of the damage and the currency in which the cost of the damage will be charged to the cardholder within 10 business days of the return date of the rented car.

20. For delayed or amended charge transactions relating to damages where you have written to the cardholder, the cardholder may, at no cost to you, provide written confirmation of an alternative estimate of cost of the damage within 10 business days of receipt of original written confirmation detailing the cost of the damage from your company.

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

22. You must wait 20 business days from the date of the confirmation receipt provided to the cardholder before processing a charge for damages.

*A business day is understood to be Monday through Friday 09h00-17h00 excluding Saturday and Sunday and public holidays.

6. lodging and accommodation

Best Practice for minimising chargebacks
At Barclaycard we understand that chargebacks are an ongoing concern. We know that certain types of chargebacks occur more frequently amongst hotel, lodging and accommodation providers. To support you, we have created this Best Practice guide to help you understand the correct procedures for dealing with chargebacks and provide advice on how to reduce the cost to your business.

Though it is in your best interests to authorise every transaction, please remember that **AUTHORISATION DOES NOT GUARANTEE PAYMENT** – it confirms only that:

1. the card has not been reported lost or stolen at the time of the transaction
2. there are sufficient funds available at the time of the transaction.

As the rules stand, except for contactless transactions, you will still be liable for any transactions should the genuine cardholder later state that they did not participate in or authorise a transaction. Card-not-present transactions are particularly prone to chargebacks at a later date.

Please remember: If there is no signature on the final bill, we may be unable to defend you in the event of any chargeback. There is still an element of risk if the guest is allowed to check out using the Priority Checkout Service.

6.1 Taking advance reservations
Wherever possible, the person requiring accommodation/lodging should be asked to make the reservation themselves. Of course, for practical reasons you may need to accept reservations from third parties, such as secretaries acting on behalf of their bosses.

6.2 Tips on taking telephone reservations

As telephone reservations are card-not-present transactions, we recommend you take the precaution of asking for as many details as possible in order to verify the authenticity of the unseen cardholder:

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

In addition, if the booking is for corporate purposes:

- the caller's name and position in the company/organisation
- the name of the company/organisation
- the company/organisation switchboard telephone number.

*If your reservation system allows you to check the Card Security Code given at the time of the reservation then do enter it. Even if you use a POS terminal that is unable to check the Card Security Code, still ask for it as this may deter fraudsters.

Also, you should take care to discuss and agree the room rate and the hotel cancellation policy. You must seek the caller's consent in accepting the cancellation policy. Once the caller has accepted you can then issue a reservation code.

If the reservation is made through a third party, a Travel Agent for example, ensure they advise the customer of your Terms and Conditions. You should then ask the caller to confirm the reservation in writing (either by fax or mail – see below).

Tip

When taking the reservation listen for suspicious activity, such as long pauses to any questions where the answer would be obvious to a genuine caller.

6.3 Taking reservations by fax or mail

Double check that the fax or letter looks genuine eg that it's on genuine company headed paper. Obvious questions to ask are:

- Does it contain a company logo and show correct corporate colours?
- Does it show a switchboard telephone number? Check by calling the sender; the switchboard operator would normally announce the company
- Does it contain a registered address for 'Ltd' and 'PLC' companies?
- Is it signed by someone in authority?

Faxes and mail bookings should contain the same details required for telephone reservations – except for the Card Security Code. They should also confirm acceptance of your cancellation policy. And we recommend calling the sender for confirmation of the reservation, the card details and the Card Security Code. Ideally you would also reply with your acceptance of the reservation in writing (fax or mail), together with a copy of your Terms and Conditions, including your cancellation policy.

6.4 Taking reservations over the internet

Transactions via the internet are effectively card-not-present transactions, so are more likely to result in a chargeback. It is in your own interests to process transactions with the card present, whenever possible.

When taking bookings over the internet we advise that you take the same procedures and precautions as those taken by telephone. This includes ensuring that cardholders can confirm acceptance of your Terms and Conditions eg in a tick box. We strongly recommend that your website allows 'Internet Authentication'. Available from Barclaycard, this service allows you to confirm that reservations are being made by genuine cardholders. We can provide this service as part of your existing website or you can use our own ePDQ product as your Payment Service Provider (PSP). For more details on ePDQ, visit **www.barclaycard.co.uk/paymentacceptance**

6.5 Extra tips for verifying genuine customers

- Set up your reservation system (or a stand-alone PC solution) to check the billing and company address by comparing it to the Royal Mail address. See **www.royalmail.com** or call Royal Mail Postcode Products on **0845 603 9038**. Alternatively you can invest in PC software that uses a postcode address to verify addresses. Find out more at these websites:
  - **www.streetmap.co.uk**
  - **http://uk2.multimap.com**

- Check the electoral roll. Companies like Equifax do this, and will charge for the service (**0845 600 1772** or **www.equifax.co.uk**). Alternatively you can buy and install electoral roll software
- Check the Yellow Pages or BT Telephone Directory for the customer's listing. Then call and ask for the person who sent the fax
- Barclaycard provides an ePDQ product, with inbuilt velocity checking, with parameters that you can determine. The fraud screening options are controlled and set by you.

6.6 Taking advanced lodging deposits

If you take advanced lodging deposits under the Visa and MasterCard rules, this is the only amount you are allowed to debit the customer. You will also forfeit your right to charge one night's No Show payment. If you operate a No Refund policy you must make it perfectly clear to the cardholder at the time of the reservation. And any refunds you agree to must be made to the card used for the original booking. Under no circumstances should you refund by cash, cheque or other means. Maestro cards are acceptable only when the cardholder is present, as the card must be processed electronically using the magnetic stripe or embedded chip.

6.7 Your cancellation policy

Any cancellation policy your establishment has must be clearly understood at the time of the reservation ie the customer must be asked whether they accept the policy and to confirm this is so. And the cancellation deadline should be no earlier than 72 hours before the guest is expected.

If a reservation has been made within 72 hours of the expected arrival time, the cancellation deadline will be 6.00pm on the arrival date. If you require cancellation before 6.00pm, you must mail your cancellation policy to the cardholder.

Should the cardholder cancel the reservation within the time frame detailed in your cancellation policy, issue them with a cancellation code for their records and yours.

Note:

i) If your cancellation policy differs from the above, you do risk receiving chargebacks.

ii) You can only enforce the cancellation policy when the customer pays by Visa, MasterCard or JCB card. (Maestro and Solo cards do not allow charges to be made for hotel cancellation charges.)

Tips

Check that the signature on the registration form matches that on the reverse of the card. Also check the hologram, and make sure the signature strip has not been tampered with. You can now go through the Pre-authorisation procedures below.

6.8 Guest arrivals/check-in

When your guests arrive, ask to see the card on which the booking was made, and ask them to complete a registration form. If you allow additional items (newspapers, restaurant bills etc.) to be charged to guests' rooms, your registration form should clearly show this.

6.9 No show

If a cardholder doesn't turn up, having failed to cancel their reservation, you are then entitled to charge one night's stay at the normal check-out time the following day. You can simply charge the card given at reservation.

Send a copy of the transaction receipt and a copy of your Terms and Conditions to the cardholder at their billing address. 'No Show' must be clearly written in the space where the cardholder would normally sign the transaction receipt. The transaction receipt should also clearly show the card number, expiry date and cardholder's name.

However, if the genuine cardholder later claims that they never made the original reservation then the transaction may still be charged back. We would be unable to defend a chargeback in this case. Note about Maestro/Solo cards: You may offer to reserve accommodation for UK Maestro, Maestro or Solo card customers – but be aware that you cannot debit the card for one night's lodging if the customer does not arrive.

6.10 Pre-authorisation

Pre-authorisation allows you to estimate the final bill and reserve those funds on the card account while the guest is staying with you. But this is not supported on UK Maestro, Maestro or Solo cards. Instead we recommend you obtain full payment upon check-in for the expected number of nights' stay. If the customer decides to check out early, simply provide a refund.

- The Operating guide for your terminal contains instructions on performing Pre-authorisation. This can include undertaking a Pre-authorisation using a chip and PIN-compliant card.

The cardholder will be required to input their PIN number at the time of the Pre-authorisation to confirm they are the genuine cardholder.

- Estimate the final amount and obtain Authorisation
- Do advise your guest how much you have pre-authorised, as this will reduce the funds they have available on the card. Explain to the guest that no charge has actually been made at this point, and that it is unlikely that the final bill will be exactly the same as the pre-authorised amount.

6.11 Departures/check-out

If the final bill is within 15% of the pre-authorised amount, you can process the transaction by using the code given at Pre-authorisation.

But if the final bill is more than 15% above the pre-authorised amount, you will need to obtain another Authorisation code for the difference.

6.12 Express/priority check-out service

If you operate an express check-out service, please be warned that we may be unable to defend you from a chargeback should cardholders later deny any transactions.

6.13 Extended stays

We strongly recommend that you do not allow stays of more than two weeks without asking guests to settle their bill. Those requiring longer stays should be asked to pay the current total due. Ideally, ask for their card, or you can use the card details provided at check-in (although there is a risk that this amount could be disputed at a later date if no signature or PIN is obtained). If the bill is more than 15% above the pre-authorised amount at check-in, you are required to obtain a further Pre-authorisation code for the remainder of the stay.

Please remember: If the transaction was undertaken on UK Maestro, Solo or MasterCard and additional charges have been incurred, a separate signed and swiped voucher or imprinted document must be raised as proof that the cardholder authorised these charges to debit their account.

6.14 Disputed transactions

If a transaction is later disputed, it is vital to show that the card was present and authorised (where required). Except for contactless transactions, if no signature or PIN was obtained or if Authorisation was not given then we will be unable to defend you from a chargeback. Where possible and except for contactless transactions, it is in your interest to process transactions with the card present and obtain a signature or PIN.

The most common reasons why disputed transactions are charged back for lodging or accommodation are:

1. **Reservations made using a card obtained by a fraudster who never arrives at the hotel**. Often this is because the fraudster is using your reservation system only to check that the card is valid and funds are available. They will then use the card to obtain goods from other retailers fraudulently. The first time the genuine cardholder will be aware that their card has been used fraudulently is when they receive their card statement and they see they have been charged your No Show charge.

2. **Not replying to requests for information**. Under card scheme rules, the Card Issuer is entitled to request details of any transaction. In most instances, they require only a copy of the final transaction receipt, showing the card was present at the transaction and was authenticated by the cardholder – either by a signature or PIN. Sometimes, however, the Card Issuer may require a full breakdown of the charge. The Request for Information from Barclaycard will give details of what is required. Please ensure you reply within 14 days – failure may result in the Card Issuer making a chargeback.

6.15 Replying to requests for information and notification of chargebacks

If Barclaycard advises that a cardholder is disputing a charge, always ensure you supply the correct information to help us defend the dispute.

6.16 No show charges

For No show charges please send us a copy of the transaction receipt/invoice clearly showing the card details and 'No Show' written on the signature box of any receipt. We also need proof that the cardholder was informed of – and accepted – your Terms and Conditions.

6.17 Express/priority check-out charges

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

- a copy of the transaction receipt captured at check-in proving the card was present and a Pre-authorisation carried out
- a copy of the hotel registration showing the cardholder's signature and acceptance of the charge for the agreed length of stay etc.

6.18 Additional charges

If the dispute was over charges levied since the cardholder checked out (eg minibar charges, breakfast on the last day etc.) please send a copy of the transaction receipt with the words 'Signature on file' in the cardholder signature box. Also, please send a copy of the hotel registration card showing the cardholder's signature and that they accepted that additional charges may be made to their account.

For more information on preventing chargebacks, please click onto our website at
www.barclaycard.co.uk/informationzone/chargebacks

7. contact numbers

Customer Services Department

Please call us on **0844 811 6666*** when you:

- require additional PDQ terminals
- have a query about your statement
- need to order more procedural literature or point of sale materials
- require information on products and services
- wish to advise us of a change in your details eg change of address or change of bank or if you significantly change the type of goods or services that your original Merchant Agreement applies to
- need assistance with any other query or problem.

PDQ Helpdesk

Please call us on **0844 811 6666*** when you:

- need to report a fault with a PDQ terminal, supplied by us
- have any query relating to transactions processed through your PDQ terminal
- have any other PDQ-related query.

Opening hours

Customer Services Department and PDQ Helpdesk.

Monday to Sunday: **8.00am to 12.00 midnight**.

Bank Holidays: **9.00am to 6.00pm**.

Christmas Day: **Closed**.

Authorisation

Please call us on **0844 822 2000*** when you:

- require Authorisation for a transaction over your floor limit (in the event of a PDQ terminal or power failure)
- are suspicious about a card, a card presenter or the circumstances surrounding a card transaction
- are concerned about the validity of a card
- are prompted to do so by your PDQ terminal.

Multiple mail and telephone order transactions

Please call us on **0844 811 4470*** for:

- Authorisation of more than one mail or telephone order transaction at a time.

Opening hours

Authorisation Department, multiple mail and telephone order transactions and cheque validation/guarantee.

Open **24 hours a day, 7 days a week** (including Christmas Day).

Cheque validation/guarantee

Please call us on **0800 515 788*** for:

- 24-hour-a-day validation of Barclays Bank cheques guaranteed by a Barclays Connect card, Barclaycard Visa card or a Barclays Premier card.

Sales Centre

Please call us on **0800 61 61 61*** if you are planning to extend your existing business by opening additional branches or offices in other locations, or by trading over the internet, or you intend to move into a completely new business. Our Sales Centre will assist you to ensure that the necessary approval, documentation and systems are in place. You should also tell us if your business is going through a change of ownership or legal entity.

Opening hours

Monday to Friday: **8.30am to 6.00pm**.

Saturdays, Sundays and Bank Holidays: **Closed**.

Chargeback Department

Please call us on **01604 614 012*** whenever you have a question about chargebacks or retrievals.

Please quote your case-ID when calling. This is always quoted at the top of our letters. It is made up of several digits followed by a dash and then a shortened form of a month, along with two more digits eg 1234-01JAN05. This is the unique reference that is assigned to each retrieval or chargeback.

Alternatively, you can email your query to us at **chargeback.queries@barclaycard.co.uk**. Our chargeback department can also provide bespoke advice on the steps you can take to prevent transactions being charged back to you, as well as help you understand why disputes occur. For advice tailored to your business, please call us on the above number or email us at **chargeback.education@barclaycard.co.uk**

E-commerce Team

Please call us on **0844 822 2099*** if:

- you need information or assistance about trading over the internet.

Opening hours

Chargeback Department and eCommerce Team.

Monday to Sunday: **8.00am to 12.00 midnight.**

Bank Holidays: **Closed.**

Christmas Day: **Closed.**

Complaints handling

We want to hear from you if you feel unhappy about the service you have received from us. Letting us know your concerns gives us the opportunity to put matters right for you and improve our service to all our customers. You can complain in person by visiting our Barclaycard Head Office in Northampton, in writing, by email or by telephone. Details of our complaint handling procedures are available from our Customer Services Department by contacting them by telephone on **0844 811 6666*** or at **www.barclaycard.co.uk/paymentacceptance**

8. glossary

Some of the terms used in the card processing business are unique to the industry.

These brief explanations will help you understand the way in which we work.

Card acquirer

Like Barclaycard, a bank or financial institution which is a member of card schemes such as Visa or MasterCard. Acquirers enter into Agreements with Merchants to process card transactions on their behalf and arrange settlement.

Card-not-present

This refers to card transactions undertaken when the card is not present at the point of sale eg mail order.

Card Issuer

A Card Issuer is a bank, building society or financial institution that issues payment cards.

Card Security Code and Address Verification Service

A service which helps to reduce mail, telephone and internet fraud.

Card schemes

A card scheme is a payment card body, for example Visa. Visa is a card scheme with member banks issuing Visa payment products. For example Visa Credit, Visa Debit and Visa Electron cards.

Other card schemes include MasterCard, whose members issue MasterCard and Maestro (debit) cards.

Each of the card schemes has their own infrastructures and product offerings and member banks choose which scheme and which product they wish to provide their banking customers with.

Card types

There are different types of card:

- Credit card – cardholders can spend up to limits agreed with their card issuer
- Debit card – which is debited to the cardholder's bank account
- Charge card – cardholder spend has to be repaid monthly
- Business card – issued mainly to employees of small and medium-sized companies for miscellaneous business expenditure
- Corporate card – usually issued to employees of large,

blue-chip companies and Government Departments, for travel and entertainment, as well as some other types of business purchase

- Purchasing card – often used by large companies and Government Departments for business supplies, such as company stationery and agency staff
- Fleet card – used by large companies to cover motoring expenses incurred by their employees.

Card processing options

You can accept these cards for both electronic and paper transactions:

- Visa Credit
- MasterCard
- Visa Debit
- Commercial cards
- JCB.

These cards are for electronic transactions only:

- Visa Electron
- Maestro
- Any unembossed cards
- Non-UK cards.

Chargebacks

Chargebacks can be initiated by the cardholder or Card Issuer. Occasionally, a cardholder will dispute a transaction shown on his or her statement with the Card Issuer. If the cardholder's complaint is valid, the amount of the transaction may be charged back to the retailer.

Chip cards

These are the normal bank payment cards but with a computer microchip built into them. The microchip provides a means of securely storing cardholder information.

Chip and PIN

The cardholder enters a unique 4-digit PIN instead of signing a receipt.

This new technology has been rolled out across the UK and will eventually be worldwide. The main objective is to reduce fraudulent transactions which cost businesses and the banking industry millions of pounds each year.

Code 10 calls

When a card or a card presenter arouses your suspicions, you must ring our Authorisation Department immediately on **0844 822 2000**.* If you cannot speak freely because the customer is nearby, tell the operator that you are making a Code 10 call. You will then be asked various questions and instructed as to what steps are necessary.

Compromised card numbers (card number mismatch)

Compromised card numbers are those illegally copied from genuinely held cards.

Fraudsters are currently encoding these numbers into the black magnetic stripe on the back of stolen cards, to produce what appears to be a valid card. Invariably, the embossed number will differ from the magnetic stripe details and this will show on the terminal receipt. These details must be compared when a transaction is undertaken.

Contactless

A contactless transaction is a transaction that is processed utilising wireless technology, where the payment instructions are securely exchanged between a chip card and a specially adapted point of sale terminal. The value of any single transaction is limited to a certain amount (currently £10 – as at April 2009). Any change in this amount would be communicated separately.

ePDQ

Our secure online service for card payment Authorisation and settlement (available as Cardholder Payment Interface (CPI) and Merchant Payment Interface (MPI)).

ePDQ-Lite

Our payment processing system for mail, phone and fax orders, as well as non-automated internet shopping.

Encryption

The process of converting a message so that it is unreadable.

Fall up

As a routine security check, contactless transactions are periodically required to be undertaken as chip and PIN transactions. This checks that the person using the card is the genuine cardholder and is known as a Fall up transaction. Your terminal will advise you when this is the case.

File Transfer Protocol (FTP)

A common method of transferring files across the internet.

Firewall

Computer hardware, software and physical measures which protect confidential information whilst it is on a web-server.

Floor limit

Floor limits are set by us and the card schemes. When a transaction is above your floor limit you must obtain Authorisation.

Home page

The opening page of your website.

Hot Card Warning Notice

Hot cards are those which, due to fraudulent use or cardholder overspending, the Card Issuer has decided to prohibit from further transactions. When records show a hot card has been used in a certain outlet, a Warning Notice is issued to the retailer in question. A reward of £50 is generally paid to anyone recovering and returning a card that is subject to a Hot Card Warning Notice.

Internet transaction

Any payment transaction made by a cardholder, via an electronic network, when the Merchant is not present.

Issue number

A feature of some UK Maestro and Solo cards.

Merchant Voucher Summary (MVS)

The summary voucher which must accompany any sales and refund vouchers when they are paid into a Barclays branch or posted to FDI for processing.

Payment Service Providers (PSPs)

PSPs are companies who offer transaction routing facilities to businesses wishing to trade over the internet.

PDQ

PDQ is the brand name of the electronic processing system developed by us.

PIN

Personal Identification Number. A unique 4-digit number a cardholder will use to verify that they are the true cardholder.

Polling

During the night, and provided you have completed the end-of-day procedure correctly, details of card payments will be collected from the equipment through a phone line. This process is known as polling, and relates to off-line PDQ terminals only.

Pre-authorisation

Pre-authorisation allows you to estimate the final bill and reserve those funds on the card number while the customer is with you.

Recurring transactions

Regular card payments for goods or services such as insurance premiums. These cannot be made with Solo or Maestro cards.

Retrieval

This is a request from a Card Issuer for a copy of a transaction. In the case of a mail or telephone order this will be details of the cardholder's authority to debit their account, together with a copy of the sales voucher or terminal receipt.

SecureCode

A MasterCard approved authentication product designed to allow Maestro and MasterCard to authenticate individual Maestro and MasterCard electronic commerce payments.

Secure Sockets Layer (SSL)

An accepted protocol, which enables secure card payment transactions to be made over the internet.

Server

A central computer that makes services and data available.

Split sale

A transaction which is split between more than one card, or a combination of card, cash or cheque.

Supervisor card

A plastic card which will be supplied with your PDQ terminal and may be required to process a refund electronically or during the end-of-day banking procedure.

Transaction laundering

This is the unacceptable practice of processing someone else's card transactions via your Merchant number.

Us/We

This refers to Barclaycard.

You

This means you as an individual Merchant, or you as a representative of your company.

Various useful telephone numbers are listed throughout this guide. Calls to some of the numbers are charged at national rate and may be monitored or recorded in order to maintain high levels of security and quality of service.

useful numbers

Authorisation: **0844 8222000**
Chargebacks: **01604 614012**
E-Commerce Team: **0844 8222099**
Mobile Top Up Service: **0844 8114414**
Name and Address Check Service: **0844 8114440**
PDQ Helpdesk/Customer Services: **0844 8116666**
Sales Centre: **0800 616161**
Summary VAT: **0844 8222060**
UK Paper Rolls: **0844 8222044**

This information is also available in large print,
Braille and audio format by calling **0844 811 6666**.*

*Calls may be monitored or recorded in order to maintain high levels of security and quality
of service. Calls to 0800 numbers are free if made from a UK landline. Calls to 01604 numbers
will cost no more than 4p per minute, minimum call charge 5.5p (current at August 2009)
for BT customers. Calls to 0844 811/822 numbers will cost no more than 5p per minute,
minimum call charge 5.9p (current at November 2010). Calls to 0870 numbers will cost no more
than 8p per minute, minimum call charge 5.9p (current at August 2009) for BT customers.
The price on non-BT lines may be different.

www.barclaycard.co.uk/paymentacceptance

Verified by Visa:
Merchant Deployment Best Practices Factsheet

The rollout of Verified by Visa (VbV) is gathering momentum across the globe. By September 2005 29,000 merchants across Europe were using the service and this number is growing quickly.

Introduction

As VbV evolves some very valuable lessons can be learned from the marketplace.

This Factsheet provides details of the way that the service should be configured and provides useful best practices information - for those merchants already using VbV, and for those who are about to deploy it.

Mandate: Inline Authentication Window

When implementing VbV, merchants have traditionally had two options in the way they configure the authentication windows - that is, pop-up windows or in-line windows.

With the pop-up authentication windows, research has shown that cardholders often mistake a new window as an advertising message, and will often close it without checking. In addition, cardholders with slower connections to the Internet are even more likely to close pop-up windows, often doing so before the window has completed loading in the browser.
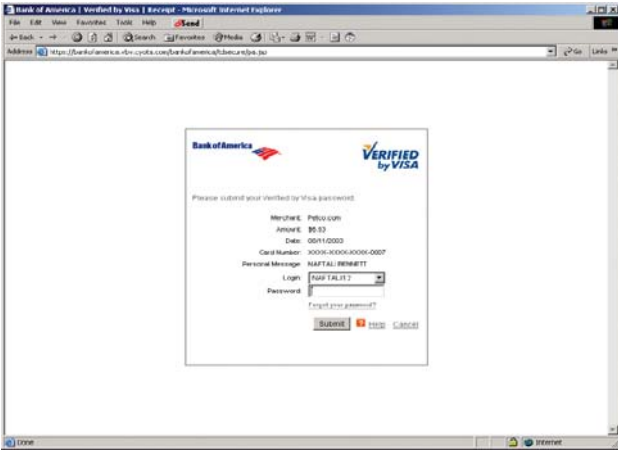
Full Inline
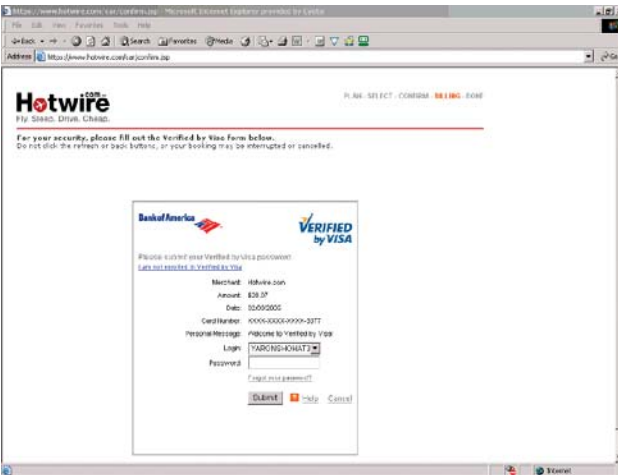
Frame Inline

Closing a pop-up authentication window in this way impact the authentication process, cause unpredictable results and adversely affect the cardholder experience. One of the key lessons learned is that the window closure rates are substantially less with the inline authentication window.

In addition, as the rate of pop-up advertising has increased, pop-up suppression software (sometimes referred to as "pop-up killers") has gained increased market awareness and usage. Such software does not only occur in stand-alone applications, but some browsers and online service providers have begun to incorporate pop-up suppression as a standard feature of their service.

Visa strongly recommends that existing VbV merchants reconfigure the authentication page as inline windows, rather than pop-ups. New merchant deployment of VbV should only be implemented with inline windows.

There are two possible options for deploying inline authentication windows:

Important aspects to consider when deciding on frame inline or full inline:

> Full inline has the benefit of a simpler implementation and less scope for misunderstandings and mistakes.

> Frame inline displays the VbV authentication page in the merchant's main window with the merchant's header. Therefore, VbV is seen as a natural part of the purchase process. It is recommended that the top frame include the merchant's standard branding in a short and concise manner and keep the cardholder within the same look and feel of the checkout process.

> Frame inline implementation must also:
  - Provide enough screen space for the window to fit in. The recommendation is to use a top frame only in order to have a less "crowded" screen.
  - Ensure that the VbV authentication window is not pushed out of the viewable area for low-resolution screens.
  - Ensure that the frame does not include any other links or exit points that may distract the user from completing the VbV authentication process (such as "search" options, standard navigation menu, etc.).
  - Avoid using the HTML element iframe which can cause compatibility issues.
  - Ensure that all frames must be of HTTPS type. Avoid mixing HTTP and HTTPS.
  - Provide simple and correct instructions and allow cardholders with an easy way to go back.

Best Practice: 'Pre-message' Notification

Pre-message increases cardholder awareness and prepares the cardholder for the next screen to be displayed. It is best to include generic text and not to make any assumptions that might confuse cardholders.

'Pre-message' Notification

Best Practice: VbV Logo

Research has shown that the VbV process is more successful and flows more smoothly when merchants include the VbV logo on the site and particularly at the checkout page.
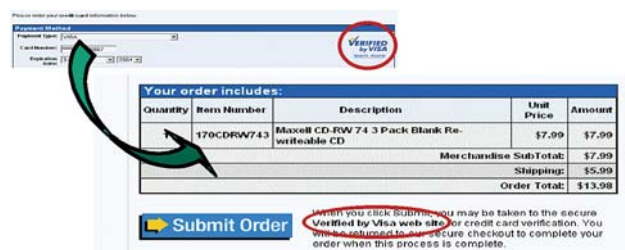
VbV logo

Best Practice: "Back" Button Functionality

Where the policy of the merchant allows the use of the 'back' button, verify that it functions properly and test it thoroughly. Analysis has shown that some inline deployments do not function properly when a cardholder clicks the "Back" button. In some cases, when the "Back" button is clicked an alert is presented warning that the previous page has expired. Seeing this message some cardholders may close the window. Merchants should ensure that their inline deployment responds accordingly when cardholders click "Back". This feature should also be fully tested.
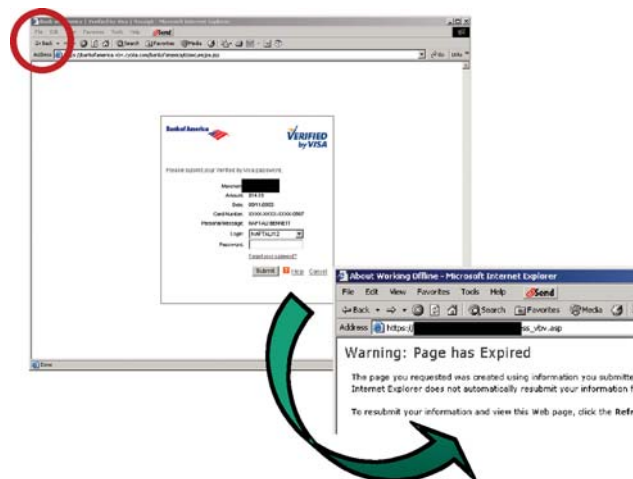
"Back" Button Functionality

VISA

Best Practice: Merchant Plug-In (MPI) configuration

In terms of configuring the MPI to connect to the Visa Directory Server (DS), Visa's strong recommendation is to:

> Use Uniform Resource Locator (URL) for routing messages to the Visa DS (and not straight IP addresses)

> Enable automatic "failover" to the alternative DS URL if receiving a network failure from the primary center.

The following table contains the Visa DS URLs for merchants based in Europe:

	URL
OCC DS	dsw.visa3dsecure.com/DSMsgServlet
OCE DS	ds.visa3dsecure.com/DSMsgServlet

Best Practice: VbV for cardholders only

Visa recommends that the use of VbV should be restricted to web-using customers.

Some early experience has shown that some multi-channel merchants operate a "sales rep zone", whereby sales representatives use the website infrastructure to process telephone order transactions. They will therefore key customer orders into the website when speaking to the cardholder on the telephone.

It is recommended that merchants should avoid deploying VbV at these zones.

Further information

For further generic information on VbV, merchants should contact their acquiring bank or visit **www.visaeurope.com**.

strength through knowledge

Your introduction to chargebacks and retrievals

payment acceptance

barclaycard

strength through knowledge

We know that chargebacks can be a real problem for your business, and costly too. If a transaction is charged back you could lose both the payment and the goods or services that you've provided – plus any time spent on administration, selling or delivering the 'sale'.

This guide will help you better understand both chargebacks and retrieval requests. It also tells you how you can help us defend chargebacks on your behalf – with the right evidence and information, we may be able to stop you from losing out on the payment.

contents

retrieval requests

What is a retrieval request?

A retrieval request, sometimes called a request for information (RFI), is simply us asking you for information about a transaction at the request of a card issuing company. This happens when a cardholder queries a transaction with the card issuing company because they don't recognise it and would like further information to help jog their memory and identify if it is genuine or fraudulent.

Under the Card Scheme regulations we must respond to the card issuing company's retrieval request with information about the transaction. This means we'll need you to provide detailed information about the transaction for us to send back to them so that they can share it with their cardholder.

A retrieval request itself is not a chargeback and your account will not be debited the disputed amount – you can find out more about chargebacks on page 5.

How will I be contacted?

When we have a retrieval request for a transaction you've processed, we'll send you a retrieval schedule (international) or retrieval letter (sterling) detailing the transactions that have been queried. You'll receive these either in the post or by fax.

Example of a retrieval schedule (international)

Card number	Curr amt	Txn date	Mrch ref	Case ID	Merch no	Merchant
1111222233334444	95.83/EUR	85.93/GBP	565656ABC	1234-01JUN09	1234567	Merchant name
4444333332222111	675.00/EUR	631.62/GBP	454545CAB	4567-01JUN09	1234567	Merchant name

Example of a retrieval letter (sterling)

PLEASE FAX BACK TO 01604256661
REF CASE ID 1234-01JUN09/LDTA 30-JUN-09

barclaycard

THE MANAGER
COMPANY
CONTACT NAME
ADDRESS
ADDRESS
ADDRESS

RETRIEVAL
PAYMENT ACCEPTANCE
DEPT FX, 1234 Pavilion Drive
Northampton NN4 7SG
FAX: (01604) 256661

(POTENTIAL FRAUDULENT TRANSACTION)

PLEASE FAX YOUR REPLY TO (01604) 256661 OR POST TO THE ABOVE ADDRESS

CARD NUMBER	: 1111222233334444		
CARD NUMBER	: 1111222233334444	TRANS DATE	: 03-MAY-09
EXPIRY DATE	: 10-OCT-12		
RETAILER REF	: 1234ABCD	OUTLET	: 1234567
TERMINAL NUMBER	: 1234567		
SEQUENCE NUMBER	: 000000000111		
TERMINAL TYPE	: PDQ		
TRAN AMOUNT	: £100.00	STORE REF	: 1234567
KEYING INDICATOR	: SWIPED		

Dear <name>

PLEASE SUPPLY A CLEAR AND LEGIBLE COPY OF THE SIGNED VOUCHER/DETAILS RELATING TO THE ABOVE TRANSACTION BY 15 JUNE 2009.

PLEASE BE ASSURED WE WILL DO EVERYTHING WE CAN TO PREVENT A CHARGEBACK TO YOUR ACCOUNT. HOWEVER, THE CARD ISSUER MAY STILL PROCESS A DEBIT FOR A LATE REPLY OR OTHER REASON AT A LATER DATE. To ensure we action your reply as soon as possible please fax your reply to (01604) 256661.

CUSTOMER SERVICE – CHARGEBACKS

PLACE YOUR VOUCHER/DETAILS HERE

TO FIND OUT MORE INFORMATION ON HOW TO REDUCE THE RISK OF CHARGEBACKS AND RETRIEVALS IN THE FUTURE, PLEASE REFER TO YOUR PROCEDURE GUIDE OR VISIT
www.barclaycard.co.uk/business/existing-customers/chargebacks

How long do I have to reply to a retrieval request?

Your documentation must be received by us within 14 calendar days from the date that we first notified you of the retrieval request.

Where should I fax my retrieval reply to?

Fax your multicurrency (or international) retrievals to 0044 (0) 1604 253195.

Fax your sterling retrievals to 0044 (0) 1604 256661.

What happens if I don't respond to the retrieval request in time?

Failure to respond to a retrieval request within the set time frame could result in a chargeback being raised that we won't be able to defend on your behalf. And that means it's highly likely that your account would be debited for the disputed amount. So it's in your interests to make sure we receive your documentation within 14 days.

If I respond to the retrieval request, can a chargeback still be raised?

A retrieval request can be closely followed by a chargeback if the Card Issuing Company doesn't receive sufficient information about the transaction. That's why it's important you send as much information as possible in your reply to the retrieval request.

Unfortunately, some retrieval requests can still lead to a chargeback even when all the correct information on the transaction has been supplied. Once the Card Issuing Company has raised a chargeback case you're at risk of being debited for the disputed amount. Please refer to the chargebacks section for further information.

chargebacks

What is a chargeback?

A chargeback is a transaction where you may have initially received payment but the transaction is subsequently rejected by the cardholder or the Card Issuing Company and your account is debited with the disputed amount.

We don't raise chargebacks – the Card Issuing Company does, usually on behalf of their cardholder. Please be assured that we'll do everything possible to defend the chargeback on your behalf. However, the nature of the dispute and the type of chargeback will greatly affect what actions we're able to take under the Card Scheme rules as well as the outcome of the defence claims.

How will I know that I have been charged back?

If you've received a chargeback, we'll let you know by notification letter (see example opposite), fax or schedule, telling you why. In some cases, depending on the nature of the chargeback, this communication will advise you that we're 'pending' or putting the chargeback debit on hold for 14 days, while we wait for the requested response (or in other words, a reply to a retrieval request) from you.

What reasons are given for a disputed transaction?

The most common reasons include:

- transaction not recognised

- not responding in time to a request for a copy of a transaction (a retrieval request)

- the transaction is duplicated – so the cardholder was charged more than once

- the transaction wasn't authorised

- the goods or services haven't been received.

Full lists of the chargeback codes and reasons, as set by the Card Scheme Regulators, are provided in the 'reason codes' section starting on page 8.

Example of a chargeback notification letter

payment acceptance

barclaycard

January 29 2009
TEL: 01604 614012

REF: CASE ID 1187-26JAN09/DOYLA/M63
YOUR REF: PRIOR CASE ID: 1234-28DEC08

THE MANAGER
COMPANY
CONTACT NAME
ADDRESS
ADDRESS
ADDRESS

FINANCIAL EXCEPTIONS
PAYMENT ACCEPTANCE
1234 Pavilion Drive
Northampton NN4 7SG

Reason Code of
chargeback case

PLEASE FAX YOUR REPLY TO (01604) 256661 OR POST TO THE ABOVE ADDRESS

OUTLET/MERCHANT: 1234567   RETAILER REF : 2222 333333
CARDHOLDER : NAME NOT GIVEN BY CARD ISSUER
CARD NUMBER : 1111222233334444
TAPE SERIAL : AABBCC   TRANS DATE : 03-JAN-09
TRAN AMOUNT : £178.16
DISPUTED AMOUNT: £178.16
TERMINAL TYPE : POS   KEY IND: CONTINUOUS AUTH

Exact amount disputed
by the Cardholder

Dear Sir/Madam,

CARDHOLDER DOES NOT RECOGNISE TRANSACTION

We regret to inform you that the Card Issuing Company has advised us their cardholder does not recognise the
above transaction.

As part of our commitment to provide excellent customer service, Barclaycard will endeavour to assist you in
resolving this matter. To enable us to pursue this case on your behalf and to give the cardholder every
opportunity to recognise the transaction, we require the following information:

FOR CARD PRESENT TRANSACTIONS
• A full description of the Goods or Services provided
• A delivery address if applicable
• A legible signed/swiped (not keyed) Sales receipt
• A legible signed and imprinted verification voucher.

**If you are unable to reply to us by 12.00pm noon on the 12 February 2009, arrangements will be made to debit
you. Should you accept this Chargeback, there is no need to contact us. To ensure that we action your reply as
soon as possible, please fax your reply quoting case ID 1187-26JAN09 to (01604) 253385.**

How long do I have to respond to a chargeback notification letter?

Chargeback rules and time restrictions are set by the Card Scheme Regulators and are very stringent. It's therefore absolutely essential that if you're able to provide compelling evidence to help us to defend your chargeback, you reply within 14 days from the date of our chargeback notification letter.

Why do I need to reply?

Because in certain circumstances and with the necessary defending evidence, we may be able to defend the chargeback for you, even if your chargeback notification advises that you've already been debited.

Where should I send my reply to?

Your chargeback notification letter will advise you of the correct postal address that should be used to send your response back to us. Or you can fax your reply to us.

Fax your multicurrency (or international) chargeback replies to 0044 (0) 1604 253195.

Fax your sterling chargeback replies to 0044 (0) 1604 253385.

Should I refund my customer for the disputed transaction?

No. It's important that you don't refund the cardholder because this could result in your account being debited twice. If a refund has already been processed to the cardholder's account, please provide us with full details so we can defend the case on your behalf.

Reason codes

Visa, MasterCard and UK Debit Maestro each have their own set of reason codes for chargeback cases. These denote the reason why the transaction is disputed and each reason code has its own regulations set by the relevant card scheme.

Code	Name and description
V30	Services not provided or merchandise not received – the cardholder is stating that they did not receive the services or goods that they paid for.
V41	Cancelled recurring transaction.
V53	Not as described or defective merchandise – the cardholder is stating that the service/goods that they received were either defective or not what was originally described to them by the merchant.
V57	Fraudulent multiple transactions – the cardholder acknowledges participation in one transaction with the merchant. However, they deny authorisation of any further charges.
V60	Illegible fulfilment (of retrieval case) – the Card Issuing Company received the merchant's transaction information from the retrieval case but the documents are illegible/incorrect.
V62	Counterfeit transaction – the cardholder denies authorising or participating in the disputed transaction. A counterfeit card may have been used.
V70	Card recovery bulletin or exception file.
V71	Declined authorisation – the Card Issuing Company is stating that the merchant processed the transaction despite having obtained a Decline authorisation response.
V72	No authorisation – the Card Issuing Company is stating that an authorisation code was required for the transaction but that it was not obtained.
V73	Expired card – the Card Issuing Company is stating that the transaction was processed with an expired card.
V74	Late presentment – the Card Issuing Company is stating that the transaction was not processed within the required time frame for settlement.

Code	Name and description
V75	Transaction not recognised – the cardholder is claiming that they do not recognise the transaction on their statement.
V76	Incorrect currency or transaction code – the Card Issuing Company is stating that the transaction was not processed in the correct currency.
V77	Non-matching or invalid account number – the Card Issuing Company is stating that an incorrect card number was charged for the transaction.
V78	Service code violation – the Card Issuing Company is stating that an authorisation code was not obtained.
V80	Incorrect transaction amount or account number – the cardholder is stating that the amount of the transaction is higher than the amount that they agreed to be charged for or were quoted for.
V81	Fraud – 'card present' environment – the cardholder denies participating in or authorising the transaction that was undertaken in a 'card present' environment.
V82	Duplicate processing – the cardholder is stating that the same transaction was processed more than once to their account.
V83	Fraud – 'card absent' environment – the cardholder denies participating in or authorising the transaction that was undertaken in a 'card absent' environment.
V85	Credit not processed – the cardholder is stating that the refund due to them has not been processed.
V86	Paid by other means – the cardholder is stating that the transaction was paid for by other means and has provided evidence to support the alternative payment.
V90	Non-receipt of cash or load transaction value at ATM or load device.
V93	Risk identification service.
V96	Transaction exceeds limit amount.

Code	Name and description
M01	Requested transaction receipt not received – the cardholder is claiming that they do not recognise the transaction on their statement and the retrieval request raised prior to the chargeback was not fulfilled.
M02	Requested transaction receipt illegible – the Card Issuing Company received the transaction information from the retrieval case but the documents are illegible or missing.
M07	Card recovery bulletin.
M08	Transaction not authorised – the Card Issuing Company is stating that an authorisation code was required for the transaction but that it was not obtained.
M12	Non-matching account number – the Card Issuing Company is stating that an incorrect card number was charged for the transaction.
M31	Transaction amount differs – the cardholder is stating that the amount of the transaction is higher than the amount that they agreed to be charged for or were quoted for or that they paid for the transactions by other means.
M34	Transaction duplication – the cardholder is stating that the same transaction was processed more than once to their account.
M35	Expired card – the Card Issuing Company is stating that the transaction was processed with an expired card.
M37	Fraudulent transaction – the cardholder denies participating in or authorising the card present/card not present transaction.
M40	Fraudulent processing of transactions – the cardholder acknowledges participation in one transaction with the merchant. However, they deny authorisation of any further charges with the same merchant.
M41	Cancelled recurring transaction.
M42	Late presentment – the Card Issuing Company is stating that the transaction was not processed within the required time frame for settlement.
M46	Correct transaction currency not provided – the Card Issuing Company is stating that the transaction was not processed in the correct currency.
M47	Exceeds floor limit, not authorised and fraudulent transaction – the cardholder denies participating in or authorising the transaction and the Card Issuing Company is stating that an authorisation code was required for the transaction and was not obtained.
M49	Questionable merchant activity.
M50	Credit posted as a purchase – the cardholder states that their account was due to be credited; however, the transaction was posted as a debit.

Code	Name and description
M53	Not as described – the cardholder is stating that the service/goods that they received were either defective or not what was originally described to them by the merchant.
M55	Goods or services not provided – the cardholder is stating that they did not receive the services or goods that they paid for.
M57	Credit card activated telephone transaction.
M59	Addendum, no-show or ATM dispute. Various specific reasons within this reason code – these are the most frequently used:
RS3	ATM dispute.
RS5	Guaranteed Reservation Service – the cardholder cancelled the reservation, or the merchant did not meet the terms of the booking as agreed to at the time of booking (see MasterCard regulations for full list).
RS6	Payment transaction – local law, restrictions or other legislative constraints prevent the Issuer from accepting the transaction.
RS7	Addendum dispute – the cardholder is stating that they did not authorise an addendum charge to their original transaction.
M60	Credit not posted – the cardholder is stating that the refund due to them has not been processed.
M62	Counterfeit transaction – the cardholder denies authorising or participating in the disputed transaction; a counterfeit card may have been used.
M63	Cardholder does not recognise transaction on their statement.
M70	Chip liability shift – the cardholder denies authorising or participating in the disputed transaction; a counterfeit card may have been used at a non-Chip-capable terminal.
M71	Chip/PIN liability shift.

Code	Name and description UK Debit Maestro
01	Split Sale – when a transaction is split down into smaller amounts so full amount can be processed. Original transaction will be over floor limit.
02	Cardholder did not perform a cardholder present PIN keyed entry transaction.
03	Transaction submitted after authorisation not approved.
04	Transaction not authorised.
05	Card expired.
06	Late transaction entry.
07	Transaction duplication.
08	Credit not processed.
09	Cardholder disputes transaction amount.
10	Non-fulfilment of documentation requested by the Issuer from the acquirer.
11	Requested supporting documentation illegible/missing required data/contains incorrect data.
12	Hot card – card number that was listed on one of the hot card files and was not referred to when it should have been.
13	Fraudulent transaction at non-PIN-capable cardholder-activated Terminal Outlet.
14	Invalid Card – a transaction which has not been authorised by the Issuer.
15	Non-existent account – not authorised by the Issuer.
16	Transaction at cardholder-activated terminal outlet is above ceiling limit.
18	Invalid transaction.
19	Invalid signature.
20	Missing signature.
21	Violated card – fraud chargeback, transaction performed with a lost or stolen card.
22	Cardholder not present – transaction not initiated by bona fide cardholder.
24	Secondary identification not recorded/ not cardholder's.
25	Old transaction – transaction date of the point of sale is more than 180 days old prior to the processing date.
26	Pre-valid S2 card standard card.

Code	Name and description UK Debit Maestro
27	Fraudulent magnetic stripe – transaction has been authorised.
28	Fraudulent mobile phone pre-payment – CNP.
29	Invalid IIN and goods or services not delivered – (electronic commerce transactions only).
32	Fraud transaction at non-Chip/PIN-capable semi-attended cardholder-activated terminal (SACAT).
33	Transaction performed at non-Chip-capable terminal with counterfeit magnetic stripe.
34	Chip transaction not declined, referred or sent online when required by card or issuer.
35	Fraudulent unidentified fallback transaction performed with Chip at Chip-capable terminal.
36	Transaction performed at non-PIN-capable terminal with lost or stolen PIN-capable card.
99	Inter-member agreement chargeback has been agreed by authorised staff.

Defences

Chargeback defences vary by reason code. Chargeback reason codes can be divided into six main dispute groups:

Cardholder does not recognise	Fraud	Authorisation
Processing error	Cancelled/returned	Non-receipt of goods/services

The next few pages will give you an idea of what you can provide in defence when you receive a chargeback falling into one of these groups.

Cardholder does not recognise

Why would this type of chargeback be raised?

This type of chargeback would typically be raised because the cardholder doesn't recognise a transaction on their statement, or can't recall the value of the transaction processed.

What can you provide in defence?

The minimum requirement in accordance with the Card Scheme rules to defend these reason codes is additional information about the transaction that may not appear on the cardholder's statement.

We'd simply ask you to provide all the details and information that you have on record for the transaction, including a full description of the merchandise or services provided/purchased. We'd also advise you to respond to all chargebacks received under these reason codes because, as long as you respond within the set deadlines, there's a very good chance we'll be able to represent the case for you.

Fraud

Why would these types of chargebacks be raised?

Typically, a fraud chargeback will be raised because the cardholder claims that they neither participated in nor authorised a transaction that has been processed to their account.

For these reason codes the cardholder must sign a disclaimer confirming that they didn't authorise the disputed transactions.

To defend fraudulent chargebacks you must prove that the genuine cardholder of the account charged participated in or authorised the disputed transaction(s).

The defence mechanisms available to you will depend on your industry type and the sales method used to accept the transaction.

What can you provide in defence?

- Fully completed and signed verification voucher.

- Signed delivery receipt at the cardholder's address.

- Compelling evidence to prove that the genuine cardholder participated in the transaction.

- Any documentation that you may have which proves the transaction was undertaken by the genuine cardholder.

Authorisation

Why would these types of chargebacks be raised?

Typically, an authorisation chargeback is raised because the Card Issuing Company is stating that an approval code and valid authorisation code was needed but not obtained for a transaction. Sometimes the cardholder's account is out of order or closed.

What can you provide in defence?

If we granted authorisation we'll defend this type of chargeback using our information from our internal systems or Visa/MasterCard online logs – so we'll only contact you if further information is needed.

If authorisation is received via a third party, a copy of the authorisation log proving that the full amount of the transaction was approved and an authorisation code was obtained will be needed to defend the case.

Processing error

Why would these types of chargebacks be raised?

Usually these types of chargebacks are raised when the cardholder believes that an incorrect charge has been processed by the merchant or there's been a processing error.

Different reason codes in this dispute group will need different information from you to defend the chargeback. We'll explain the reason for the chargeback in the notification letter we send you.

What can you provide in defence?

- Evidence to show that the transaction was processed within the time frames stipulated by the Card Schemes should be provided – such as a transaction receipt or screen shot showing the date that the transaction took place.

- Proof that the transaction was properly processed with the correct currency code which was quoted to the cardholder at the time of the transaction.

- A copy of a legible transaction receipt or booking record showing the card number quoted by the cardholder. This proves that the transaction was processed to the correct card number.

- Proof that, if the amount of the transaction processed was altered from the original quote, the amendment is in accordance with your terms and conditions and that the cardholder agreed to the altered amount.

- Evidence that all transactions processed to the cardholder's account are valid transactions and that no duplication has occurred. For example, you could provide copies of invoices, tickets, transaction receipts or screen prints of bookings.

- Documentation to show that you didn't receive payment by other means such as cash, cheque or an alternative credit card.

- Documentation to show that the transaction was a valid debit and that no credits are due to the cardholder.

Cancelled/returned

Why would these types of chargebacks be raised?

Chargebacks can be raised under these reason codes because:

- the cardholder has stated that they returned the goods to you but haven't yet received a refund

- the cardholder has stated that they cancelled a booking or reservation but haven't received a refund

- a recurring transaction can no longer be processed to a cardholder's account

- goods or services were defective or not as described.

For these reason codes the cardholder must have attempted to resolve the dispute with you before their Card Issuing Company would raise a chargeback. If a cancellation was made, they would also have to provide their cancellation reference.

What can you provide in defence?

You should provide any information or documentation that would help to prove that the cardholder is not due a refund in accordance with your terms and conditions. If goods were received by the cardholder or the services rendered were used by the cardholder, proof of this should be provided (see 'Non-receipt of goods/services' for further guidance).

Non-receipt goods/services

Why would these types of chargebacks be raised?

Typically a chargeback will be raised under these reason codes when a cardholder believes that they didn't receive the goods or services that they purchased. Often:

- the cardholder may have misunderstood their purchase e.g. the cardholder believes they purchased a six month service when it is actually only for three

- you may have failed to deliver goods, or only partly delivered goods

- or the services may have been only partly rendered, or not at all.

What can you provide in defence?

If goods were delivered, you should provide evidence that they were received at the cardholder's address, such as:

- a signed delivery receipt by the genuine cardholder or tracking documentation from the courier

- any additional information or evidence you have to show that the cardholder received the goods, such as emails received from the cardholder.

If services were provided, you need to have evidence that the cardholder received them. This could be one of the following examples:

- a signed car rental agreement at the pick-up of the vehicle

- a signed transaction receipt proving that the cardholder was present to receive the services

- signed check-in documentation for a hotel stay or evidence that the cardholder used other hotel services such as the mini-bar, restaurant etc

- a copy of the invoice for the services provided

- proof that the services were offered/accessible but the cardholder chose not to use them.

dedicated support

We hope you've found this introduction useful, but it really is just the start of how we can help you. Because we recognise that chargebacks are an ongoing concern, we have a dedicated Portfolio Manager for each business sector to help reduce your exposure to chargebacks – and challenge them on your behalf whenever we can.

For more information on the type of support your business can expect to receive, please contact a member of the chargeback team on **01604 614012*** or by email to **ChargebackTeamPortfolio.Managers@barclaycard.co.uk**
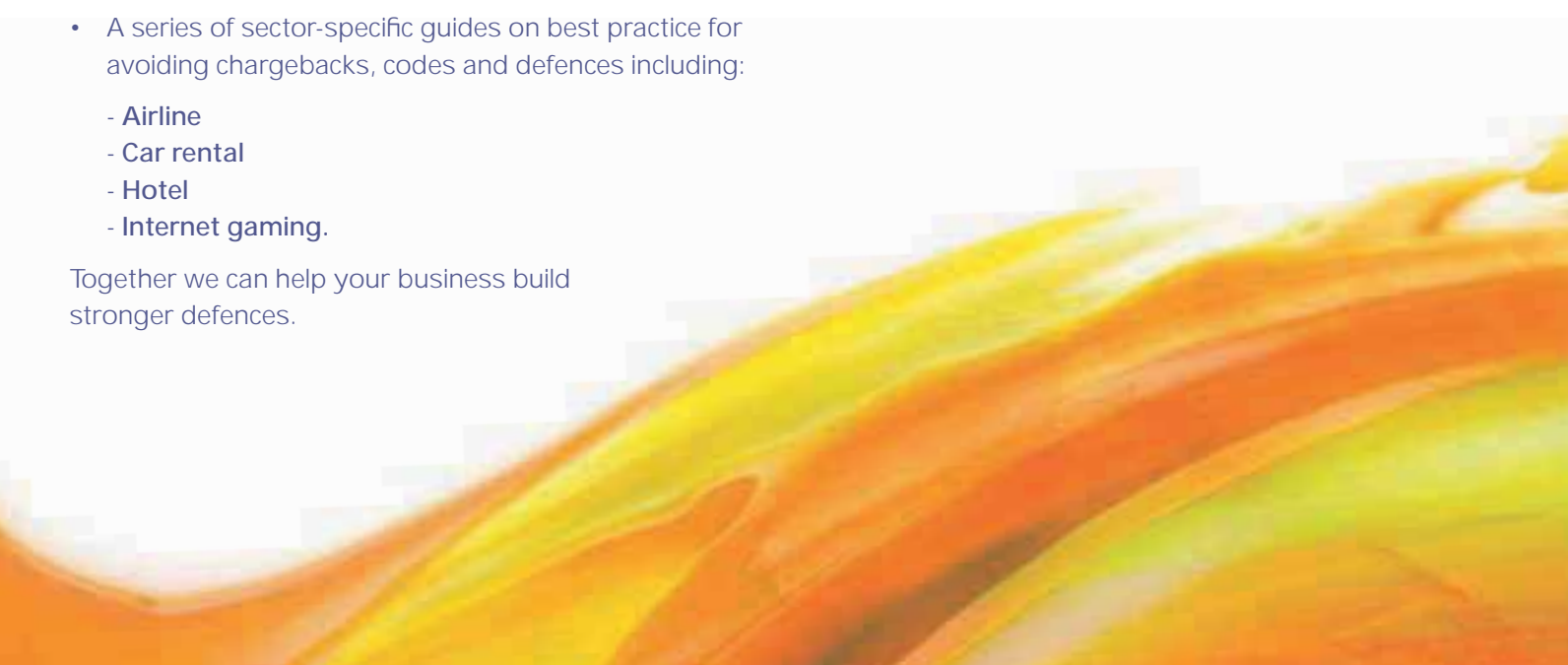
need further help?

This guide is just one in the series we've developed to help you better understand what chargebacks are, why they occur and what you can do to reduce their impact on your business. More detailed guides are available.

Other guides available include:

- **"don't lose out"** – A guide to preventing chargebacks on Cardholder present transactions

- **"be prepared"**– A guide to preventing chargebacks on card not present transactions

- A series of sector-specific guides on best practice for avoiding chargebacks, codes and defences including:

  - **Airline**
  - **Car rental**
  - **Hotel**
  - **Internet gaming.**

Together we can help your business build stronger defences.

glossary

Listed below is a summary of the terminology which you may hear or see quoted in documentation.

Acquirer

The financial institution that provides card processing services to the merchant.

Cardholder

The owner of the card used to make a purchase.

Card Issuing Company/Issuer

The financial institution that issued the credit or debit card to the cardholder.

Card Scheme

A network such as Visa, MasterCard, Amex, Maestro etc that acts as a gateway between the acquirer and card issuer for authorising and funding transactions.

Card Scheme Rules/Regulations

Rules set by the Card Schemes, that all card issuers and acquirers must adhere to.

Merchant

The business accepting credit or debit card payments for products or services sold to the cardholder.

Representment

The process used by the acquirer to return the chargeback to the card issuer with information to defend the dispute.

This document is available in large print, Braille and audio
by calling **0844 811 6666**.*

*For BT business customers, calls will cost no more than 5p per minute, minimum call charge 5.9p (current at
April 2010). The price on non-BT phone lines may be different. Calls may be recorded and/or monitored.

www.barclaycard.co.uk/business/existing-customers/chargebacks

Visa Account Updater For Issuers

Increase Revenue, Enhance Cardholder Convenience and Lower Customer Service Costs

Issuer Benefits

- Maintains continuity of payment relationships by reducing the opportunity to switch payment method or cancel the service when account information changes.

- Helps achieve deeper penetration into the account-on-file segment, including the $2.2 trillion* bill payment segment.

- Improves customer service by minimizing declined transactions and increasing authorization approvals.

- Can increase revenue by minimizing customer switching of payment choice, thereby saving the revenue stream from recurring transactions.

- Helps decrease expenses by avoiding extra cost of processing declines, chargebacks and customer service.

- Helps reduce impact of card upgrades and helps to retain customers by making payments with Visa more convenient.

Visa® Account Updater (VAU) enables the electronic exchange of updated account information among participating merchants, acquirers and Visa card issuers.

Serving as an automated, dedicated and secure clearinghouse, VAU delivers updated cardholder account information in a timely, efficient and cost-effective manner, benefiting acquirers, merchants, issuers and cardholders.

VAU makes it easier for issuers to retain cardholders by maintaining continuity in the payment relationship after account information changes occur. Using a secure protocol, issuers submit updated information to VAU. The updates are made available to acquirers quickly and cost-effectively. Acquirers request account information on behalf of their enrolled merchants, then forward it on to them.

For merchants that maintain customer account information on file—like recurring and auto bill payment providers, subscription services, certain online merchants and preferred customer travel and entertainment programs—VAU makes accepting Visa an even more attractive option. At the same time, it increases the authorization approval rates while decreasing costs caused by outdated account information.

The Value of VAU

VAU helps avoid disruption in customer relationships and recurring payments due to Visa account information changes. Account-on-file cardholders are among an issuer's most valuable customers. By committing to use their accounts regularly, they provide an issuer with a dependable revenue stream, and are less likely to close their accounts over time.

On average, 30 percent of accounts incur a change to an account number or expiration date, or they are closed every year. When cardholders are inconvenienced—especially by unpredictable changes such as product upgrades and lost or stolen card replacements—they may not update all of the merchants with whom they have ongoing relationships. Consequently, account-on-file merchants continue to bill using out-of-date information, resulting in declined transactions and extra costs. In addition, when they contact the cardholder for updated information, they run the risk of payment switching or service cancellation.

* See back for details.

VISA

Cardholder Benefits

- Offers a seamless account update process.

- Provides uninterrupted service from participating merchants.

- Reduces negative experiences caused by declines.

- Does not require cardholder action to communicate changes to participating merchants.

VAU provides updated account information to merchants so that recurring transactions can continue without interruption. It is used prior to an authorization attempt and does NOT replace or alter normal authorization rules. The service simply enables higher probability of authorization approvals for non-credit-related decline reasons.

VAU creates value for all parties in the payment process.

How VAU Works

Issuers and acquirers must meet VAU service participation requirements. Acquirers can only enroll merchants who have been individually evaluated and qualified by Visa.

Issuers submit electronic updates to VAU when a cardholder's account information changes due to a product upgrade, a portfolio conversion, card expiration, loss or theft, account closure or other reasons, such as combining accounts after marriage. VAU handles any risk or unique privacy situations using a "contact cardholder" notice.

Through their acquirers, enrolled merchants submit inquiries regarding accounts with which they have ongoing relationships. VAU processes inquiries against its database and provides responses to the acquirer. Visa will only respond to specific data elements within an inquiry file from a preregistered merchant. Responses include account number or expiration date updates, closed account advices and contact cardholder advices. The acquirer forwards the responses to the requesting merchants, who must then update on-file accounts *before* requesting an authorization.

Account-On-File Merchants — Preferred Customers — Online — Recurring Payments — Travel Agents Fast Check-In — INQUIRIES — Account Inquiries — Account Updates — **VISA** ACCOUNT UPDATER — UPDATES — Account Info Refresh
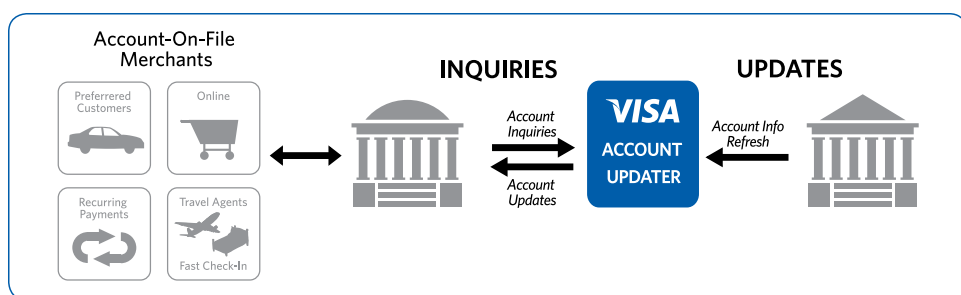
For More Information

- Contact your Visa Account Executive; or

- Call Visa Customer Service at **1-888-847-2242**; or

- Email the Visa Account Updater Product Office at **updater@visa.com**.

- Issuers and acquirers can visit Visa Online at **www.us.visaonline.com** in the U.S. or **www.visainfo.ca** in Canada.

All VAU data is transmitted through a secure direct connection between the endpoint and Visa via Open File Delivery (a component of Visa's Direct Exchange) or the Visa File Exchange Service. VAU information is stored in a database inside Visa's firewall, and browsing access is not allowed.

VAU provides daily and monthly management reports to both issuers and acquirers. Report delivery and access varies by each region. See the VAU Implementation Guide for details.

TYPES OF VERIFICATION MEASURES THAT CAN BE USED BY SERVICE USERS TO HELP TO VERIFY CUSTOMER DETAILS FOR THE PURPOSE OF ACCEPTING DIRECT DEBIT AS A PAYMENT MECHANISM

Please note – the following is not a definitive list and service users may therefore have identified other, equally acceptable, mechanisms for verifying customer details. The sponsoring bank is required to approve any additional mechanisms identified after ratification by Bacs Payment Schemes Ltd. This list should not be read or understood as being, in any way, an endorsement or recommendation by Bacs Payment Schemes Ltd of the suppliers or products named and is current at time of production.

Method	Comments / Availability	Brief Description	Name	Address	Account Details
Know Your Customer (KYC) Identity Checks	These measures would fit best with face to face sign up method				
Passport			x		
Driving Licence			x	x	
Household bill e.g. 2 household bills dated within 3 months			x	x	
Bank Statement			x	x	x
Tax Bill / Notification of Tax code			x	x	
Birth Certificate			x		
Data Checking and Database maintenance products	There are a number of useful databases and packages available, which are continually updated and allow Service users to check details in real time				
Electoral roll		A useful tool for verifying name and address details	x	x	
Identity Check – offered by Experian	www.experian.co.uk	Can be used where there is a risk of identify fraud and can determine whether the customer exists by using independent data sources to confirm the information provided. These checks can provide greater assurance that the customer is who they say they are.	x		

GB Accelerator	www.gb.co.uk	A data capture software package that references sources of information on UK individuals and households from the National Register, which includes the UK Electoral Roll, Royal Mail Postcode Address File (PAF) and BT database.	x	x
CIFAS – UK Fraud Prevention Service	www.cifas.org.uk	A UK membership based fraud prevention data sharing scheme pooling information on fraud and attempted fraud.	x	
The Bereavement Register (TBR)	www.the-bereavement-register.org.uk	TBR is compiled from information volunteered by the family and friends of the recently deceased, containing in excess of 2.8 million records. The Bereavement Register (TBR) was launched in February 2000 as a service to the consumer to ensure the prompt removal of a deceased's details from the databases of direct mail companies. The file is updated on a monthly basis and grows by approximately 30,000 records per month.	x	
Mortascreen	www.mortascreen.co.uk	Containing over 5 million records, the Mortascreen file has a range of new data sources, including information previously directed to The Bereavement Register. It incorporates probate records, obituary notices, Royal Mail returns marked "Deceased", website notifications and data from freepost cards issued at local Register Offices. Mortascreen holds information dating back to 1988 and receives up to 40,000 new records every month. Both Mortascreen and the Bereavement Register enable Service Users to protect themselves against identity fraud. They are managed by the Read Group and are also available from a number of affiliate organisations.	x	
Directory enQuiry Record (DQR) – Telephone Number Verification		Can be used by Service Users to verify and validate incorrect or potentially fraudulent applications by checking the phone number, before the standard DDI application procedure starts. In addition, this service can be used to verify or append a telephone number to an address, compensating for missing, mis-keyed or out of date records. The release of ex-directory details and Directory enQuiry Record (DQR) data, means that Service Users can use software packages that can also identify households with ex-directory numbers and through DQR provide an increase of up to 5% of standard telephone append results. This service now covers 90% of UK households, making this a very complete and up to date source of name address and telephone number data. This will assist in customer identification and there are a number of organisations that can supply this service.	x	x
Deduping services – to detect & flag duplicates in your database	Available from a number of companies	Packages that will detect and flag duplicates in data. For Paperless Direct Debit Service Users, identifying matching details could help to reduce identity fraud i.e. by picking up multiple names at the same address. At the lowest level, it will detect and flag duplicated	x	x

		individuals, at the second level it will flag family matches where it finds two or more records for the same family group (at the same address). Finally, at level three, it will flag households, where individuals, not necessarily with the same family name, share an address. These services are available from many organisations.		
Gone Away suppression (GAS)	Compiled by the Read Group and available from a number of affiliate companies	A key source of information regarding home movers in the UK and consists of over 12 million records, updated every quarter. The recently included Universal Suppression Service expands the suppression capabilities of software packages with access to an additional 6.5 million gone-away records.	x	
National Change of Address File (NCOA)	www.ncoa.co.uk	Enables Service Users to identify home-movers on their database by screening records against the Royal Mail National Change of Address (NCOA) file. NCOA processing can provide new addresses where available or can be used in reverse to trace and confirm previous addresses. The NCOA can assist in ensuring that goods are supplied to the correct address and is available from the Royal Mail and a number of affiliate companies.	x	
Bank Wizard Absolute	www.experianpayments.com	A unique real-time verification service that confirms the connection between customers and their bank account details by comparing a customer's information with that held by their bank, reducing the risk of misapplied payments and fraud.	x	x	x
DD-iD (Direct Debit Limited)	www.directdebit.com	A unique electronic service that is able to algorithmically crosscheck the key databases against an individual's identity. Flexible levels of risk checking are available to fit business process and meet scheme compliance.	x	x	x
VALIDATE - ID	www.bemac.com	Real time validation of customer's bank details and verification of customer's identity and address, utilising information from UK's leading credit reference agencies. Plug & Play API for integration to CRM, significantly minimising the risk of payment fraud, payment rejections and misapplied payments.	x	x	x
SAVS	Available from a number of companies	Address Validation Service from SmartAuth that checks validity and format of addresses.	x	
Quick Address (uses Postcode Address File to capture address details)	www.qas.com	Ensures that consumer or business name and address data is captured accurately at source, improving business efficiency and customer service and reducing wasted costs.	x	
Postcode Address File (PAF)	Available from a number of companies	Setting up new Payer details requires more than just a sort code and account number. Address details need to be checked for future correspondence including	x	

		confirmation of DDI set up and any advance notice requirements. There are 26.5 million addresses held on the Postcode Address File (PAF); the source of UK postcodes, and this file is constantly changing. Service Users therefore need to regularly cleanse their data against PAF. This validation method will assist in providing reliable address details, which will help to establish customer identity. Other benefits include the provision of addresses in a consistent format, the ability to correct historical address records and turn them into useable data and reliable database analysis. The PAF is supplied by the Royal Mail and a number of affiliate companies.			
Other					
Deposit – Sometimes taken as additional security			x		x
– Credit Card check via Streamline – Debit Card via POS	www.streamline.com/				x
Check existing records			x	x	x
Cheque obtained from bank account			x		x
Validation / Verification of Account and / or Sort Code Details					
Bank Wizard	www.experianpayments.com	A comprehensive bank account validation software and service, which includes checking of account numbers, bank sort codes and Building Society Roll and Reference Numbers.			x
Account Checker	www.directdebit.com	Validates Bank and Building Society sort code data			x
Modulus checking	Further details available from servicedesk@bacsservices.co.uk	Tables confirming that the account number quoted is valid for the accompanying sort code. (They do not verify that the account is correct for the named beneficiary). Available in printed form with a data table on diskette, or incorporated in payment software packages			x
Transposing e.g. 9, 10 & 12 digit account numbers	Available from a number of companies	A number of account numbers and sort codes need to be transposed from the form in which they are issued to the payer into the form required for the processing of the payment, either by Direct Debit or Bacs Direct Credit.			x
ISCD	Further details available from servicedesk@bacsservices.co.uk	A data file of valid bank and building society sort codes, which are regularly updated and can be incorporated in payment systems. All Bacs approved software packages include this validation.			x
Crediting and Debiting Building Society Account Numbers	Available from http://www.bacs.co.uk/bacs/businesses/resources/subscriber+library/	This guide helps Bacs service users address Direct Credit and Direct Debit payments to building society accounts with nonstandard account details. To help service users, this guide also includes former building			x

		societies with nonstandard accounts.			

Paperless Direct Debit

An introduction to the service

Contents

An introduction to Paperless Direct Debit

Direct Debit has long been recognised as the simplest and most cost-effective way to collect payments. Now it's even easier to sign up customers to the service.

AUDDIS service users can now sign up customers to Direct Debit using the telephone, the Internet, telephone keypad, face-to-face or interactive TV, without the payer having to sign a paper DDI, subject to the conditions in section 16 of 'The Service User's Guide and Rules to the Direct Debit Scheme'.

Purpose

The purpose of this guide is to introduce Paperless Direct Debit and outline the requirements for its operation. The Rules are mandatory and no departure from them is allowed. If a service user fails to adhere to these Rules, the sponsor has the right to remove that service user from the Direct Debit Scheme.

Rules

A full copy of the Rules for Paperless Direct Debit is included in section 16 of 'The Service User's Guide and Rules to the Direct Debit Scheme' and must be read in conjunction with this document. If you are in any doubt, please contact your sponsor.

The advantages of Paperless Direct Debit to businesses and organisations are clear:

- By offering Paperless Direct Debit sign-up at 'point of sale', you can eliminate much of the paperwork, delay and postage costs associated with setting up Direct Debits

- By applying modulus checking at 'point of sale' (mandatory for PDD service users), you can ensure that customer bank and building society details are taken much more accurately, therefore eliminating later costly administration problems

- You can begin the collections process earlier, as you don't need to wait for the payer to complete and return the Direct Debit Instruction

- Telesales techniques can help increase sales conversions

- You will be offering an improved quality of service to your customers, offering them 'online sign-up', in line with many large organisations who already offer this service.

Paperless Direct Debit is also better for your customers:

Customers have the same benefits which apply to normal Direct Debit sign-up. There are no changes to the three main safeguards – an immediate refund in the event of an error, normally 10 working days advance notice of the account being debited and the right to cancel at any time.

- Consumer protection is maintained through the Direct Debit Guarantee

- Increased simplicity and convenience for the payer, with no forms and no delays.

Making the most of Paperless Direct Debit

Planning and developing a successful telemarketing programme needs care and attention if it is to succeed, whether it's by telephone, internet, telephone keypad, face-to-face or interactive TV. The purpose of this guide is to help your organisation achieve that.

The suggestions in this booklet have been designed to ensure the highest quality standards and best practice in relation to Paperless Direct Debit service quality.

It includes sample telephone or on-line marketing scripts and screens which you can use or modify to suit your business or organisational needs around key elements such as the Direct Debit Guarantee offered through the Direct Debit Scheme. The approval of your sponsor must always be gained before use.

If Paperless Direct Debit sign-up is being outsourced, there must be an automated link between the service user and the outsourcing agent. This will protect against incorrect re-keying of information and therefore eliminate discrepancies in key fields, i.e. payer's sort code, account number, name and will ensure compliance with the AUDDIS Rules.

Other Direct Debit marketing material referred to in the guide is available on request from your Sponsor.

How to become a Paperless Direct Debit service user

Becoming a Paperless Direct Debit service user can be achieved by completing the following steps:

1. Service users must have live AUDDIS status before they can begin using the Paperless Direct Debit service, but, they can apply at the same time their AUDDIS application is made.

2. Complete the AUDDIS and separate Paperless Direct Debit application form issued by your sponsor.

    a) A service user wishing to join the Paperless Direct Debit Service must apply to its sponsor who will assess the application. The service user must complete a separate application for each SUN. Authority to begin Paperless Direct Debit sign-up will only be given when, and if, the sponsor is satisfied that the service user meets the requirements of these Rules. A service user can only use the Paperless Direct Debit sign-up method authorised by its sponsor. If additional methods are required the service user must make a subsequent application to its sponsor.

    b) If the Paperless Direct Debit form is submitted with an AUDDIS application, the AUDDIS timescales will be applicable. Service users will be allowed to join the Paperless Direct Debit service on their AUDDIS joining date, providing they have met all the criteria.

3. Your sponsor will require certain criteria to be met for AUDDIS and Paperless Direct Debit. These must be met before your application is signed off for live running e.g. vetting criteria which will include technical, financial checks and the execution of a new Indemnity, if the original Indemnity was signed prior to 1.1.2004.

4. Ensure that system amendments for AUDDIS incorporate Paperless Direct Debit requirements.

5. Prepare an AUDDIS migration plan if applicable, detailing the various Bacs testing requirements.

6. Your sponsor must approve all Paperless Direct Debit material, including scripts, confirmation letters, internet screens, and all other material prior to use, and must authorise any subsequent changes.

7. Prepare staff training and briefings incorporating Paperless Direct Debit. This is essential to avoid wrong messages being given out by staff and to maintain the quality of the Direct Debit Scheme (refer to training on page 14).

8. Consider a phased roll out if there are several different applications involved. One type of application per SUN is recommended in order to better control and manage Paperless Direct Debit operations.

9. Set up the appropriate monitors and apply measures to establish the level of service, i.e. number of sign-ups, number of cancellations following confirmation letters, number of unpaids and number of queries.

   This will not only help ensure your service is acceptable, but also highlight areas for improvement.

10. Service users should have a method of confirming the Paperless Direct Debit sign- up, such as voice recording. This will assist service users when dealing with customer queries.

The marketing of Paperless Direct Debit

The following sign-up scripts have been developed to keep the marketing of Paperless Direct Debit as simple and effective as possible.

If you are selling goods or services by telephone, this script can be added at the end of the sale. If you are using the internet, you can use this script as the basis for a series of screen prompts and dialogue boxes.

If you are trying to convert existing customers to Direct Debit, you will need to prepare an opening script or screen which introduces the subject of Direct Debit as an easier way to pay regular or irregular payments.

Include the core benefits of paying by Direct Debit for your customers:

• It is less expensive than paying by cheque – for example, there are almost no stationery or postage costs

• It saves time – no cheques to write and post, or envelopes to find

• It reduces the possibility of forgetting to pay

• It is the only payment method with a money-back guarantee

• The payer retains control – with advance notice, a choice of payment dates in most cases and they can cancel at any time

• It makes paying large bills more affordable by spreading the payments

In addition, if you are offering any incentives or discounts for Paperless Direct Debit, you should include these in this section of your script or on-screen information.

Suggested outline of Paperless Direct Debit script

This script is a guide for Paperless Direct Debit transactions. It can be adapted to suit a business or an organisation's needs, but it must be approved by the service user's sponsor prior to use. It is to be used for telephone, telephone key pad and face-to-face applications. The following are mandatory inclusions:

- Verification that the customer is the account holder and therefore the payer. If the customer is not the account holder a paper DDI must be sent to the payer for completion. A list of verification measures to assist in verifying the payers details is available from http://www.bacs.co.uk/Bacs/Businesses/Resources/SubscriberLibrary/Pages/default.aspx

- Taking the payer's bank or building society account number, sort code and account name

- Confirm that the person entering into the transaction is the only person required to authorise debits from the account. If more than one person has to authorise debits from the account a paper DDI must be sent to the payer for completion

- Advice of the advance notice period

- Confirmation of bank details back to the payer

- An explanation of the Direct Debit Guarantee – this must be provided in full if the payer confirms they require this

- Advice of the company name that will appear against the Direct Debit on the payer's bank statement

- A service user who is unable to lodge the DDI within 10 working days of the Direct Debit set-up must advise the payer that the Direct Debit will not be set up on their bank account until XXXX (depending on when the service user will lodge the DDI). However in all circumstances the service user must transmit the DDI no later than 6 months from the date of set-up. The payer must still be sent confirmation of the Direct Debit details within 3 working days. Failure to lodge the DDI within these timescales may result in increased instances of rejected DDIs.

Best practice standards

It is recommended that branch address details are confirmed back to the payer.

NB. Branch address details in service user software may differ to those provided by the payer e.g. Service centre details i.e. a centralised or part centralised processing location.

Assuming the payer has agreed to buy and asks, for example, to pay by monthly Direct Debit and the monthly amount to be debited has been agreed.

OK thank you. To avoid delay and to save you having to fill in any paperwork I can set up your Direct Debit Instruction right now over the phone. Would that be helpful?

Payer agrees.

Please can you confirm that you hold a UK bank / building society account and you are the account holder?

If no, seek another method of payment.

If yes, proceed.

Can I confirm that you are the only person required to authorise debits from this account?

If more than one person is required to authorize debits on the account, issue a paper DDI and close call.

If OK, capture bank details.

Can you confirm the name of the account you wish to be debited?

Take details.

Can you confirm the branch sort code of the account you wish to be debited?

Take details (if unsure direct caller to cheque book).

Can you confirm the account number of the account you wish to be debited?

Take details (if unsure direct caller to cheque book or bank statement).

Ask if they have used this account to make Direct Debit payments before as some banks or building societies may not accept Direct Debits for certain types of account.

Apply modulus checking.

Let me just confirm your account details back to you.

The account name is XXXXXX, is this correct?

Payer confirms.

The account sort code is XX-XX-XX, is this correct?

Payer confirms.

The account number is XXXXXXXX, is this correct?

Payer confirms.

We've agreed that the monthly amount will be £_____, but is there a particular day of the month you would like the money to come out of your account, for instance just after you're paid?

If no preference is given, agree on the most suitable day for the service user.

The first collection will come out of your account on DD/MM and on the same day each month (depending on the frequency agreed) thereafter.

The company name that will appear on your bank statement against the Direct Debit will be XXXXXX. That's it you have set up your Direct Debit Instruction with us. You will be sent confirmation of this in the post within 3 working days of this phone call.

Or (if incorporating the advance notice with the confirmation letter)

The company name that will appear on your bank statement against the Direct Debit will be XXXXXX. That's it you have set up your Direct Debit Instruction with us. You will be sent confirmation of this no later than 10 working days before the first collection. (Service user must ensure that the Direct Debit collection date is within the following 4 weeks, otherwise they must issue the confirmation letter within 3 working days as above.)

All Direct Debits are protected by a guarantee. I can read it to you now or you can read it in our confirmation letter, which would you prefer?

If answer is 'YES' read it now, continue.

If the caller does not wish to hear the guarantee go to the end.

In the future if there is a change to the date, amount or frequency of your Direct Debit, we will always give you X working days notice in advance of your account being debited. In the event of an error, you are entitled to an immediate refund from your bank or building society. You have the right to cancel at any time and this guarantee is offered by all the banks and building societies that accept instructions to pay Direct Debits. A copy of the safeguards under the Direct Debit Guarantee will be sent to you with our confirmation letter.

That completes the setting up of your Direct Debit Instruction. Thank you very much for your time today. Goodbye.

If the payer already has a Direct Debit with the service user or is buying multi products i.e. gas and electricity, then the script does not have to be repeated. However, it must be made clear to the payer, how many Direct Debits are being set up, the references and the fact that the Direct Debits will be taken from the same account.

If the payer asks how is it possible to set up a DDI over the phone.

We have recently started using an enhanced service provided by the banking industry so we are able to set them up over the telephone. All the normal safeguards of the Direct Debit Guarantee still apply and we will always confirm the content of these calls to you in writing.

If the payer would prefer to use the post and receive a paper instruction for completion and return.

I can do that for you. Is there a particular concern that you have with setting up the Direct Debit over the phone now?

If the payer would still prefer to use the post.

I can send you the forms in the post or, if you prefer, you can call back later. All the information you need to set up a Direct Debit Instruction is on your cheques.

If the payer is not the account holder.

As you are not the account holder, we will need to send the account holder a Direct Debit Instruction to complete and return. Can I confirm the address to send this to?

If the payer says he is concerned over the security of information.

I can understand that, but I can assure you that all information is retained in the strictest confidence. In the event that you have any queries or dispute an entry on your bank account you can of course rely on the Direct Debit Guarantee. Does that ease your concerns enough to want to go ahead now?

Yes – continue with script.

No – payer wants information in the post, check details and close politely.

If the payer says he is concerned over mistakes being made.

I understand your concern and to reduce customers' concerns a number of measures are in place to safeguard against genuine mistakes. There is the Direct Debit Guarantee. Firstly, if at any time money is debited from your account incorrectly the banks and building societies guarantee to refund it. Secondly, no changes to the date, frequency or amount debited can be made without notifying you normally at least XX working days in advance of your account being debited. And finally, you have the right to cancel any Direct Debit at any time simply by writing to your bank or building society, with a copy to us. A copy of these safeguards will be included in our confirmation letter.

Does that answer your concerns sufficiently for you to want to go ahead with the Direct Debit set-up now?

Yes – continue with script.

No – payer wants information in the post, check details and close politely.

Suggested outline of internet Direct Debit script

The following are suggested screen prompts for customers accessing an internet site for Direct Debit sign-up. Service users may be working with internet agencies or other experienced web professionals, but if not, they should use these scripts verbatim. All service users must include the following mandatory items within their screens.

- SSL server security must now be present and be a minimum of 128 bit

- A postal and email address must be provided to the payer

- A general enquiries / customer service contact number must be given to assist the payer if he has any urgent issues or a complaint to raise

- The information required to complete the on-screen DDI does not need to be captured directly onto the on-screen DDI, but once completed a copy of the DDI complying with the mandatory format in section 16.11 must be displayed and available for printing by the payer

- Verification that the customer is the account holder and therefore the payer. If the customer is not the account holder a paper DDI must be sent to the payer for completion or a copy must be available for printing, see section 16.12. A list of verification measures to assist in verifying the payers details is available from http://www.bacs.co.uk/Bacs/Businesses/Resources/SubscriberLibrary/Pages/default.aspx

- Taking the payer's bank or building society account number, sort code and account name

- Confirm that the person entering into the transaction is the only person required to authorise debits from the account. If more than one person has to authorise debits from the account a paper DDI must be sent to the payer for completion or a copy complying with the mandatory format in 16.12 must be available for printing by the payer

- Confirmation of bank details back to the payer.

NB. Branch address details in service user software may differ to those provided by the payer e.g. Service centre details i.e. a centralised or part centralised processing location.

- Advice of the advance notice period*

- Advice of the company name that will appear against the Direct Debit on the payer's bank statement*

- An explanation of the Direct Debit Guarantee or a copy of the Guarantee, as shown in section 16.11

*Strongly recommended but not mandatory if a copy of the Guarantee is being provided, see above.

- A service user who is unable to lodge the DDI within 10 working days of the Direct Debit set-up must advise the payer that the Direct Debit will not be set up on their bank account until XXXX (depending on when the service user will lodge the DDI). However in all circumstances the service user must transmit the DDI no later than 6 months from the date of set-up. The payer must still be sent confirmation of the Direct Debit details in the post within 3 working days. Failure to lodge the DDI within these timescales may result in the DDI being rejected.

Example script

Assuming the payer has agreed to buy and asks, for example, to pay by monthly Direct Debit and the monthly amount to be debited has been agreed.

Stage one: Opening

Direct Debits can now be set up on-line or over the telephone in addition to the original postal method.

All the normal Direct Debit safeguards and guarantees apply. No changes in the amount, date or frequency to be debited can be made without notifying you at least XX working days in advance of your account being debited. In the event of any error, you are entitled to an immediate refund from your bank or building society. You have the right to cancel a Direct Debit Instruction at any time simply by writing to your bank or building society, with a copy to us.

Stage two: Sign up of bank details

In order to set up your Direct Debit Instruction on-line you will need to provide the following information through the setting up procedure (your cheque book contains all the bank details that you require):

- Bank or building society name and account number, sort code and branch address.

- If you are not the account holder, a paper Direct Debit Instruction will be sent for completion. Please click to end

- If this is a personal account continue with the set-up procedure

- If it is a business account and more than one person is required to authorise debits on this account, a paper Direct Debit Instruction will be sent to the payers for completion. Please click to end.

Alternatively you can print off your on-screen Direct Debit Instruction and post it to us. If you are unable to print please contact us on XXXXXX (tel no) and we will post you a paper Direct Debit Instruction.

If you do not wish to proceed any further please click to END.

The details of your Direct Debit Instruction will be sent to you within 3 working days or no later than 10 working days before the first collection.

Click the mouse on YES or NO to confirm details:

YES (onto next stage)

NO (redo form)

CANCEL to stop the set-up procedure (go back to start page).

Stage three: Reconfirming the details to the customer

These are the details that you have entered to set up the

Direct Debit Instruction:

Name of account holder

Branch sort code /__ __/__ __/__ __/

Bank account number   /__/__/__/__/__/__/__/__/

Amount to be debited from bank account (if known) £__/__/__/__/__/__/__/__/__•__/__/

Date each month for collection (or other collection frequency) /__/__/

The company name which will appear on your bank statement against the Direct Debit will be XXXXXXXX.

Click mouse on YES or NO to confirm details:

YES (onto next stage)

NO (redo form)

CANCEL to stop the set-up procedure (go back to start page).

Stage four: Address for the letter of confirmation

Your Direct Debit Instruction will be confirmed to you by e-mail within 3 working days. Alternatively the confirmation letter incorporating your advance notice will be received by you no later than 10 working days prior to the first collection date. If you prefer to receive this by post please indicate the address you would like this to be sent to.

Click for next stage (stage five)

Stage five: Completing the sign up

That completes the setting up of your Direct Debit Instruction and the confirmation of the instruction will be sent to you within 3 working days or be received by you no later than 10 working days before the first collection.

Thank you very much for your Direct Debit Instruction details. Here is the Direct Debit Guarantee for your information. (Direct Debit Guarantee appears on-screen).

Company Name
Company Address

Instruction to your Bank or Building Society to pay by Direct Debit

DIRECT Debit

Name(s) of Account Holder(s)

Bank/Building Society Account Number

Branch Sort Code

Name and full postal address of your Bank or Building Society

To: The Manager   Bank/Building Society

Address

Postcode

Service User Number

Reference Number

Instruction to your Bank or Building Society
Please pay (insert Company Name) Direct Debits from the account detailed in this Instruction subject to the safeguards assured by the Direct Debit Guarantee. I understand that this Instruction may remain with (insert Company Name) and, if so, details will be passed electronically to my Bank/Building Society.

Date

Day / Month / Year

Banks and Building Societies may not accept Direct Debit Instructions for some types of account

SUBMIT   CLEAR

To be printed off by customer, completed and returned to the service user. The Direct Debit Guarantee to be retained by the payer.

The Direct Debit Guarantee

DIRECT Debit

- This Guarantee is offered by all banks and building societies that accept instructions to pay Direct Debits

- If there are any changes to the amount, date or frequency of your Direct Debit (insert your organisation name) will notify you (insert number of) working days in advance of your account being debited or as otherwise agreed. If you request (insert your organisation name) to collect a payment, confirmation of the amount and date will be given to you at the time of the request

- If an error is made in the payment of your Direct Debit, by (insert your organisation name) or your bank or building society, you are entitled to a full and immediate refund of the amount paid from your bank or building society

  - If you receive a refund you are not entitled to, you must pay it back when (insert your organisation name) asks you to

- You can cancel a Direct Debit at any time by simply contacting your bank or building society. Written confirmation may be required. Please also notify us.

Please fill in the whole form using a ball point pen and send it to:

Company Name

Company Address

Name(s) of Account Holder(s)

Bank/Building Society account number

Branch Sort Code

Name and full postal address of your Bank or Building Society

To: The Manager   Bank/Building Society

Address

Postcode

DIRECT Debit

Instruction to your Bank or Building Society to pay by Direct Debit

Service User Number

Reference

Instruction to your Bank or Building Society
Please pay (insert Company Name) Direct Debits from the account detailed in this Instruction subject to the safeguards assured by the Direct Debit Guarantee. I understand that this Instruction may remain with (insert Company Name) and, if so, details will be passed electronically to my Bank/Building Society.

Signature(s)

Date

Banks and Building Societies may not accept Direct Debit Instructions for some types of account

Suggested outline communications plan for service users

To ensure that customers receive the right advice, it is vital that all your staff are fully informed of the correct procedures for Paperless Direct Debit as set out in section 16 of 'The Service User's Guide and Rules to the Direct Debit Scheme'.

Internal communications

Around three months or more ahead of the launch of your new service, it's helpful to draw up a list of key activities.

Why not create a special identity for all communications and activities regarding Paperless Direct Debit?

This will have the benefit of making what you say instantly recognisable and will improve the quality of what you say. For instance, all communications could be on special paper, should feature the Direct Debit logo and maybe a character or symbol of your choice.

- Staff briefing, to cover WHAT the product is offering, WHY it has been introduced and HOW it will benefit customers and staff alike. The latter is particularly important as staff have to be enthusiastic about Paperless Direct Debit in order to sell the product to customers and to provide them with reassurance. It is important that a correct allowance is made to telephone sales people to encourage them to sign-up Paperless Direct Debit

- Make sure management cascade the briefing to all staff via team meetings or other company communication channels

- Prepare and issue a sales guide or aide memoire, making it easier for your staff to understand the changes in collections procedures.

Select a company 'Champion' for the new service, possibly a senior manager, to lend extra internal credibility to this new collections process.

- Place information about Paperless Direct Debit in your staff magazine or newspaper

- Post news bulletins on notice boards

- Create a question and answer sheet to prepare staff for any enquiries from customers

- Update your marketing literature to include the offer of the facility.

External communications:

- Include details of the Paperless Direct Debit facility as a standard part of your direct mailings to customers

- Promote the fact that there is now a more convenient way of signing up for a Direct Debit in all advertising and marketing literature.

Use the Direct Debit Champion mentioned earlier in external communications to add further credibility to Paperless Direct Debit.

The key messages that should be put over when discussing Paperless Direct Debit are:

- There are no changes to the three main safeguards of the Direct Debit Scheme – immediate refund in the event of an error, XX working days advance notice of any change and right to cancel at any time. Taking out a Direct Debit Instruction over the telephone, or over the Internet or via other methods is often the quickest and most convenient way of signing up

- In press relations, Paperless Direct Debit should be presented in the context of the telephone or Internet or other methods as being the modern medium for collections

- Customers can, in some cases, have the choice of other payment methods and of waiting for a paper Direct Debit Instruction to be sent if they prefer, although this may delay their application payment or – in the case of insurance – their cover.

Direct Debit training programme

The more your staff understand the benefits of Paperless Direct Debit – and the Direct Debit Scheme in general – the greater your chances of success with your campaign.

The effectiveness of your Direct Debit programme demands a high level of interest and participation from your staff. To achieve this there are a number of training options available. Details of the training courses and their providers can be found at http://www.bacs.co.uk/training

Customers' frequently asked questions about Direct Debit and Paperless Direct Debit

What is a Direct Debit?

Direct Debit is a payment of an agreed amount made from a customer's bank or building society account to a named organisation (the service user) authorised by a Direct Debit Instruction. The amounts and dates may vary, although they are always advised to the payer in advance.

Can I cancel a Direct Debit Instruction?

Yes. Instructions can be cancelled by writing to your bank or building society. A copy to the service user is also very helpful.

What happens if a mistake is made?

If an error is made by the service user or your bank or building society, you are guaranteed a full and immediate refund from your branch of the amount paid.

What happens when the amount or date changes?

You will be notified in writing in advance (normally 10 working days) of the collection allowing you time to query the amount or date if necessary. A Direct Debit Instruction stands until cancelled so there is no new Direct Debit Instruction to sign when the amount or date of collection changes.

If I set up a Direct Debit over the telephone or via the internet, what record will I have of the agreement?

You will be sent written confirmation of your Direct Debit Instruction within 3 working days of the telephone call or other on-line sign-up, or alternatively no fewer than 10 working days before the first collection. Simply check the details and contact the organisation you're paying if you have a query. Regardless of what method of sign up you agree to, you are still covered by the Direct Debit Guarantee.

Does agreeing a Direct Debit Instruction mean that money can be taken out of my account whenever the service user likes?

No. A service user can only collect the amount notified to you, and you will be advised of any change to the date, frequency or amount in writing.

What if I have insufficient money in my account to pay a Direct Debit?

If it is returned unpaid, the Direct Debit will normally be re-presented within a few days.

What sort of account do I need to use Direct Debits?

Most current accounts at banks and building societies can be used to make Direct Debit payments. Some types of account however, do not accept Direct Debits. If you have any doubts, please speak to your bank or building society branch.

Can any organisation collect money by Direct Debit?

No. Banks and building societies only permit organisations with known integrity and sound financial and administrative capabilities to collect money by Direct Debit. These checks are even more stringent in the case of Paperless Direct Debit.

Will I still receive bills or statements?

Yes, but they will only be for information and to check against your bank or building society statement.

M1328/07/09

Recurring Payments
Best Practices
Guide

Table of Contents

Definitions

Recurring Transaction

The Visa International defines a recurring transaction as:

"Multiple transactions processed at predetermined intervals, not to exceed one year between transactions, representing an agreement between a Cardholder and Merchant to purchase goods or services provided over a period of time."

Key components to this definition include:

▶ Cardholder establishes a relationship with a merchant to receive ongoing services or goods until the contractual arrangement is cancelled

▶ Cardholder gives permission to the merchant to bill his account on a recurring basis

▶ Transaction amount may be a fixed amount or may vary with each billing

▶ Payment relationship consists of more than the initial transaction, with future payments occurring on a regular cycle not to exceed twelve months

Installment Transactions

Installment transactions are often confused with recurring transactions. Visa International defines an installment transaction as:

"A single purchase of goods and services billed to an account in multiple segments, over a period of time agreed between a Cardholder and Merchant."

The distinction between the two transactions is that, a recurring transaction is payment for goods or services that are received over time, however, an installment transaction represents a single purchase, with payment occurring on a schedule agreed by a cardholder and merchant.

Recurring Payment Indicator

Visa has improved the identification of recurring transactions within the authorization and settlement messages to facilitate more accurate decision-making by Issuers and recognition by Cardholders. Visa requires the Recurring Payment Indicator in all authorization and clearing records. Recurring transactions tend to be low risk than single occurrence card not present transactions, and therefore, should be approved if the account is in good standing.

Cardholder Benefits & Best Practices

Cardholder Benefits

Recurring Payments offer many benefits to cardholders by:

▶ Ensuring timely payments, thereby providing uninterrupted service and elimination of any late payment fees

▶ Eliminating the time and expense associated with initiating manual payments, such as postage expenses

▶ Providing convenience with quick access to billing details and payment options online

Cardholders Best Practices

Cardholders should consider the following when entering into a recurring payment agreement with a merchant:

▶ Advise merchants of any changes to card billing details such as new expiration dates, new account numbers, etc. This will ensure that the services provided continue uninterrupted, and any potential late fees are avoided

▶ Understand the merchant's cancellation policies and method of contacting the merchant

▶ Retain a copy of the payment agreement

Merchant Benefits

Merchant Benefits

▶ Increases customer loyalty

▶ Increases customer service value by facilitating payment convenience

▶ Improves cash flow via timely and regular payment

▶ Reduces cash handling and check management, number of touch points (manual processes)

▶ Eliminates cash handling and check management costs

▶ Improves efficiency

Merchant Best Practices

This section identifies common best practices for merchant who process recurring transactions.

General Practices

The following best practices will help merchants manage recurring transactions effectively:

▶ Allow customers to choose the billing date. This will help ensure that the cardholder's funds are available.

▶ Inform the cardholder the name that will be presented. Ensure that the "Doing Business As" name, or some other name easily recognized by the cardholder is used when billing or corresponding with the cardholder.

▶ Provide a clear statement of the cancellation policy on the cardholder's agreement or merchant website. This will help minimize chargebacks.

▶ Provide the cardholder with clear information concerning the billing arrangements, all charges related to the delivery of goods and services, and merchant contact details for any inquiries or changes to the contract. If billing notification is via online, send a pre-authorization reminder 14 days prior processing event. (see Section 9 for sample template).

▶ Ensure that billing is discontinued immediately upon the cardholder fulfilling the cancellation terms – provide the cardholder with cancellation confirmation including when the last billing will occur if this has not already occurred, or if a credit is due when the credit will be processed. This will help minimize chargebacks.

▶ Ensure that the cardholder is notified when goods or services cannot be delivered or provided on the agreed upon date. This will help minimize inquiries or chargebacks.

▶ Provide cardholder with an easily assessable merchant contact number for customer service

inquiries, and also the right to terminate the recurring transaction

▶ Ensure an authorization request is made for all payments and approved before submitted for clearing

▶ Ensure all transactions reflect the Recurring Payment Indicator

▶ Contact the cardholder to obtain alternative account billing details if the authorization response is a decline.

![VISA]

Merchant Pre- Billing Notification

Merchants who provide this type of customer notification prior to submitting an authorization request for a recurring transaction should see less disputes when done regularly.

Merchant Pre-Billing Notification Sample

To: customer name@account.com **From:** merchant name@account.com

Subject: Recurring transaction notification **Date:** 3 May 2004 03:15:02 -0500

Dear Customer Name,

This email confirms your authorization* of the transaction listed below, entered on 5/3/2004 at 3:14:49 AM has been processed and will be debited from your account.

Transaction Origination Date: 5/3/2004
Name on Account: Cardholder Name
Amount: $14.95
Description: Approved recurring charges on 2004-04-03

*You have authorized Merchant Name Services, Inc and your financial institution to initiate the transaction detailed below. You have acknowledged that the origination of debit or credit transactions to your account must comply with the provisions of local laws. This authorization is to remain in full force and effect until Merchant Name Services, Inc has received written notification from you of its termination in such time and manner as to afford Merchant Name Services, Inc and your financial institution a reasonable opportunity to act on it.

Processed for: Merchant Name Services, Inc
Phone #: 909-832-8879
Email: merchant name@isp.com

The Service User's Guide and Rules to the Direct Debit Scheme

Version 3
December 2007

The Service User's Guide and Rules to the Direct Debit Scheme
Version 3 amendments

A list of the **main** changes to the Service User's Guide and Rules to the Direct Debit Scheme are given below together with changes that will have an impact on Service User's documentation e.g. 'All example forms, letters and reports within the Guide have been replaced to reflect the changes in terminology'. Please refer to the particular section for full details of the changes.

Section	Change
ALL	Name of Guide changed to The Service User's Guide and Rules to the Direct Debit Scheme
Introduction	Notation to advise that terminology within the Guide has been changed from Originator and OIN to Service User and SUN
ALL	All example forms, letters and reports within the Guide have been replaced to reflect the changes in terminology. (See item above)
ALL	Alignment following re-branding from BACS to Bacs and BACSTEL-IP to Bacstel-IP
ALL	Page numbers now run consecutively through the Guide. Section dividers have been removed and sub-sections added to the Contents page.
Various	Changes to web address, Bacs and VocaLink
Various	Advice of effective date when AUDDIS will be mandatory for all new Service Users that submit direct to Bacs
2.6	Advice that use of correction fluid, staples or sellotape on the Indemnity is not permitted
3.2	Notation of additional optional field allowed on the DDI
12.3	Additional text relating to 'Keeping Bacstel-IP software up to date'
15.14	Change to 2nd bullet point relating to AUDDIS users reverting to non-AUDDIS
15.20	Example of 'Request for copy DDI form including Indemnity Claim' deleted
16.10	Additional text advising that a copy DDI must be available for printing

CONTENTS

INTRODUCTION

With effect from December 2007, this document formerly 'The Originator's Guide and Rules to the Direct Debit Scheme', shall be known as 'The Service User's Guide and Rules to the Direct Debit Scheme'. All previous references within this document, to 'Originator' and 'Originator Identification Number' have been replaced with 'Service User' and 'Service User Number' respectively. The example forms contained within this document have been changed to reflect this. Service Users developing new or replacement forms should comply with the guidelines laid down within this document.

This Guide and Rules replaces all previous rules and agreements issued to Service Users but no statement made in this Guide is to be taken in any way whatsoever to prejudice the rights of the Banks under the Direct Debit Indemnity.

- The Rules will evolve over time and will be revised and updated as necessary. It is the Service Users responsibility to maintain updates to the Guide and ensure the latest version of the Rules applying to Service Users are available.

- No departure from the Rules is allowed. If in doubt as to interpretation or application contact your Sponsor.

Purpose

This Guide has been produced to modernise the Scheme, ensure it takes advantage of new business methods, technology and to remove redundant practices.

The intention of this Guide and Rules is to standardise the Direct Debit Scheme and its application for all participants.

The requirements detailed in this Guide are mandatory and will be found in each appropriate section. In order to ensure rule clarity and avoid ambiguity the words 'must' and 'shall' are used in the text.

The Guide is intended for Service Users who are required to apply the Rules of the Direct Debit Scheme and operate within the set procedures as defined.

Reference to Paying Banks' procedures and responsibilities are for the Service User's information. Paying Bank charges for Direct Debit fall within the banker-customer terms and conditions of each Paying Bank and as such are outside the scope of the Direct Debit Scheme

The Direct Debit Scheme may be used only to collect amounts in pound sterling within the United Kingdom (for this purpose this includes the Channel Islands and the Isle of Man).

Conventions

- In this document the term 'Bank' is generally used to include Banks, Building Societies and other bodies participating in the Scheme on behalf of customers. Not all such participants are Banks for the purposes of the Banking Act 1986

- Similarly 'Paying Bank' is used generally to denote a Bank, Building Society or other financial institution to whom Direct Debits may be addressed

- Service Users may be referred to as Originators. Similarly Service User Numbers may be referred to as Originator Identification Number.

- The title 'AN Company Limited', 'FM Client', 'ABC Agency Bank', 'Any Bank Plc', 'ABC Sponsor', and 'A Service User' are quoted as fictitious company names throughout this Guide

How to find your way around the Scheme Rules Guide.

- The Scheme Rules are divided into discrete sections which cover a specific operational aspect of the Scheme.

These sections are listed on the contents page at the beginning of the Guide. It starts with an overview of the Scheme through to becoming a Service User and setting up the Direct Debit Instruction (DDI), to amendments and cancellations and how the Scheme is monitored.

- **Glossary of terms**. Throughout the text, you will see this icon in the right hand margin. The icon signifies that a brief explanation of the word emboldened in the text can be found in the Glossary of terms

- **Cross referencing**. An item or topic in one section may also appear in another section or later in the same section. Where this is considered to be significant, the cross reference appears in the right hand margin of the page.

1 AN OVERVIEW OF THE DIRECT DEBIT SCHEME

Introduction

This section provides a high level overview of the Scheme. It covers the Scheme and its management, how it is controlled, its ownership, how it can benefit the **Service User**, its customers and a brief description of the processes involved.

1.1 The Direct Debit Scheme

The Direct Debit Scheme is an efficient way for organisations to collect regularly occurring payments from large numbers of customers. It is solely a method of collecting payments and the Banks are not responsible for any underlying contracts between the Service User and the Payer.

The Direct Debit Scheme has benefits for all parties concerned in the payment cycle and is therefore growing in popularity with Service Users and customers.

The Scheme is used by insurance companies, charities, local authorities, public utilities, hire purchase companies, building societies, manufacturers, suppliers and a wide range of other organisations which collect large volumes of payments.

Bacs Payment Schemes Limited is the institution responsible for the administration and operation of the Direct Debit Scheme and is owned by the following financial institutions, known as: the Sponsors (Members).

Abbey National plc	Co-operative Bank p.l.c.
Alliance & Leicester plc	Coutts & Co.
AIB Group UK Plc	Lloyds TSB Bank plc
Bank of England	HSBC Bank plc
Bank of Ireland	Nationwide Building Society
Bank of Scotland	NatWest Bank Plc
Northern Bank Limited	Northern Rock Plc
Barclays Bank PLC	The Royal Bank of Scotland plc
Clydesdale Bank PLC	Ulster Bank Limited

1.2 The Benefits of the Direct Debit Scheme

There is now widespread use of Direct Debits – around two thirds of people in the UK pay at least one bill this way and the volume of Direct Debits is growing each year. However Direct Debit not only benefits the bill payer. The Scheme brings considerable cost saving advantages to the payments industry. In this introduction we examine the key benefits of the Direct Debit Scheme for Service Users and **Payers** alike.

The Direct Debit Scheme allows a Payer to authorise regular payments from his bank account. These amounts can vary by amount and date, as long as the Payer has been given adequate Advance Notice.

The benefits for the Service User

- Reduced collection errors leading to better service quality

- Reduced administration costs

- Certainty of payments and improved cash flow

- Increased customer retention

- Increased take-up as costs can be spread across the year.

The benefits for the Payer

- An easy and convenient payment method

- Ensures that payments are made on time

- Direct Debit can help with budgeting by spreading payments over time

- Attracts discounts and incentives from many Service Users

- Guaranteed refund in the event of error.

It is the only payment scheme that protects the interests of the Payer with a guarantee. The **Direct Debit Guarantee** provides assurance to the Payer that any monies debited in error will be immediately refunded by the Payer's Bank. Advance Notice must be given if the terms of the payment change and the Payer may cancel a Direct Debit Instruction at any time.

1.3   Becoming a Direct Debit Service User

With effect from 1st January 2008 it is mandatory for all new Service Users that submit DDI's direct to Bacs to use AUDDIS.

An organisation wishing to join the Scheme should contact its Bank who will advise it of the steps involved in becoming a **Service User**. Its Bank will consider the request to **Sponsor** an organisation as a Direct Debit Service User. The organisation must execute an **Indemnity**, in a prescribed standard form, in favour of all Banks participating in the Scheme.

There are different versions of the Indemnity according to the legal status of the organisation applying to become a Direct Debit Service User.

On acceptance of an organisation's application, a unique **Service User Number (SUN)** is allocated. The Sponsor will provide the Service User with the Rules.

The Scheme is sometimes unsuitable for non-corporate bodies because the Indemnity liability in <u>all</u> such cases falls directly upon individuals without limitation as to time and amount. Under these circumstances it is recommended that you seek legal advice.

The Service User must submit all documentation it intends to use in its Direct Debit operations, to its Sponsor, for prior approval.

1.4 The Direct Debit Instruction

The Direct Debit Instruction - design

The Direct Debit Instruction (DDI) is the method by which Service Users obtain the Payer's authority and account details to debit his account. The design of the DDI must follow the prescribed format and be agreed by the Sponsor.

The Direct Debit Guarantee

The Direct Debit Guarantee is offered by the Paying Banks as an assurance to Payers that:

- In the event of error they will be immediately refunded by the Paying Bank

- Advance Notice will be given before collections are made

- They may cancel the DDI at any time.

The Direct Debit Guarantee must be issued to the Payer with the DDI or the Advance Notice.

Completion and lodgement

Once the completed DDI has been returned by the Payer, the Service User must ensure that all relevant information is recorded before lodging it with the Payer's Bank.

Upon receipt, the Payer's Bank will either accept or reject the DDI. If rejected the DDI is returned to the Service User.

1.5 The Advance Notice

This is the method by which Service Users give notice to the Payer before the first Direct Debit is collected. It must also be given if the due date, frequency or amount changes.

The Service User may agree the period of Advance Notice with the Payer. The default period in the absence of any other agreements is a minimum of 10 **working days** plus postal time. As such the time period used in the Direct Debit Guarantee is the time allowed between the Payer receiving the Advance Notice and the first / amended collection.

1.6 The Collection Process

This is the process whereby the Service User collects Direct Debits from its Payers. The management and timing of the collection is the Service User's responsibility. The collection must be made accurately and in a timely manner. The total of any Direct Debit collection is credited to the Service User's account on the same day as collections are debited from the Payers' account.

The collection process includes preparing and handling **Bacs** submissions, the reconciliation of amendments, cancellations and advice to Service Users on error recovery.

Service Users are responsible for ensuring that payments collected using the Scheme can legally be demanded and collected in this way, without contravening consumer protection or other legislation.

Direct Debit is the method of collecting payments and the Banks are not responsible for any underlying contract between the Service User and the Payer.

1.7 Unpaid Direct Debits

Direct Debits may be returned unpaid by the Paying Bank when:

- the Paying Bank gives advice to the Service User of change of circumstances to the DDI (e.g. Instruction cancelled)

- a Payer disputes the due date, amount or frequency of a Direct Debit

- the Paying Bank is referring the collection back to the Service User as notification of non-payment e.g. 'Refer to Payer'.

An unpaid Direct Debit will be debited from a Service User's account either 2 or 3 working days after the **entry day**.

1.8 Re-presentation of Unpaid Direct Debits

A re-presented Direct Debit is a debit which has been previously returned by the Paying Bank as unpaid. An unpaid Direct Debit may be re-presented by the Service User within one month of the date on which first presentation was made. It must be for the same amount as originally presented.

1.9 Direct Debit Instruction Amendment and Cancellation

Any change, amendment or cancellation of the DDI advised by the Payer, takes effect as soon as it is received by the Paying Bank or the Service User. The Paying Bank must advise the Service User, failure to do so may result in liability for the Paying Bank.

1.10 Indemnity Claims

Paying Banks will refund the Payer in the event of an error. If the error is made by the Service User, Paying Banks will use the Indemnity Claim process to reclaim the refund from the Service User.

The Service User must settle an **Indemnity Claim** within 14 working days of the date of the claim. The Service User may in certain circumstances raise a counter claim.

See section 11.2 for Valid Counter Claims

Where the Paying Bank has made a payment in error, it may send a **Refund Request** form to the Service User. The Service User may settle this at its discretion.

1.11 AUDDIS (AUtomated Direct Debit Instruction Service)

AUDDIS automates the lodgement of DDIs from Service Users to the Paying Banks electronically.

With effect from 1 January 2008 the use of AUDDIS to submit DDIs is mandatory for all new Service Users that submit direct to Bacs.

The paper DDI will remain with the Service User who must provide a copy to the Paying Bank within 7 working days if requested to do so.

1.12 Marketing

It is the role of the Sponsor to provide information, advice and guidance upon all aspects of the Service User's Direct Debit operations, including marketing advice.

1.13 Standing Order Conversion

A number of Service Users also receive payment from some of their customers by **Standing Order**. This is an automated collection initiated by the Payer's Bank on behalf of the Payer for a fixed amount on a fixed date.

Service Users can increase efficiency and reduce costs by converting customers to collection by Direct Debit.

1.14 Monitoring of the Scheme

The Service User must seek advice from their Sponsor if in doubt as to any aspect of the Scheme and its Rules.

The Service User must advise its Sponsor of any changes to its status, communications literature or Bacs submissions. Sponsors will monitor the operations of the Scheme to ensure the required standards are achieved and maintained by all **participants**.

1.15 Exit from the Scheme

A Service User may withdraw from the Scheme voluntarily. In addition a Service User may be required to withdraw by its Sponsor or due to termination of its legal capacity (e.g. bankruptcy or winding up).

The Sponsor will manage the Service User's withdrawal from the Scheme. Even though the Service User has ceased to collect Direct Debits it is still liable for any Indemnity Claims which may be raised by the Paying Banks for Direct Debits applied to the Payer's account during the period of the Service User's participation in the Direct Debit Scheme. In all cases this liability is not restricted in respect of time or amount.

2 BECOMING A DIRECT DEBIT SERVICE USER

Introduction

An organisation wishing to join the Scheme should contact its Bank who will advise it of the steps involved in becoming a **Service User**. Its Bank, will consider the request to **Sponsor** the organisation as a Direct Debit Service User. The organisation must execute an **Indemnity** in favour of all Banks participating in the Scheme.

The Scheme is sometimes unsuitable for non-corporate bodies because the Indemnity liability in some cases falls directly upon individuals without limitation as to time and amount.

The Service User must submit all documentation it intends to use in its Direct Debit operations to its Sponsor for prior approval.

2.1 Application for sponsorship

The application of a prospective Service User must stand on its own merits. It is the Sponsor's duty to assess the suitability of the prospective Service User. Consideration must include:

- contractual capacity

- financial standing

- the quality of its administrative control.

A Service User must have a registered address in the UK and a UK sterling bank account. Bacs reports will be available to download via **Bacstel-IP** and the Bacs payment services website. Details of Bacs reports are included in the Service User Guide – Bacstel-IP.

A Service User must complete and lodge an Indemnity with its Sponsor. A Service User which is an overseas registered company, or which has its principal place of business overseas, must provide legal opinion that the Indemnity would be enforceable under the overseas jurisdiction and / or provide proof of adequate assets within the UK jurisdiction.

See section 2.4 for Standard Indemnity.

The success of the application will not be influenced by the existence or availability of any private insurance to cover a Service User's Indemnity liability.

Third party support for the liability assumed under the Indemnity is unacceptable to the Sponsor. However, in this context, the relationship between parent and subsidiary companies is not deemed a third party relationship, and may be taken into consideration for so long as it lasts, provided an Indemnity has been given by the parent company.

Service Users may in some instances hold an account with more than one Bank. In such instances Service Users will be sponsored by all the Banks with whom an account is held for that **SUN**. Collected funds must be credited to an account in the name of the Service User which must be held by the Sponsor(s). Each Sponsor shall be responsible, without limit of time and amount, for Direct Debits collected under the Service User's account maintained with it under that SUN.

Agency Bank sponsorship

Agency Banks can nominate their customers to participate in the Scheme by being Sponsored by one of the Member Banks.

If an Agency Bank wishes to participate in the Scheme as a Service User, it must complete one of the Standard Forms of Indemnity and be Sponsored by one of the Member Banks. The set-up process will then be the same as for any other organisation becoming a Service User.

If an Agency Bank wishes to nominate one of its own customers as a Service User under the Direct Debit Scheme, then the Agency Bank must ensure the following are adhered to:

- The customer (that Service User) must complete one of the Standard Forms of Indemnity

- The Agency Bank must indemnify its Sponsor by signing an Agency Bank Indemnity

- It must complete an Agency Bank Letter of Nomination, proposing its customer as a Direct Debit Service User

- It must adopt the standard set-up procedures the same as for any other Service User.

The Agency Bank is responsible for ensuring its customers adhere to the Scheme Rules.

2.2 Standard Service User set-up

This is the process by which Service Users are registered and prepared for Direct Debit collection.

Allocation of the Service User Number (SUN)

If the application is accepted by the Sponsor, the Service User will be allocated a unique Service User Number (SUN) which must be quoted on all DDIs and the records sent to Bacs.

The SUN and the Service User's **registered name** will be advised to all the Sponsors and Bacs by the Service User's Sponsor. Service Users must ensure that they quote their registered name on all Direct Debit communications.

Service Users will be notified by their Sponsors when their SUN is set-up on the Bacs database. They must allow sufficient time (4 weeks minimum) from this date before lodgement of DDIs with the Paying Banks. This period is required to allow the Sponsor to notify the Paying Bank of the Service User's SUN.

A Service User can only collect Direct Debits using the SUN on the DDI signed by the Payer. If the Service User wishes to collect from the Payer under a different SUN it must obtain a new DDI from the Payer. The same SUN cannot be used by more than one Service User.

Service User's communication literature, Bacs input format and design of documents

The Service User must obtain prior approval from its Sponsor for all documentation it intends to use within the Direct Debit Scheme.

This approval will extend to:

-   communications addressed by Service Users to Payers with the object of encouraging Payers to sign a DDI. This will avoid any discrepancy in the information provided by Service Users and Banks to Payers

-   communications addressed by Service Users to Bank branches to seek their co-operation in some special procedure

-   the DDI – the registered name of the Service User of the Direct Debit must be clearly identified on the DDI and must be used by Service Users in **Field 9 of the Bacs data record** which may appear on the Payer's bank statement against the relative debit

-   Advance Notices

-   communications relating to amalgamation of payments

-   any sequence of operations, in so far as these operations involve Payers or Bank branches

-   format of Bacs input file, including usage of the full range of transaction codes.

2.3   Variations from the standard set-up

There are agreed exceptions to the standard set-up rules which will always require prior authorisation of the Sponsor before implementation.

  Authorisation of a variation in procedure will not diminish any liability under the Indemnity that might otherwise arise.

Trading names

•   Service Users must have a separate SUN for each trading name. Each trading name must be registered at Bacs. **Service names** cannot be registered.

•   The registered trading name must be used on both the DDI and the Direct Debit record (field 9 of the Bacs data record). The use of service names is not permissible unless accompanied by the trading name.

•   Collected funds shall be credited to an account owned by the Service User, either in its **registered name** or trading name and held with its Sponsor(s).

Facilities management

Facilities management is:
'A Service User taking responsibility for the collection or administration of Direct Debits on behalf of another organisation, not necessarily being a Service User in its own right' (FM client). This is distinct from the case of a **commercial bureau** which merely undertakes the processing function on behalf of a Service User or **management administration**.

A Service User may contract with such an organisation to manage its Direct Debit application. This would include:

- corresponding with the Payer, receipt of completed DDIs and lodgement with the Paying Banks

- management of returned, amended and cancelled DDIs.

- management of collection files sent to Bacs and the collection of Direct Debit records on the payment due date(s). Reconciliation of processed, rejected and returned items.

• It will be necessary for the appropriate contractual arrangements covering the **facilities management** application to be in place before the Service User provides such a facility

• The SUN must be registered at Bacs in the format of 'AN Company Limited re FM Client' and this registered format must then be identified on the DDI, where the FM Client is the legal entity on behalf of whom A N Company Limited (the Service User) is collecting the funds

• A Service User must use a separate SUN for each FM Client. If the FM Client requires the collection to be made using trading names, then the Service User must have a separate SUN for each trading name of that FM Client

• Either the name of the Service User or FM Client (or both names) quoted on the DDI must be used with the Direct Debit collection record. (**Field 9** of the Bacs data record).

Proceeds from the collection of Direct Debits under the "facilities management" agreement for any new FM Clients taken on by a Service User must be directed to an account in the name of the DD Service User, specifically designated "Clients" / "Trust" accounts. All such accounts must be held at the same bank i.e. the Service User's Sponsor Bank. No funds should be paid directly into an FM Client's own account. In such cases the Service User will accept liability for any Indemnity Claims irrespective of whether or not claims can be recovered from the FM Client to whom the funds have been released. The Sponsor authorising such an arrangement will assume responsibility for its Service User's activities.

2.4 The Indemnity

As a condition of participation in the Direct Debit Scheme, a Service User must execute a standard form of Indemnity which must be obtained from its Sponsor. By executing the Indemnity the Service User is bound by the terms and conditions of the Indemnity.

The purpose of the Indemnity is to underwrite the protection offered to the Payer under the Guarantee.

Service Users should note that the liability is unlimited as to;

a) Time   -   the liability will continue in respect of Direct Debits originated prior to receipt by the Banks of written notice of termination of the Indemnity.

b) Amount -   the liability of a Service User arises in respect of Direct Debits originated in error. Also where a Service User has failed to collect, consequential losses attributable to such errors may also arise. (e.g. failure to collect an insurance premium can result in loss of cover.)

Wherever possible, the Indemnity should be executed as a deed in compliance with the Companies Acts or equivalent legislation. If execution in this manner is not possible, advice should be sought from the Sponsor. Any alternative method of execution will always require an authorising resolution to be given by the board or other governing body of the Service User.

After execution, the signed Indemnity and accompanying authorising resolution (if, exceptionally, the Indemnity is not executed as a deed) must be returned by the Service User to its Sponsor.

A Service User must immediately advise its Sponsor if there is any change in its legal status, including a change brought about by merger or insolvency. In this event, the Service User must obtain new DDIs from its Payers. In exceptional circumstances, arrangements can be made to transfer DDIs from one SUN to another, and to a different legal entity, subject to strict safeguards. Service Users must refer to their Sponsor if they wish to make such arrangements.

Should a Service User cease to collect Direct Debits under the Direct Debit Scheme, the Service User must provide written notice of termination to its Sponsor. The Service User will continue to be liable for all Direct Debits originated during its period of participation in the Scheme and any subsequent **Indemnity Claims** raised by the Paying Banks.

2.5   Dates on Indemnity documentation

If exceptionally, the indemnity is not executed as a deed, the Indemnity must not be signed until after any necessary authorising resolution has been passed.

2.6   Example of prohibited practices

- The Indemnity cannot be amended in any way

- Use of correction fluid, staples or sellotape on the Indemnity is not permitted.

2.7 Example of a Standard Indemnity

Standard Indemnity – to be used for limited companies and other incorporated bodies.

STANDARD INDEMNITY

To Abbey National plc
Alliance & Leicester Commercial Bank plc
AIB Group UK Plc
Bank of England
Bank of Ireland
Bank of Scotland
Barclays Bank PLC
Clydesdale Bank PLC
Co-operative Bank p.l.c.
Coutts & Co.

Lloyds TSB Bank plc
HSBC Bank plc
Nationwide Building Society
NatWest Bank Plc
Northern Bank Limited
Northern Rock Plc
The Royal Bank of Scotland plc
Ulster Bank Limited
Yorkshire Bank PLC

and all other financial institutions to whom sorting code numbers have been allocated and whose customers' accounts may receive Direct Debits from us.

1. In consideration of your each accepting instructions from time to time from us, or from our agent or anyone purporting to be our agent, to debit yourselves or the account of your customers with the amounts specified in such instructions.

   WE UNDERTAKE TO INDEMNIFY each of you, on your first demand, against any claim made against you as a result, directly or indirectly, of your acting or failing to act on any such instruction.

2. The claims referred to in paragraph 1 above include legal actions, and references to any ombudsman or similar scheme, as well as demands made directly to you. We agree that any of you may accept, reject or compromise any claim without consulting us and without thereby reducing our liability under this indemnity.

3. We acknowledge that the operation of the Direct Debit Scheme as a high volume system does not always allow the checking of every debit against instructions held, and agree that this Indemnity shall apply whether or not any such check has been made, and whether or not any instruction has been received from your customer and remains in force.

4. We similarly agree that you are under no obligation to enquire whether or not any condition or purpose of payment specified in any instruction has been complied with.

5. We agree at all times to comply with the rules of the Direct Debit Scheme as set out in the Originators' Guide and Rules to the Direct Debit Scheme, as amended from time to time.

6. We shall make payment under this Indemnity on your first demand and without proof of loss within 14 working days of the date of a properly completed claim from you.

   6.1 Having paid a claim under this Indemnity, we retain the right to make a repayment claim against you to the extent that any loss was caused by your or your agents' failure to comply with the requirements of the Direct Debit Scheme set out in the *Originator's Guide and Rules to the Direct Debit Scheme (the Guide)* as amended from time to time, and in accordance with the procedures set out in the Guide. (In the Guide, such a repayment claim is called a "Counter Claim".)

   6.2 Any repayment claim shall be made following the procedures set out in the Guide within **14** days of payment of the claim.

   6.3 Following resolution of the repayment claim any sum due to us will be paid within **90** days.

7. This Indemnity is given in addition to any other indemnity already given either by us or by any other person in support of our participation in the Direct Debit Scheme. Should there be a direct conflict between any of the terms of this Indemnity and any earlier one, the term of this Indemnity shall prevail.

8. This Indemnity shall continue to apply notwithstanding any payment made by us, any account stated, or any compromise, waiver, or indulgence made by either you or us in respect of any claim or repayment claim.

9. This Indemnity shall not be affected by any change in name of any of you, or of us, or of any change in the legal status of any of you including any change brought about by merger or amalgamation, in which case it shall apply for the benefit of the merged company, or any successor company.

10. We may terminate this Indemnity at any time by giving notice to our sponsoring bank and to each other financial institution who has accepted the cover it provides, but shall remain liable in respect of any debits that have been originated before such notice is received by each institution.

11. This Indemnity shall be governed by, and interpreted in accordance with, the laws of England.

12. Any legal proceedings against us arising out of this Indemnity may be commenced, at your choice, in either the courts of England (to which we irrevocably and unconditionally submit) or the courts of the country in which we are incorporated or the courts of any country in which we carry on business.

13. We shall promptly inform you of any change in our name or in our legal status, including any change arising by virtue of the operation of the Insolvency Acts 1986 or any other insolvency or similar legislation in the United Kingdom or elsewhere which applies to us, and including any change effected for the purpose of reorganisation.

14. Should we at any time become, or discover we are, legally incapable of giving effect to this Indemnity (either as a whole or partially) we shall notify you forthwith and shall cease to originate Direct Debits, and shall take such other reasonable steps as you may require in order to protect the interests of your customers and the integrity of the Direct Debit Scheme. If as a result of incapacity we are only partially disabled from giving effect to this Indemnity we shall continue to fulfil all our other obligations under it.

15. Any notice required to be given to us in connection with this Indemnity or any claim may (in addition to any other place at which they may properly be served) be delivered to us at our registered office, or at any address at which we carry on business or at the address given below, or at such other address as may be given by us to BACS Limited for this purpose.

EXECUTED AS A DEED by _____ plc / Limited

(Company registration number_____)

this_____day of_____20_____

_____ Director
(Name in capitals)   (Signature of person signing)

_____ Director/Secretary
(Name in capitals)   (Signature of person signing)

1446/01/04

2.8 Example of Standard Indemnity (Partnership)

Example of Standard Indemnity to be given by a Partnership other than a Limited Liability Partnership (LLP)

Note that each partner of a firm is jointly and severally responsible for any loss which may arise out of a partnership. Every partner must sign the Indemnity.

A new Indemnity must be taken each time a firm changes its partners.

STANDARD INDEMNITY – PARTNERSHIP

To   Abbey National plc   Lloyds TSB Bank plc
     Alliance & Leicester Commercial Bank plc   HSBC Bank plc
     AIB Group UK Plc   Nationwide Building Society
     Bank of England   NatWest Bank Plc
     Bank of Ireland   Northern Bank Limited
     Bank of Scotland   Northern Rock Plc
     Barclays Bank PLC   The Royal Bank of Scotland plc
     Clydesdale Bank PLC   Ulster Bank Limited
     Co-operative Bank p.l.c.   Yorkshire Bank PLC
     Coutts & Co.

and all other financial institutions to whom sorting code numbers have been allocated and whose customers' accounts may receive Direct Debits from us.

1   In consideration of your each accepting instructions from time to time from us, or from our agent or anyone purporting to be our agent, to debit yourselves or the account of your customers with the amounts specified in such instructions

    WE INDIVIDUALLY AS WELL AS JOINTLY UNDERTAKE TO INDEMNIFY each of you, on your first demand, against any claim made against you as a result, directly or indirectly, of your acting or failing to act on any such instruction.

2   The claims referred to in paragraph 1 above include legal actions, and references to any ombudsman or similar scheme, as well as demands made directly to you. We agree that any of you may accept, reject or compromise any claim without consulting us and without thereby reducing our liability under this indemnity.

3   We acknowledge that the operation of the Direct Debit Scheme as a high volume system does not always allow the checking of every debit against instructions held, and agree that this Indemnity shall apply whether or not any such check has been made, and whether or not any instruction has been received from your customer and remains in force.

4   We similarly agree that you are under no obligation to enquire whether or not any condition or purpose of payment specified in any instruction has been complied with.

5   We agree at all times to comply with the rules of the Direct Debit Scheme as set out in the Originators' Guide and Rules to the Direct Debit Scheme, as amended from time to time.

6   We shall make payment under this Indemnity on your first demand and without proof of loss within 14 working days of the date of a properly completed claim from you.

   6.1   Having paid a claim under this Indemnity, we retain the right to make a repayment claim against you to the extent that any loss was caused by your or your agents' failure to comply with the requirements of the Direct Debit Scheme set out in the *Originator's Guide and Rules to the Direct Debit Scheme (the Guide)* as amended from time to time, and in accordance with the procedures set out in the Guide. (In the Guide, such a repayment claim is called a "Counter Claim".)

   6.2   Any repayment claim shall be made following the procedures set out in the Guide within **14** days of payment of the claim.

   6.3   Following resolution of the repayment claim any sum due to us will be paid within **90** days.

7   This Indemnity is given in addition to any other indemnity already given either by us or by any other person in support of our participation in the Direct Debit Scheme. Should there be a direct conflict between any of the terms of this Indemnity and any earlier one, the term of this Indemnity shall prevail.

8   This Indemnity shall continue to apply notwithstanding any payment made by us, any account stated, or any compromise, waiver, or indulgence made by either you or us in respect of any claim or repayment claim.

9   This Indemnity shall not be affected by any change in name of any of you, or of us, or of any change in the legal status of any of you including any change brought about by merger or amalgamation, in which case it shall apply for the benefit of the merged company, or any successor company.

10   We may terminate this Indemnity at any time by giving notice to our sponsoring bank and to each other financial institution who has accepted the cover it provides, but shall remain liable in respect of any debits that have been originated before such notice is received by each institution.

11   This Indemnity shall be governed by, and interpreted in accordance with, the laws of England.

12   Any legal proceedings against us arising out of this Indemnity may be commenced, at your choice, in either the courts of England (to which we irrevocably and unconditionally submit) or the courts of the country in which we are incorporated or the courts of any country in which we carry on business.

13   We shall promptly inform you of any change in our firm name or in the names of the partners or in our legal status, including any change arising by virtue of the operation of the Insolvency Acts 1986 or any other insolvency or similar legislation in the United Kingdom or elsewhere which applies to us, and including any change effected for the purpose of reorganisation. We shall each continue to be bound by this Indemnity notwithstanding any change in the composition of the partnership. Notice of retirement of a partner shall be treated as a notice terminating his liability under paragraph 9 above for debits made after such notice, but shall not as such affect or terminate the liability of the continuing partners.

14   Should we at any time become, or discover we are, legally incapable of giving effect to this Indemnity (either as a whole or partially) we shall notify you forthwith and shall cease to originate Direct Debits, and shall take such other reasonable steps as you may require in order to protect the interests of your customers and the integrity of the Direct Debit Scheme. If as a result of incapacity we are only partially disabled from giving effect to this Indemnity we shall continue to fulfil all our other obligations under it.

15   Any notice required to be given to us in connection with this Indemnity or any claim may (in addition to any other place at which they may properly be served) be delivered to us at the address given below, or at such other address as may be given by us to BACS Limited for this purpose, or at any other place at which we carry on business.

EXECUTED AS A DEED this..................day of.................................20..........by us being all the partners in the firm of

....(Originator) whose principal place of business is at..

Name	Signature	Witnessed by[†]
1		
2		

[†]Signature, name and address of witness

By Signing this Indemnity you will be accepting unlimited liability for any claims that may be made arising out of your Direct Debit operations. Only sign it if you wish to be bound by it. It is in your own interest to take legal advice before signing.

1448/01/04

2.9   Other Forms of Indemnity

Modified forms of the Indemnity are available for execution by the following types of organisation:

- Partnership subject to Scottish law

- Large professional partnership (separate English/Welsh/NI and Scottish forms)

- Limited Liability Partnership

- Sole Trader*

- Unincorporated Association*

- Parent company in support of Service User subsidiary

- Agency Bank.

A Service User must seek guidance from its Sponsor before using any of these forms.

Note that execution by a sole trader, or by any person on behalf of a club, society or other Unincorporated Association imposes unlimited personal liability on the signatories, who are strongly recommended to take legal advice before giving the Indemnity.

3   THE DIRECT DEBIT INSTRUCTION

Introduction

The Direct Debit Instruction (DDI) is the method by which Service Users obtain the Payer's authority to debit his account. It is important that the DDI provides all the necessary information to enable collection by Direct Debit and that the Payer is provided with a clear understanding that they have given their authority to debit their account. There is a standard format for the DDI which has been designed to make it easy for the Payer to complete and to ensure that all the details necessary to set up the DDI are obtained. The design of all DDIs must be approved in writing from the Service User's Sponsor **before the DDIs can be issued by the Service User**. The reverse of a DDI must not set out information that might be taken to be part of the Instruction. Where it is intended that additional information for Payers should be printed on the reverse of the DDI, the Sponsor's approval in writing must first be obtained.

The Direct Debit Scheme provides for Direct Debit Instructions (DDIs) to be obtained and lodged in three separate distinct ways:

* The standard DDI, whereby a paper DDI is physically signed by the Payer and lodged by the Service User with the Paying Bank before commencing Direct Debit operations;

* Under AUDDIS a paper DDI is obtained as above but only the information is lodged with the Paying Bank, the paper copy remaining with the Service User;

* Paperless DDI, whereby the DDI itself may be completed electronically, or over the telephone then lodged under AUDDIS.

The requirements for the standard DDI are given below applying also in all other cases unless otherwise stated.

3.1   Content of the Direct Debit Instruction

The DDI must hold the following information.

* The Service User's name and address

* Direct Debit logo

* Service User's SUN

* The heading 'Instruction to your Bank or Building Society to pay by Direct Debit'

* The name and full postal address of the Bank or Building Society where the Payer's account is held

* The name(s) of account holder(s)

* The Payer's branch sort code

* The Payer's Bank or Building Society account number

See section 3.8 for example.

- The Service User's reference
- Payer's instruction to debit his or her account including reference to the Direct Debit safeguards under the Direct Debit Guarantee, signature(s) and date.

The **Direct Debit Guarantee** must be provided to the Payer with the DDI, Advance Notice or other correspondence issued in respect of the application. Service Users are advised to print the Guarantee on the bottom of the DDI as a tear off portion to be retained by the Payer.

The only additional information which is permitted on the DDI is an optional area for a Service User's official use only, and the Service User's company logo.

The Service User's official use area is provided solely for the internal use of the Service User. Text in this box will not be read by the Paying Bank. It **must** include the words shown in the example form.

For Service Users who include a DDI within a publication i.e. magazine / journal it must be noted that the DDI must still hold the above information with the exception of the Direct Debit Guarantee which may be omitted due to the constraints of available print space. Service Users must however include a copy of the Guarantee with the Payer's **Advance Notice** or other correspondence to the Payer.

All DDIs must be variable in terms of amount, date and frequency. As such, neither the amount, date nor frequency, must be quoted on the DDI, the exception being use of the Service User's 'official use box'. However, these details must be advised to the Payer by Advance Notice.

3.2 Guidelines for design of the Direct Debit Instruction

- The prescribed order of information boxes must be maintained on the face of the Instruction

- **The maximum size of** a DDI must be A4, 1/3 A4 size DDI is also acceptable
- **The minimum size of** a DDI must be 110mm by 70mm, this includes published instructions
- The DDI must be clearly separated from any other text. No additional material can appear within the boundary of the Instruction, with the exception of the official use box
- The paper Instruction delivered to the branch must be rectangular to facilitate ease of handling / storage
- The presentation of the Direct Debit logo must conform to, 'The Direct Debit Identity Guidelines' and should be positioned on the top right hand side of the DDI adjacent to the Service User's Number

- Bilingual Instructions, e.g. English / Welsh, are acceptable, however the Direct Debit logo can only be used in its approved English format

- The standard heading 'Instruction to your Bank or Building Society to pay Direct Debits' is mandatory

- Clear instructions to the Payer for the return of the form must be shown on the face of the DDI

- The authority text to debit the Payer's account must always be printed above the Payer's signature box

- Where the Service User is undertaking a **Standing Order** conversion the instruction to cancel the Standing Order must be printed as a section at the bottom of the DDI

- Service User's name and address which must be pre-printed

- A Service User may have a Service User's 'official use box' on the DDI, which may be used to record information not pertinent to the Payer's authority for the Direct Debit application

- The SUN must be pre-printed or stamped on the **DDI**

- Optional – An additional field may be added to the DDI to capture the signatory's name e.g. when obtaining a DDI from a corporate customer the words 'Print name' may be added either adjacent to or below the signature line.

3.3 The Direct Debit Guarantee

It is recommended that the Guarantee is printed as a tear off strip at the bottom of the DDI so that it can be retained by the Payer. For Service Users who print the DDI in a publication and are not able to include the Direct Debit Guarantee due to the constraints of available print space, the Guarantee must be issued to the Payer with the **Advance Notice** or other correspondence issued in respect of the application. A Service User must enter the number of days Advance Notice which will be given to the Payer in respect of payments to be collected under the DDI.

The Service User may agree the period of Advance Notice with the Payer. The default period in the absence of any other agreement is a minimum of 10 **working days** plus postal time. As such, the time period used in the Direct Debit Guarantee is the time allowed between the Payer receiving the Advance Notice and the first / amended payment.

Service Users must not present a Direct Debit for collection prior to the expiry of the notice period plus the postal delay.

The Paying Bank must meet the terms of the Direct Debit Guarantee.

3.4 Choice of Collection Date

There is no objection to the Service User indicating in the Service User's 'official use box' the dates on which collections are intended to be made, or even offering a choice of date. The box must however prominently include the words 'This is not part of the Instruction to your Bank or Building Society'. The contents of this box will not be read or monitored by the Paying Bank. Under no circumstances should any reference to amounts or dates be shown anywhere on the form outside the Service User's 'official use box'.

3.5 Standing Order conversion

A number of Service Users also receive payment from some of their customers by **Standing Order**. This is an automated collection initiated by the Payer's Bank on behalf of the Payer for a fixed amount and date.

There is a standard combined DDI / Related Standing Order Cancellation form to be used when the Service User is running a conversion campaign.

See section 14.4 for an example.

3.6 Service User's responsibilities

The **Service User** must ensure that all proposed literature in respect of its Direct Debit application is approved by its Sponsor. If an error is discovered after the printing of the approved DDI the Service User must immediately contact its Sponsor who will advise of the appropriate action to be taken. This may involve the destruction of the erroneous DDIs and reprinting in the correct format.

Service Users must ensure that the DDI is correctly completed prior to despatch to the Paying Bank and that the Payer has not added any amount or date restrictions to the DDI. DDIs can only be lodged with the Paying Bank by the Service User and not directly by the Payer.

A Service User using the tear off slip DDI format for additional information must ensure that this is detached before submission to the Paying Bank.

See section 3.8.5 for an example.

The DDI is not evidence of any contract between the Service User and the Payer's Bank.

3.7 Example of prohibited practices

The use of certain practices and additions to the DDI are prohibited.

- Multiple SUN or **Reference** choices must not be used on the DDI (Except for AUDDIS, see Section 15.4 for further details).

- The use of the words 'account number' must not be used to describe the Service User's reference

- The wording of the Direct Debit Guarantee as detailed in this Guide must not be varied in any way

- The **SUN** number printed or stamped on the DDI must not be altered once the Payer has signed the DDI

- The DDI must not be used for the collection of a **single payment**. A single payment can be defined as a Direct Debit, which will only be collected once. **Irregular payments**, which occur more than once in a 13 month period, are allowed by the Scheme

- Service Users must not combine a Standing Order Mandate with a DDI e.g. '*I / We authorise you to charge my/our account with you by Standing Order or Direct Debit for the credit of A. N. Company Ltd*.'

- The Service User must not make reference on the DDI of the proposed collection date and / or that the first collection will include all back collections e.g. '*The first Direct Debit will include all amounts which are due up to the date the Instruction is presented*.'

- The Service User must not vary the text or make any addition to the DDI except in the Service User's 'official use box'

- The Service User must not include an address disclosure clause within the DDI e.g. '*You are hereby authorised to advise A.N. Company Ltd of my/our address upon request*.'

- The use of adhesive labels on DDIs is not permitted in any form

- The Service User must not lodge DDIs which contain only a copy of the Payer's signature

- The DDI must not be lodged with any form or contract required by the Service User in respect of the service / product offered

- Fixed amount or date DDIs are no longer supported by the Scheme. New fixed amount or fixed date DDIs must not be sought from customers

- The Service User must not lodge DDIs which are not completed in English

- The Service User must not print on the DDI itself any details that the Payer needs to keep, including dates and times of collections.

3.8   The Direct Debit logo

The Direct Debit logo is a powerful visual identity which has been developed to increase recognition of and positive attitudes towards Direct Debit.

The Direct Debit logo must be included on all Direct Debit Instructions. It should also be featured in all literature promoting Direct Debit.

The Logo

To avoid any conflict of style and for the sake of clarity, the logo should always appear in 100% strength black on a DDI. If black is not being printed a predominant colour must be used. The logo may appear on a background colour or tint providing it remains prominent.

Format and typestyle

There are two acceptable uses of the logo:
a) Landscape format
b) Portrait format

The logo should never appear without the approved format of lettering. The characters used in the wording have been specially and exclusively designed to complement the logo; they are unique. As a result, no existing typeface exactly matches the lettering and so attempts to match the wording through typesetting are neither feasible nor acceptable.

Exclusion zone

To be effective the logo must have a degree of prominence and visibility that will maximize its impact. When developing printed material, an area around the logo and lettering should be left free of any other matter. Leave a minimum area on all sides of the logo equal to the capital letter height of the 'D' of Direct.

Minimum size

There is a minimum acceptable size for the logo. The capital letter height of the 'D' of Direct should never be less than 2mm.

3.8.1 The Direct Debit Guarantee

The Direct Debit Guarantee provides assurance to the Payer that any monies taken in error by the Service User or the Paying Bank will be immediately refunded by the Payer's Bank. It confirms to the Payer that he may cancel a Direct Debit at any time. There are two forms of Direct Debit Guarantee wording as illustrated below. The Service User must use the form of wording that is most appropriate to its organisation, however it must not vary the wording in any way. Please note that the standard wording is shown on all DDI templates in this guide.

See section 11.3 for details on Refunding the Payer's account

<div style="border: 3px solid black; padding: 20px;">

The Direct Debit Guarantee

DIRECT Debit

- This Guarantee is offered by all Banks and Building Societies that take part in the Direct Debit Scheme. The efficiency and security of the Scheme is monitored and protected by your own Bank or Building Society.

- If the amounts to be paid or the payment dates change, *(insert your company name)* will notify you *(insert number of)* working days in advance of your account being debited or as otherwise agreed.

- If an error is made by *(insert your company name)* or your Bank or Building Society, you are guaranteed a full and immediate refund from your branch of the amount paid.

- You can cancel a Direct Debit at any time by writing to your Bank or Building Society. Please also send a copy of your letter to us.

</div>

3.8.1 The Direct Debit Guarantee (continued)

<div style="border: 3px solid black; padding: 20px;">

The Direct Debit Guarantee

DIRECT Debit

- This Guarantee is offered by all Banks and Building Societies that take part in the Direct Debit Scheme.

- If an error is made in the payment of your Direct Debit, either by us, *(insert your company name)*, or by your Bank or Building Society, you are entitled to a full and immediate refund from your bank branch. Simply contact your Bank or Building Society to arrange a refund, or if you prefer contact *(AN Company)* and they shall arrange to repay you direct.

- You can cancel a Direct Debit at any time by simply contacting your Bank, Building Society or us. Written confirmation may be required.

- If there are any changes to the amount, date or frequency of your Direct Debit *(insert your company name)* will notify you in advance of your account being debited, this will be *(insert number of)* working days or as otherwise agreed.

- If you request us to collect a payment, confirmation of the amount and date will be given to you at the time of the request.

</div>

3.8.2a Recommended Direct Debit Instruction with Service User's 'official use box'

This is an example where the Service User's 'official use box' is to be used for additional information on the DDI.

DIRECT Debit

A N Company
logo or name

Instruction to your Bank or Building Society to pay by Direct Debit

Please fill in the whole form including official use box using a ball point pen and send it to:

A N Company
Any Street
Any Town
Anywhere
AB1 2CD

Service User Number (SUN)

FOR (AN COMPANY) OFFICIAL USE ONLY
This is not part of the instruction to your Bank or Building Society.

Name(s) of Account Holder(s)

Bank/Building Society account number

Branch Sort Code

Name and full postal address of your Bank or Building Society

To: The Manager   Bank/Building Society

Address

Postcode

Instruction to your Bank or Building Society
Please pay (A N Company) Direct Debits from the account detailed in this Instruction subject to the safeguards assured by the Direct Debit Guarantee. I understand that this Instruction may remain with the (A N Company) and, if so, details will be passed electronically to my Bank/Building Society.

Signature(s)

Date

Reference

Banks and Building Societies may not accept Direct Debit Instructions for some types of account

✂

This guarantee should be detached and retained by the Payer.

DIRECT Debit

The Direct Debit Guarantee

- This Guarantee is offered by all Banks and Building Societies that take part in the Direct Debit Scheme. The efficiency and security of the Scheme is monitored and protected by your own Bank or Building Society.
- If the amounts to be paid or the payment dates change (A N Company) will notify you (insert number of) working days in advance of your account being debited or as otherwise agreed.
- If an error is made by (A N Company) or your Bank or Building Society, you are guaranteed a full and immediate refund from your branch of the amount paid.
- You can cancel a Direct Debit at any time by writing to your Bank or Building Society. Please also send a copy of your letter to us.

A4 Instruction Version 1

3.8.2b Recommended Direct Debit Instruction without Service User's 'official use box'

DIRECT Debit

A N Company
logo or name

Instruction to your Bank or Building Society to pay by Direct Debit

Please fill in the whole form using a ball point pen and send it to:

A N Company
Any Street
Any Town
Anywhere
AB1 2CD

Service User Number

Reference

Name(s) of Account Holder(s)

Instruction to your Bank or Building Society

Please pay (A N Company) Direct Debits from the account detailed in this Instruction subject to the safeguards assured by the Direct Debit Guarantee.

I understand that this Instruction may remain with the (A N Company) and, if so, details will be passed electronically to my Bank/Building Society.

Bank/Building Society account number

Branch Sort Code

Name and full postal address of your Bank or Building Society

To: The Manager   Bank/Building Society

Address

Postcode

Signature(s)

Date

Banks and Building Societies may not accept Direct Debit Instructions for some types of account

✂ —

DIRECT Debit

The Direct Debit Guarantee

- This Guarantee is offered by all Banks and Building Societies that take part in the Direct Debit Scheme. The efficiency and security of the Scheme is monitored and protected by your own Bank or Building Society.
- If the amounts to be paid or the payment dates change (A N Company) will notify you (insert number of) working days in advance of your account being debited or as otherwise agreed.
- If an error is made by (A N Company) or your Bank or Building Society, you are guaranteed a full and immediate refund from your branch of the amount paid.
- You can cancel a Direct Debit at any time by writing to your Bank or Building Society. Please also send a copy of your letter to us.

A4 Instruction Version 2

3.8.3a1/3 A4 Direct Debit Instruction with Service User's 'official use box'

A N Company
logo or name

Instruction to your Bank or Building Society to pay by Direct Debit

DIRECT Debit

Please fill in the whole form using a ball point pen and send to:
AN Company, Any Street, Any Town, Anywhere.

Name and full postal address of your Bank or Building Society

To: The Manager   Bank/Building Society

Address

                              Postcode

Name(s) of Account Holder(s)

Bank/Building Society account number

Branch Sort Code

Service User Number

Reference

FOR (A N COMPANY) OFFICIAL USE ONLY
This is not part of the instruction to your Bank or Building Society.

Instruction to your Bank or Building Society
Please pay (AN Company) Direct Debits from the account detailed in this Instruction subject to the safeguards assured by the Direct Debit Guarantee. I understand that this Instruction may remain with (AN Company) and, if so, details will be passed electronically to my Bank/Building Society.

Signature(s)

Date

Banks and Building Societies may not accept Direct Debit Instructions for some types of account

1/3 A4 Instruction Form1

✂ —

This guarantee should be detached and retained by the Payer.

The Direct Debit Guarantee

DIRECT Debit

- ■ This Guarantee is offered by all Banks and Building Societies that take part in the Direct Debit Scheme. The efficiency and security of the Scheme is monitored and protected by your own Bank or Building Society.
- ■ If the amounts to be paid or the payment dates change (A N Company) will notify you (insert number of) working days in advance of your account being debited or as otherwise agreed.
- ■ If an error is made by (A N Company) or your Bank or Building Society, you are guaranteed a full and immediate refund from your branch of the amount paid.
- ■ You can cancel a Direct Debit at any time by writing to your Bank or Building Society. Please also send a copy of your letter to us.

3.8.3b1/3 A4 Direct Debit Instruction without Service User's 'official use box'

A N Company
logo or name

Instruction to your Bank or Building Society to pay by Direct Debit

DIRECT Debit

Please fill in the whole form using a ball point pen and send to:
AN Company, Any Street, Any Town, Anywhere.

Name and full postal address of your Bank or Building Society

To: The Manager   Bank/Building Society

Address

Postcode

Name(s) of Account Holder(s)

Bank/Building Society account number

Branch Sort Code

Service User Number

Reference

Instruction to your Bank or Building Society
Please pay (AN Company) Direct Debits from the account detailed in this Instruction subject to the safeguards assured by the Direct Debit Guarantee. I understand that this Instruction may remain with (AN Company) and, if so, details will be passed electronically to my Bank/Building Society.

Signature(s)

Date

Banks and Building Societies may not accept Direct Debit Instructions for some types of account

1/3 A4 Instruction Form 2

✂ —

This guarantee should be detached and retained by the Payer.

The Direct Debit Guarantee

DIRECT Debit

- ■ This Guarantee is offered by all Banks and Building Societies that take part in the Direct Debit Scheme. The efficiency and security of the Scheme is monitored and protected by your own Bank or Building Society.
- ■ If the amounts to be paid or the payment dates change (A N Company) will notify you (insert number of) working days in advance of your account being debited or as otherwise agreed.
- ■ If an error is made by (A N Company) or your Bank or Building Society, you are guaranteed a full and immediate refund from your branch of the amount paid.
- ■ You can cancel a Direct Debit at any time by writing to your Bank or Building Society. Please also send a copy of your letter to us.

3.8.4a. Small format Direct Debit Instruction – landscape

These minimum size Direct Debit Instructions can be used when printed in a journal or magazine.

A N Company
logo or name

Instruction to your Bank or Building Society to pay by Direct Debit

DIRECT Debit

Please fill in the form and send to: AN Company, Any Street, Any Town, Anywhere.

Name and full postal address of your Bank or Building Society

To: The Manager   Bank/Building Society

Address

Postcode

Name(s) of Account Holder(s)

Branch Sort Code

Bank/Building Society account number

Service User Number

Reference

Instruction to your Bank or Building Society
Please pay (AN Company) Direct Debits from the account detailed in this Instruction subject to the safeguards assured by the Direct Debit Guarantee. I understand that this Instruction may remain with (AN Company) and, if so, details will be passed electronically to my Bank/Building Society.

Signature(s)

Date

Banks and Building Societies may not accept Direct Debit Instructions for some types of account

A6 Instruction Form

3.8.4b. Small format Direct Debit Instruction – portrait

A N Company
logo or name

DIRECT Debit

Instruction to your Bank or Building Society to pay by Direct Debit

Please fill in the form and send to:
AN Company, Any Street, Any Town, Anywhere.
Name and full postal address of your Bank or Building Society

Service User Number

| | | | | | |

To: The Manager   Bank/Building Society

Address

Postcode

Name(s) of Account Holder(s)

Branch Sort Code

Bank/Building Society account number

Reference

Instruction to your Bank or Building Society
Please pay (A N Company) Direct Debits from the account detailed in this Instruction subject to the safeguards assured by the Direct Debit Guarantee. I understand that this Instruction may remain with the (A N Company) and, if so, details will be passed electronically to my Bank/Building Society.

Signature(s)

Date

Banks and Building Societies may not accept Direct Debit Instructions for some types of account.

A6 Instruction Form b

3.8.5 A4 Direct Debit Instruction with 'tear-off official use slip'

DIRECT Debit

A N Company
logo or name

Please fill in the whole form using a ball point pen and send to:
AN Company, Any Street, Any Town, Anywhere.
Name and full postal address of your Bank or Building Society

To: The Manager   Bank/Building Society

Address

_____

_____

                                      Postcode

Name(s) of Account Holder(s)

_____

Bank/Building Society account number

_____

Branch Sort Code

_____

Reference

_____

Banks and Building Societies may not accept Direct Debit Instructions for some types of account

Instruction to your Bank or Building Society to pay by Direct Debit

Service User Number

_____

Instruction to your Bank or Building Society
Please pay (A N Company) Direct Debits from the account detailed in this Instruction subject to the safeguards assured by the Direct Debit Guarantee. I understand that this Instruction may remain with the (A N Company) and, if so, details will be passed electronically to my Bank/Building Society.

Signature(s)

_____

_____

Date

✂ -

This is not part of the Instruction to your Bank or Building Society and must be detached by (A N Company) before submission to the Paying Bank

✂ -

This guarantee should be detached and retained by the Payer

The Direct Debit Guarantee

DIRECT Debit

■ This Guarantee is offered by all Banks and Building Societies that take part in the Direct Debit Scheme.
   The efficiency and security of the Scheme is monitored and protected by your own Bank or Building Society.

■ If the amounts to be paid or the payment dates change (A N Company) will notify you
   (insert number of) working days in advance of your account being debited or as otherwise agreed.

■ If an error is made by (A N Company) or your Bank or Building Society, you are guaranteed a full and immediate
   refund from your branch of the amount paid.

■ You can cancel a Direct Debit at any time by writing to your Bank or Building Society.
   Please also send a copy of your letter to us.

3.8.5 DDI+tear_off

3.8.6 A4 Bi-lingual Direct Debit Instruction (Welsh)

DIRECT Debit

A N Company logo or name
arwydd neu enw Unrhyw Gwmni

Please fill in the whole form using a ball point pen and send it to:
Cwblhewch y ffurflen gyfan gan ddefnyddio pen inc, ac anfonwch hi at:

A N Company	Unrhyw Gwmni
Any Street	Unrhyw Stryd
Any Town	Unrhyw Dref
Anywhere	Sir
AB1 2CD	AB1 2CD

Name(s) of Account Holder(s) / Enw(au) deiliad/deiliaid y cyfrif

Bank/Building Society account number
Rhif y cyfrif Banc/Cymdeithas Adeiladu

Branch Sort Code / Cod Didoli Cangen

Name and full postal address of your Bank or Building Society
Enw a chyfeiriad llawn eich Banc/Cymdeithas Adeiladu

To: The Manager
At: Y Rheolwr

Bank/Building Society
Banc/Cymdeithas Adeiladu

Address / Cyfeiriad

Postcode / Cod post

Instruction to your Bank or Building Society to pay by Direct Debit
Cyfarwyddyd i'ch Banc neu Gymdeithas Adeiladu i dalu drwy Ddebyd Uniongyrchol

Service User Number / Rhif Defnyddiwr Gwasanaeth

Reference / Cyfeirnod

Instruction to your Bank or Building Society
Cyfarwyddyd i'ch Banc neu Gymdeithas Adeiladu

Please pay (A N Company) Direct Debits from the account detailed in this Instruction subject to the safeguards assured by the Direct Debit Guarantee. I understand that this Instruction may remain with the (A N Company) and, if so, details will be passed electronically to my Bank/Building Society.

A fyddech cystal â thalu (Unrhyw Gwmni) o'r cyfrif a nodir ar y cyfarwyddyd hwn yn amodol ar y mesurau a sicrheir gan y diogelwch Gwarant Debyd Uniongyrchol. Deallaf y gall y cyfarwyddyd hwn aros gyda (Unrhyw Gwmni) ac, os felly, anfonir manylion yn electronig i'm Banc/Cymdeithas Adeiladu.

Signature(s) / Llofnod(ion)

Date / Dyddiad

Banks and Building Societies may not accept Direct Debit Instructions for some types of account
Gall Banciau/Cymdeithasau Adeiladu wrthod derbyn cyfarwyddiadau i dalu Debydau Uniongyrchol o rai mathau o gyfrifon

✂ -

This guarantee should be detached and retained by the Payer.

The Direct Debit Guarantee
Sicrwydd Debyd Uniongyrchol

DIRECT Debit

- This Guarantee is offered by all Banks and Building Societies that take part in the Direct Debit Scheme. The efficiency and security of the Scheme is monitored and protected by your own Bank or Building Society.
  Mae'r Cynllun Debyd Uniongyrchol yn cael ei warantu gan bob Banc a Chymdeithas Adeiladu sy'n cymryd rhan. Mae effeithlonrwydd a diogelwch y Cynllun yn cael ei fonitro a'i warchod gan eich Banc neu eich Cymdeithas adeiladu.

- If the amounts to be paid or the payment dates change (A N Company) will notify you (insert number of) working days in advance of your account being debited or as otherwise agreed.
  Os yw'r symiau sydd i'w talu neu ddyddiadau'r taliadau yn newid, bydd (Unrhyw Gwmni) yn eich hysbysu (nifer i'w ychwanegu) diwrnod gwaith cyn i'ch cyfrif gael ei ddebydu, neu fel y cytunwyd fel arall.

- If an error is made by (A N Company) or your Bank or Building Society, you are guaranteed a full and immediate refund from your branch of the amount paid.
  Os bydd (Unrhyw Gwmni) neu'ch Banc neu Gymdeithas Adeiladu yn gwneud camgymeriad, cewch sicrwydd ad-daliad llawn o'r swm a dalwyd eich cangen a hynny ar unwaith.

- You can cancel a Direct Debit at any time by writing to your Bank or Building Society. Please also send a copy of your letter to us.
  Gallwch ganslo Debyd Uniongyrchol unrhyw bryd trwy ysgrifennu at eich Banc neu Gymdeithas Adeiladu. Anfonwch gopi o'r llythyr hwnnw i ni hefyd, os gwelwch yn dda.

4   ADVANCE NOTICE

Introduction

Advance Notice is the method by which Service Users give notice to the Payer before the first Direct Debit is collected and following any changes to the Direct Debit collection in respect of amount, Direct Debit due date and / or frequency. The Advance Notice must be a clear and unambiguous personalised advice and must be identified as such at first glance by the Payer.

Where the Payer is paying on behalf of another person or party, the Advance Notice must be issued to the Direct Debit Payer, i.e. the person who signed the DDI. The Service User may also, at it's own discretion, and subject to proper consent having been received from the payer as required by the Data Protection Act 1998, advise the third party.

Written and electronic forms of the Advance Notice must be approved by the Service Users Sponsor before it can be issued by the Service User.

4.1   Contents of Advance Notice

The Advance Notice must be clear and provide the Payer with the following details.

- Total amount of Direct Debit to be applied to the Payer's account. If this is an amalgamation of more than one collection (where permitted) the amount of each collection forming part of the Direct Debit must also be shown

- Direct Debit due date (include date, month and year)

- Frequency of Direct Debit collection, where an Advance Notice is not issued for each collection or where an advance schedule of specific dates is not issued

- Direct Debit reference

- Advance Notice period

- Service User name and contact telephone number.

If the collection details are altered in any way a new Advance Notice must be sent to the Payer.

4.2   Time scales

The Service User may agree the period of Advance Notice with the Payer. The default period in the absence of any other agreement (the time allowed for receipt of the Advance Notice by the Payer) is a minimum of 10 working days plus postal time. When sending Advance Notice, sufficient postage time should be allowed to ensure the Payer receives the period of Advance Notice as agreed.

See section 7.1.4 and 7.2.4 for details.

- The Advance Notice period given to the Payer, prior to his account being debited, must be shown on the Direct Debit Guarantee. This Advance Notice period can however be varied by prior agreement with the Payer

- Service Users must collect the Direct Debit on or within 3 working days after the specified due date as advised to the Payer on the Advance Notice. Should the Service User fail to collect the Direct Debit as specified, further notification must be given to the Payer of the new collection date, or advice of collection amalgamation.

4.3   Valid Advance Notice

Advance Notice can be given in written, electronic form or orally. Proof to the Paying Bank that Advance Notice has been issued does not provide proof of receipt by the Payer.

- Service Users must clarify multiple collections / amalgamations. This information will assist the Paying Bank and the Service User to investigate any subsequent query which may be raised by the Payer in respect of the Advance Notice or the Direct Debit collection. The **preferred practice** is to avoid multiple collections / amalgamations and to use the one SUN, one contract procedure.

Government Departments, Public or Local Authorities

A Service User which is a Government Department or a public or local authority, collecting statutory amounts payable and where these amounts are subject to change, is required to provide individual Advance Notice to each Payer. The Scheme **does not** support advice being given in any statute or subordinate legislation duly passed or made by Parliament or where details of the change are given in a national publication, e.g. changes to VAT, insurance premium tax, etc.

Written notification

A Service User may give written notification to the Payer within the following documentation:

- a letter addressed to the Payer

- in a schedule where dates / amounts are known in advance

- *in a statement

- *in an invoice

- within a contract which may be issued between the Service User and the Payer.

* **N.B.** both of these must clearly display that collection is for Direct Debit, the amount to be debited and the debit due date, e.g. **"This invoice is for information purposes only. The amount due will be collected by Direct Debit on or immediately after …"**.

Electronic notification

Electronic notification may be given by the Service User on any form of electronic hardware. Use of electronic notification is at the Service User's risk as the duly authorised person may dispute receiving such advice.

Oral notification

Although the preferred method of Advance Notice is in written format it is accepted that in some instances, Service Users may find it necessary to give oral notification to the Payer. Service Users who do so must also accept the risk of a subsequent Indemnity Claim by the Paying Bank on behalf of the Payer who may dispute the Direct Debit. If the Service User wishes to provide the Payer with details of a series of future dated collections this must be provided in written or electronic form i.e. a schedule.

The Paying Banks cannot accept a voice recording transcript as proof of Advance Notice. However, this may be used by the Service User when in discussion with the Payer.

Notification of outstanding funds – contract cancelled

If a Payer cancels his contract and / or service with the Service User, then any outstanding sum may continue to be collected by Direct Debit, by arrangement with the Payer and provided that the existing DDI has not been cancelled. It is essential that proper and adequate Advance Notice be given to the Payer of the dates, amount and frequency of such collections.

Exceptional dispensation

Exceptionally, Advance Notice may not be required when direct action by the Payer requires the Service User to initiate a specific debit on his Bank account under an existing DDI (one off collections are not allowed by the Scheme except under AUDDIS). If any doubt exists guidance of the Sponsor must be obtained by the Service User before establishing an arrangement dispensing with the Advance Notice. Possible situations could be:

- Where a Payer requests the Service User to initiate a specific collection on his account under an existing DDI, for instance the Payer wishes to make an additional mortgage payment over and above the normal monthly payments, Advance Notice may be given by way of confirmation of the Payer's instruction at the time of the request, and the normal Advance Notice period will not apply. This procedure is only permitted where the additional collection arises in the context of an existing agreement

- when the Service User is required to debit the Payer's account following withdrawal of cash from an automated teller machine under the control of the Service User

- a written request received by the Service User from the Payer

- a request by the Payer to the Service User by means other than in writing but providing an audit trail.

4.4   Example of prohibited practices

- Oral notification of a future schedule of Direct Debit collections, where the amount and / or collection date is subject to change, is not sufficient. Such information must be given to the Payer in written or electronic form

- Announcement of any change in a professional journal or other publication is not adequate, without a separate letter addressed to the Payer. Clubs or professional institutions must issue each member with a separate notice of any change in the rate of subscription or the date of collection in accordance with Advance Notice requirements prior to that change taking place

- Advance Notices must not be sent with material which might have the appearance of 'junk mail' and thus risk being discarded before being read. If other (non-related) information is sent, to qualify as 'Advance Notice' the statement of collection changes must:

1. Be given precedence over other material.

2. Appear under the following prominent heading: 'Advance Notice of Direct Debit'.

- Direct Debits cannot be collected before the date specifically detailed on the Advance Notice. This applies whether or not the specified date is a working day

- Service Users must not use 'Advance Notice' as a mechanism for selling additional products or services in such a way that the Payer has to dispute the Advance Notice issued, i.e. Opt out, to avoid provision of the additional product or service and the associated increase in charge or premium.

4.5   Example of an Advance Notice

A N Company
Any Street
Any Town
Anywhere
AB1 2CD

Date

To: *Payers Name*
      Any Street
      Any Town
      Anywhere
      EF3 4GH

Service User Number and Name

Payer's Account Name: *A N OTHER*

Payer's Reference: *123456789 A N OTHER*

Notification of change to Direct Debit Payment, Due Date, Amount or Frequency.

With effect from .... Direct Debit payments due in respect of the above Direct Debit Instruction will now be for *£(amount)* and collected on or immediately after (date).

Should you have any queries in respect of this notification please contact (*Name & Telephone Number)*, otherwise the Direct Debit collection will be amended as detailed above.

Yours sincerely,

Company's representative

5 COMPLETION AND LODGEMENT OF THE DIRECT DEBIT INSTRUCTION

Introduction

The DDI once completed by the **Payer**, is sent to the Service User who must ensure that all the relevant information has been completed. This information is then input to the Service User's system and the DDI is dispatched by the Service User to the Payer's Bank for **lodgement**.

5.1 Completion of the Direct Debit Instruction

The DDI is the authority given by the Payer to his **Paying Bank** to allow the Service User to collect Direct Debits from his account. It is important that the Service User's name must be clearly shown on the DDI and on the Direct Debit record (Field 9 of the Bacs data record). Where collection of Direct Debits is being made in a different **trading name** this name must also be reflected on the DDI.

See section 2.2 for Standard Service User set-up.

The Payer is required to complete the following information on the DDI:

- name and full postal address of the Bank or Building Society of his account holding branch

- name(s) of the account holder(s)

- the sort code number of his account holding branch

- *his account number

- date and account holder's signature.

Clear instruction must be given to the Payer to return the completed DDI to the Service User who will lodge the DDI with the Payer's account holding branch.

Bilingual Instructions, e.g. English / Welsh, are acceptable, however the DDI information completed by the Payer must be completed in English.

***N.B.** The majority of the Paying Banks operate an 8 digit account numbering system.

5.2 Lodgement

The completed DDI must be lodged by the Service User direct with the Payer's account holding branch or dedicated processing centre. Service Users must lodge the DDI immediately or within 6 months from the date the DDI was signed by the Payer before collections may commence.

- Each DDI will be registered by the Paying Bank as a single authority given by the Payer for the collection of Direct Debits by the Service User. This is recognised by the Paying Bank as a DDI marked against the Service User's SUN and any reference allocated by the Service User

- The DDI must not have multiple SUNs or reference choices.

5.3 Rejected Direct Debit Instruction

- If rejected, the DDI is returned to the Service User immediately but no later than 3 working days from date of receipt by the Paying Bank.

- The Paying Bank will indicate on the returned DDI that lodgement has been refused e.g. unable to accept Direct Debit against account

- The Banks reserve the right to refuse lodgement of a DDI without giving a reason for doing so. In such a case the DDI will be returned to the Service User marked 'lodgement refused'

- When a Service User receives a returned DDI which has been rejected, the Service User must contact the Payer to arrange an alternative payment method

- Some Paying Banks process DDIs centrally. In this event the Service User may receive a covering 'lodgement referred or rejected' form for a number of rejected DDIs. The reason for refusal may be indicated either on each DDI or on the form as shown in the example

- Only **variable** amount DDIs are supported by the Scheme. Service Users must not send **fixed amount or date DDIs** to Paying Banks for lodgement as these are not valid DDIs under Scheme Rules.

See section 5.7 for an example of a DDI rejection form.

5.4 Service Users responsibilities

Service Users must allow a minimum of 10 working days from date of despatch for the Paying Bank to action the DDI before the first collection is presented. The first collection date cannot be prior to, but must be within 3 working days of the collection date specified to the Payer in the Advance Notice.

See section 4 for Advance Notice.

All new Service Users are required to use a **core reference** of a minimum of 6 alpha-numeric uppercase characters on the DDI. However, it is recognised that Service Users may not generate their reference until after the Payer has signed the DDI. In these circumstances, where the Payer has signed a DDI without a reference, only one reference may be used. The Service User must include this reference on all Direct Debits (**Field 10** of the Bacs data record).

See Appendix 3 Core Reference.

5.5 Paying Bank's responsibilities

Upon receipt of the DDI the Payer's Bank will validate the DDI i.e. will confirm that the Payer is one of its customers and that the DDI has been properly executed. If accepted the DDI information is recorded in the Paying Bank's customer Direct Debit records. If rejected the DDI will be returned to the Service User immediately but no later than 3 working days from date of receipt.

- Paying Banks have the right to refuse completed DDIs without giving a reason. In particular they will generally refuse completed DDIs which do not comply with the rules set out in this Guide

- Paying Banks may confirm Payer details to a Service User but are not under any obligation to do so or to disclose any additional information about the DDI or Payer's Bank details to Service Users. Any information so given is given in good faith but neither by giving such information nor by declining to give information does the Paying Bank assume any responsibility to the Service User.

5.6   Example of prohibited practices

- Service Users must not request the Payer to lodge the completed DDI direct with the Paying Bank

- Service Users must not accept a DDI with any amendments made by the Payer (e.g. amount, frequency or collection date). If a DDI is accepted with amendments the Service User will be liable for any resulting Indemnity Claims

- Service Users must not use **fixed amount / date DDIs**, as these are not supported by the Scheme

- Service Users must not request the Paying Bank to acknowledge the receipt of a DDI in any format e.g. by telephone or letter, before the first Direct Debit is presented.

5.7 Example of Bank Bulk DDI Lodgement Referred / Rejected form

This form is used by Paying Banks to inform Service Users of reasons for referring back for checking, or rejecting a DDI submitted for lodgement.

ABC BANK
Any Street
Any Town
Any Where
AB1 2CD

Date

DIRECT DEBIT INSTRUCTIONS - UNABLE TO ACTION

The attached Direct Debit Instruction(s), cannot be processed for the following reason:

Invalid Sort Code	
Invalid Account Type	
Invalid Instruction	
Account Not Held/Closed	
Account Name Differs	
Insufficient/Invalid Account Details	
Direct Debits Not Permissible On This Particular Account	
Lodgement Refused	
No Reference	
No Signature	
Other - Please Specify _____	

If appropriate, please arrange for the Instruction to be completed with valid details and returned to this office.

Manager   Branch stamp

Date _____   _____

6 DIRECT DEBIT INSTRUCTION ACKNOWLEDGEMENT

This Section has been deleted as the DDI Acknowledgement, formerly known as Part B, was withdrawn on 1st January 1998.

7 THE COLLECTION PROCESS

Introduction

This is the process whereby Service Users collect Direct Debits from its Payers who have completed DDIs. This process starts when the DDI has been successfully **lodged** with the Paying Bank. The management and timing of the collection is the Service User's responsibility.

In order to do this the Service User must maintain up-to-date records and processes designed to ensure that the collection is made accurately and in a timely manner.

7.1 Method

7.1.1 Payer's records

A Service User must maintain information for all its Payer's current records. This should cover information in respect of:

– lodgement of new DDIs

– amendments and cancellations

– record of amounts and date of payments collected including identification of initial, re-presented and final Direct Debits.

Failure to do this may result in a higher proportion of unpaid or unapplied debits, Indemnity Claims and will also affect customer service.

Management Administration

A Service User may contract an organisation to manage its Direct Debit application. However, the Service User must take full responsibility for the actions of the other organisation operating on its behalf. This action includes:

– corresponding with the Payer, receipt of completed DDIs and lodgement with the Paying Banks

– management of returned, amended and cancelled DDIs

– management of collection files sent to Bacs and the collection of Direct Debit records on the collection due date(s). Reconciliation of processed, rejected and returned items

– applying the collected funds to the Service User's account.

7.1.2 Facilities for maintaining current records

Modulus checking – Most Paying Banks operate a modulus checking facility within their systems which checks the sort code and account number combination. This information is also available to Service Users and may be used to check the Payer's account details before collections are sent to Bacs.

Industry Sorting Code Directory – A file that contains all centrally held information about the Bank and Building Society branches and offices that are connected to any of the UK clearing systems. This information is available to Service Users through Bacs and may be used to check the Payer's Bank sort code.

Crediting and Debiting Building Society accounts – A Service User's Guide – For Service Users who apply Direct Debits to Building Society accounts, a register is maintained which details the correct sort code and account number combinations for those which accept debits. This information is available to Service Users and may be used to check the Payer's account details.

7.1.3 Reference

All new Service Users are required to use a **core reference** of a minimum of 6 alpha-numeric, uppercase characters on the DDI. The Service User must include this reference on all Direct Debits (**Field 10** of the Bacs data record).

7.1.4 Collection amalgamation

It is strongly recommended that Service Users use the preferred best practice of a one contract – one DDI, approach, with a reference identifying both the DDI and the Direct Debit collection. Using this practice will eliminate risk of confusion by all parties concerned.

Service Users who currently collect more than one individual collection under a single DDI, should consider reverting to the one contract – one DDI, approach when changing their systems (hardware / software) or when migrating to **AUDDIS**. It is advisable for Service Users to contact their Sponsor prior to applying any changes, in order that they may be advised of the best way forward when planning this activity.

7.2 Preparation and submission of Bacs files

Full details of the Bacs input requirements are specified in the **Service User Guide – Bacstel-IP and the Electronic Funds Transfer – File Structures**. Service Users can obtain a copy of these documents from their Sponsor.

The Service User will extract all the Direct Debits due for collection from its computer records and generate an input file which is submitted to Bacs for processing. This file must be submitted at least 2 working days before the Direct Debit due date, see **Bacs cycle**.

Automated input is not restricted to organisations having their own computers. Prospective Service Users without such equipment are invited to discuss with its Bank the computer services which can be made available.

Commercial Computer Bureaux

A Service User may contract a **Commercial Computer Bureau** to produce and submit its Direct Debit collection files to Bacs for processing. The Service User must ensure that all collection details, are correctly advised to its bureau in time to meet the collection schedule. The bureau will generate and submit the Bacs file in time for the Direct Debit collection due date(s).

7.2.1 The Bacs cycle

The function of **Bacs** is to process automated data containing records of Direct Debits written to a standard format, for onward transmission to destination Bank accounts.

Day 1 – Input	Day 2 – Processing	Day 3 – Entry
Service User transmits automated data in accordance with the timetable laid down in the Service User Guide – Bacstel-IP.	All data accepted is processed (the working day before Entry day).	Direct Debits and associated contra entries are debited / credited to destination Bank accounts on this day.

7.2.2 Transaction codes

Direct Debits must be sent to the Payer's sort code and account number and each Direct Debit record must be submitted with the appropriate transaction code. The transaction code indicates the status of the Direct Debit collection, as detailed below:

- Transaction code 01 – For first collections, i.e. the first Direct Debit originated following the receipt at the Payer's Bank branch of a new DDI, transferred DDI or where an existing DDI has been reinstated.

With effect from 1 January 1998, the successful processing of a Direct Debit with transaction code 01 (in respect of a first payment on a new DDI) should be construed by the Service User that the Paying Bank holds a DDI. This does not apply to **AUDDIS** Service Users. If a Direct Debit using transaction code 01 is returned unpaid for any reason except for 'Refer to Payer' it may be presented again, providing it is appropriate to do so. In this case transaction code 01 must be used and a new Advance Notice sent to the Payer. However, if a Direct Debit using transaction code 01 is returned unpaid 'Refer to Payer' it must only be represented with transaction code 18. Under these circumstances, a Service User is still protected and will be able to raise a Counter Claim if the Paying Bank subsequently raise an Indemnity Claim for the reason 'No Instruction Held'.

- Transaction code 17 – For the collection of all Direct Debit payments, this code is used to indicate the collection of a standard Direct Debit, i.e. not a first, final or re-presented Direct Debit.

- Transaction code 18 – For **re-presentations**.

A re-presentation must always be submitted with transaction code 18.

- Transaction code 19 – For final collections.

Paying Banks will mark the Direct Debit Instruction as expired when a Service User uses transaction code 19.

The use of these transaction codes is mandatory and Service Users must provide for them in their systems design.

7.2.3   Payer details

The Payer's name (**Field 11** of the Bacs data record) must quote the Payer's account name. This may not necessarily be the Service User's customer.

7.2.4   Collection date, amount and frequency

It is the Service User's responsibility to ensure collection is made on the due date, i.e. the date advised to the Payer within the Advance Notice. Collection must be made on or immediately after (within 3 **working days**) the due date. Should the Service User fail to collect the Direct Debit as specified further notification must be given to the Payer, quoting the new collection date or giving advice of collection amalgamation.

Where the Service User has collected more than intended / advised to the Payer, the Service User should confirm in writing direct with the Payer, the appropriate refund arrangements.

It is advisable for Service Users to offer a choice of collection dates to its customers. This would offer budgeting options and may reduce the number of unpaid Direct Debits returned by the Paying Banks due to lack of funds.

7.2.5   Service User's account

This must be in the name of the Service User and held by the Sponsor.

7.2.6   Dormancy

All Paying Banks hold details of Payer DDIs on file for a minimum period of 13 months from **lodgement** of the DDI in the event of no collections or from the date of the last collection. i.e. length of time in calendar months after which a Paying Bank will drop details of a DDI because no Direct Debit has been collected.

A Service User requiring all DDIs under an SUN to be held for more than 13 months, from either lodgement or last collection, must apply to its Sponsor. Requests will be reviewed to ensure that the Service User, in its normal course of business, does require a **dormancy period** greater than 13 months. The Sponsor will advise the Paying Banks of a Service User's extended dormancy period. Extensions will not be approved for Service Users where there is concern that a number of Instructions may lapse if it has agreed with its Payer to suspend collections. Under these circumstances the Service User must obtain a new DDI from the Payer and lodge in the usual way.

Where a Service User has agreed to suspend collection of Direct Debits for a period which exceeds the Service User's dormancy period, the Service User must obtain a new DDI from the Payer and lodge it with the Paying Bank.

If a Service User does not present a Direct Debit against a DDI for 13 months, and has not requested an extended dormancy period, any subsequent Direct Debit must be preceded by a new DDI, otherwise the Direct Debit shall be returned 'No Instruction'.

7.2.7 Service User's short name

All Direct Debits claimed by a Service User must be collected in the same name that appears on the DDI signed by the Payer.

The description in **field 9** of the Bacs Direct Debit collection provided for the Service User's name is restricted to 18 characters. When abbreviation of the name is necessary, it must be a recognisable form of the name quoted in the DDI, as this may appear in Bank records, including the Payer's Bank statement.

Paying Banks reserve the right to amend the Service User's name on the Direct Debit record if the name quoted is not recognisable, but are under no obligation to do so.

See sections 2.2 and 2.3 for information on the use of Service User short names and trading names.

7.2.8 Monitor / control facilities

These facilities are detailed in the Service User Guide – Bacstel-IP. There are a number of facilities available to the Sponsors and Service Users which may be used to monitor / control the Service User's input, e.g.

Service User control

- **Individual item limit** – This facility enables the Service User to monitor individual collections and ensure these are within a set figure. Any items exceeding this limit will be detailed on the Service User's input report

- **Audit trail** – This facility provides an audit trial for Service Users, who may request items to be selected at random and printed on the input report.

Sponsor control

- **Bacs account limit** – The Sponsors may apply a limit against a Service User's **nominated account**. Account overlimit referrals are given to the Service User's Sponsor who must give their authority to process or extract the submission if appropriate.

7.3 Bacs reports

The Bacs generated reports must be accessed by the Service User via Bacstel-IP and the Bacs payment services website. The Service User will be responsible for reconciliation of items processed, rejected, returned, amended and cancelled Direct Debit / DDIs.

Input Reports

- Produced on day 1 of the Bacs cycle and available to download via Bacstel-IP and the Bacs payment services website. The input report is Bacs formal acknowledgement to the Service User that its collection file has been processed. The report will detail the total number and value of the Direct Debits processed and will list any amended or rejected items which have failed Bacs validation e.g. invalid destination sort code

- Service Users must check this report and action any items returned or rejected as appropriate. This process may require contact with the Payer to establish the validity of the original DDI information and if necessary the Service User must obtain a new DDI.

Automated Return of Unpaid Direct Debit (ARUDD)

Paying Banks perform modulus checks against each Direct Debit record. If an account number fails the modulus check the Paying Bank may return the Direct Debit unapplied. An item which passes the modulus check may still be returned as unapplied for various reasons e.g. account closed, the account number does not exist, etc.

- Unpaid Direct Debits are normally returned by the Paying Banks via the **Automated Return of Unpaid Direct Debit** service (**ARUDD**) and returned items debited to the Service User's account on **day 5** or in exceptional circumstances **day 6** of the cycle. Each returned item will include a 'reason code'. Service Users should check the report and take the appropriate action in respect of any unpaid Direct Debits.

When a Direct Debit is returned unpaid with the reason code 'Refer to Payer' this may be as a result of lack of funds, in which case the Service User may re-present the Direct Debit using transaction code 18 on a new collection date.

If the final Direct Debit (transaction code 19) is returned by the Paying Bank unapplied the Service User may represent the Direct Debit only with a transaction code of 18. If it is represented with any other **transaction code** it may not be accepted. Re-presentation must be made within a month from the original debit day and for the same amount.

7.4 Amendment Advices

The Service User may receive amendment advices from the Paying Bank.

Advice of incorrect details

- Where the Payer's sort code and / or account number has not been correctly detailed on the Direct Debit, the Paying Bank may apply the Direct Debit and provide advice of the correct details to the Service User either: via the Automated Direct Debit Amendment / Cancellation Service (**ADDACS**), via a Zero Account voucher, or by manual advice. Service Users must apply these changes to their data file no later than 3 working days from receipt, thus ensuring that future Direct Debit collections are submitted with the correct information.

See section 10.1 for Paying Bank generated advices.

Re-instatement advice

- A Payer may request his Paying Bank to re-instate a DDI up to 2 months following cancellation. When a re-instatement advice (ADDACS Code R) is received from a Paying Bank the Service User must confirm this action with the Payer and issue an Advance Notice.

See section 4 for full details on Advance Notices.

7.5 Payer cancellation of contract direct with the Service User

Where a Payer has given advice to the Service User to cancel the contract, this will be taken as a cancellation advice for the DDI. If the Payer owes outstanding funds to the Service User in respect of the contract, the Service User must clarify the collection method to be used to collect these outstanding funds.

See section 4.3 for details on 'Notification of outstanding funds'.

7.6 Error recovery

This section details procedures, timings and actions to be taken by the Service User in the event of errors in the collection file submitted to Bacs.

7.6.1 Single item collected in error

The guidelines detailed below should be followed by Service Users in the event of a single item error:

Before debit due day	**If Bacs file has not been submitted:** The Service User must make every effort to correct the error and recreate the Bacs file with the correct data. **If the collection file has already been dispatched to Bacs for processing:** The Service User must contact its account holding branch on the debit due day. See action detailed below 'debit **due date** plus 1'.
Debit due day plus 1	The Service User should contact the Payer's Bank branch to request the Payer's account to be recredited. Payer's Bank branch to credit the Payer's account and raise an Indemnity Claim with the Service User. The reason for the claim will be detailed as 'claim requested by Service User'. The Service User cannot counter claim in this instance. **Note: Paying Banks may request the Service User to provide its request to them in writing.**

7.6.2 Majority of submission in error

The guidelines detailed below should be followed by Service Users in the event of an error with the majority of, or the whole submission:

Up to and including Bacs input day	The Service User must call its Sponsor who will arrange to extract the file from the Bacs system, subject to Bacs processing timescales. The Service User is responsible for correcting the error, recreating the Bacs file and submitting it to Bacs for processing. If the Service User fails to collect on or within 3 working days of the original debit due date, it must issue further Advance Notice to the Payer confirming the amount to be collected and the new collection date.
Processing day plus 1	Immediately the error is detected the Service User must contact its Sponsor who will advise of the appropriate action to be taken. This will include arrangements to reimburse the Payer. The later the error is detected the more complex the recovery and reconciliation procedure will be.

Notification to the Payer [Applicable to 7.6.1 and 7.6.2 above]

Where it has not been possible to extract the erroneous file before it is processed by Bacs, the Service User must:

– give advice of the error to the **Payers** affected, detailing the appropriate recovery process

- confirm the new collection date and amount to the Payer, if the collection is to be made more than 3 working days after the original due date. The Service User must also confirm it will meet any Bank charges incurred by the Payer as a result of the error

- issue the advice to the Payers on the date the error is detected but no later than 3 working days from this date.

N.B. In the case of 7.6.2 above, the Sponsor must be kept informed of progress. It would be advisable for a Service User to advise its Press Office in order that they may prepare a statement in anticipation of the issue being advised to the press.

These procedures apply to any error relating to a Direct Debit that has been collected in error, regardless of whether it is collected before the due date or a double debit, for example.

7.6.3 Service User's system error

Service Users must have contingency arrangements available to ensure their Direct Debit collection process is unaffected or there is minimum disruption to their collection process should a system error occur. It is the Service User's responsibility to ensure collected funds are applied on the debit due date.

If the system problem is not corrected in time to allow the Service User to submit its Bacs file on the required input day, it must contact its Sponsor, as early as possible, who will advise on the appropriate options available.

Notification to the Payer

If on account of a system error, the Service User fails to collect on or within 3 working days of the debit due date, the Service User is required to inform the Payers affected, detailing what action has been taken and confirm the new collection date and amount.

7.7 Paying Bank's responsibilities

The Payer's branch will accept Direct Debits originated under the DDI upon the understanding that it will not verify or check that:

- the collection conforms to the terms of that DDI.

OR

- any purpose or condition of collection expressed in that DDI is fulfilled.

7.8   Example of prohibited practices

- New DDIs indicating collection of fixed amount and / or fixed date Direct Debits will not be permitted. Only variable amount DDIs are supported by the Scheme

- Collecting Direct Debits using **paper vouchers** is not allowed by the Scheme

- Where a DDI is held, the Service User must not ask the Paying Bank to make collection by any other means.

7.9 Example of a letter issued to the Payer by the Service User advising of a debit applied to his or her account in error

This letter is only to be used where an error has been made and the Payer needs to be advised of the appropriate remedial action.

Our Ref: xxx

Date: xxx

AN Company
Any Street
Any Town
Anywhere
AB1 2CD

Name
Any Street
Any Town
Anywhere
EF3 4GH

Dear (contact name)

Reference: Direct Debit Error

Due to an error by xxxxxx (Service User's name), an incorrect Direct Debit was applied to your account for a value of £xxx on xxx (date). With the assistance of the Banks and Building Societies we have rectified the error by requesting your account holding branch to recredit your account with the value of the erroneous debit on xxx (date).

The correct value of £xxx will now be collected on xxxx (date) and any future Direct Debits will be collected on the xx day of the month as previously advised. *See Note.

We would like to apologise for the error and any problems this may have caused you and assure you that providing excellent customer service remains our highest priority. If your account has incurred charges as a direct result of our error, please send us the necessary details (for example a copy of your Bank or Building Society statement) so that we can reimburse you. Should you have any further concerns regarding this matter, please call or write to xxxxxxxxxxxxxx. quoting the reference at the top of this letter.

Yours sincerely,

xxxxxxxxxxxxxxxxx

* Note only to be used where Advance Notice is required giving advice of new collection date.

8   UNPAID DIRECT DEBITS

Introduction

When a Direct Debit is not paid by the Paying Bank it will be returned unpaid to the Service User on the day of presentation or exceptionally on the following working day. Unpaid Direct Debits fall into 3 categories.

1. When the Paying Bank is giving advice of change of circumstances to the DDI or the Payer's account to the Service User, e.g. Instruction cancelled.

2. Where the Payer disputes the due date, amount or frequency of a Direct Debit either following receipt of an advance notice or as a result of an outstanding dispute with the Service User, e.g. single payment stop.

3. Where the Paying Bank is referring the collection back to the Service User as notification of non-payment e.g. Refer to Payer.

For categories 2 and 3 above the Service User has the option to re-present an unpaid Direct Debit to the Paying Bank for settlement.

N.B. In this section the DDI is referred to as 'INSTRUCTION'.

8.1   Reasons for return

A Direct Debit may be returned unpaid for a variety of reasons, these are detailed below with the appropriate reason codes:

Reason	Meaning of Return Code	Return Code
a) The Payer's Bank is not in a position to pay the Direct Debit; (For some reason other than the exception below) **OR** The service of a **Third Party Debt Order** (formerly Garnishee Order) or **Arrestment** on the Payer's account, his bankruptcy, liquidation or the appointment of a receiver to manage his affairs.	REFER TO PAYER	0
b) The Instruction of the Payer has been cancelled by the Payer or the Payer's Bank.	INSTRUCTION CANCELLED	1
c) Payer deceased – Instruction cancelled	PAYER DECEASED	2
d) The account of the Payer has been transferred to another Bank.	ACCOUNT TRANSFERRED	3
Continued on next page		

Reason	Meaning of Return Code	Return Code
e) The Payer has disputed the Advance Notice given (disputed timing, amount or frequency) and has requested a single payment to be stopped.	ADVANCE NOTICE DISPUTED	4
f) Account number is not recognised at the Paying Bank.	NO ACCOUNT	5
g) No Instruction held with Paying Bank.	NO INSTRUCTION	6
h) The amount of the Direct Debit differs from the amount specified in any existing fixed Instruction or Advance Notice to the Payer.	AMOUNT DIFFERS	7
i) The date of debiting is in advance of the due date specified in any existing fixed Instruction or Advance Notice to the Payer.	AMOUNT NOT YET DUE	8
j) The date of the presentation is more than 3 working days after the due date specified in any existing fixed Instruction or Advance Notice to the Payer. **OR** For re-presentations the Direct Debit has been re-presented more than one month after the original Direct Debit date.	PRESENTATION OVERDUE	9
k) The identity of the Service User differs from that specified in the Instruction.	SERVICE USER DIFFERS	A
l) Account closed. The Payer has closed his account for an unknown reason. (If Direct Debiting is to continue in such a case the Service User must obtain a new Instruction.)	ACCOUNT CLOSED	B

The above codes are subject to review and a Service User should take this into account when designing its system. Further information on how individual codes should be dealt with is detailed in Appendix 2.

8.2 The Unpaid cycle

Day 1	Day 2	Day 3
Submission of DD collection file to Bacs 'date stamp'	Bacs Processing Day	Debits applied to Payer's account
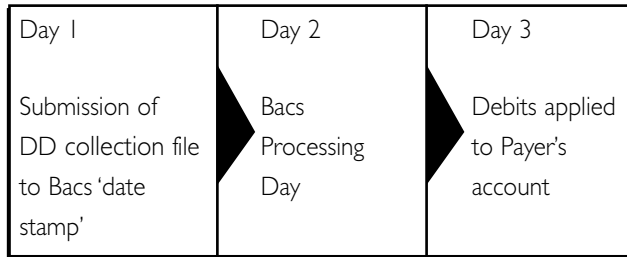
See section 8.6 Reasons for Return 'Date Stamp'.

Unpaids returned automatically

Day 3(or 4)	Day 4(or 5)	Day 5(or 6)
Payer's branch send unpaids to Bacs. Bacs validate returns and matches processing date to original DDs under this cycle.	The Automated Return of Unpaid Direct Debits Report is available to download via **Bacstel-IP** and the Bacs payment services website. Details of unpaids available to Service User's Bank.	Service User's accounts debited automatically. The Automated Return of Unpaid Direct Debits Report is available to download via Bacstel-IP and the Bacs payment services website.

Unpaids returned manually

Day 3(or 4)	Day 4(or 5)*	Day 5(or 6)
Payer's branch post (via first class post) advices of unpaids to Service User's branch.	Service User's branch debits Service User's account on receipt of advices and advise Service User. *Subject to postal delays.	Service User receives details of unpaids.

With both automated and manual unpaid Direct Debits the Service User will receive details of the original transaction code and the reason for return.

Most Paying Banks' returned unpaid Direct Debits are processed electronically via Bacs. Service Users wishing to receive details of unpaid Direct Debits in automated form should seek the advice of its Sponsor(s).

If the advice of an Unpaid Direct Debit is lost or delayed in the post and the Payer's Bank can produce documentary evidence confirming that the Direct Debit was returned unpaid within the correct time scale, then the Payer's Bank is entitled to reimbursement. The Service User's Bank should debit the Service User's account under advice, providing this is within 3 months from the original unpaid date.

8.3 Time scales

A Direct Debit will be paid, or returned unpaid by the Paying Bank on the day of presentation or exceptionally on the following working day under the following circumstances:

– due to lack of funds

– because collection has been stopped by the Payer no later than close of business on **entry day**

– because the account has been closed

– because the Payer's Instruction has been determined. e.g. death

– the lodgement of an Arrestment or Third Party Debt Order (formerly Garnishee Order) no later than close of business on entry day.

Bacs can only accept returns if they match original Direct Debits submitted under the current processing cycle and which are received on day 3/4. Service Users should seek advice from its Sponsor in the event of any queries.

An unpaid Direct Debit will be debited from a Service User's account either 2 or 3 days after the original Direct Debit entry day.

8.4 Returned Unpaid Direct Debits

Direct Debits may be returned unpaid by one of the following methods:

– by automated means via Bacs (**ARUDD**)

– manually, by use of the "Advice to Service User of an Unpaid Direct Debit" form sent by first class post to the Service User's Bank. Unpaid Direct Debits are debited to the Service User's account. The flow charts above (8.2) details the process and time frame for both automated and manual Unpaid Direct Debits. Settlement may be sent by the Service User's Bank via Bacs but must be directed to the account specified on the Bank Giro Credit attached to the unpaid advice. This must also quote the reference detailed on the Bank Giro Credit.

8.5 Example of prohibited practices

It is unacceptable for a Paying Bank to send a manual advice of unpaid Direct Debit direct to a Service User. The advice must be sent by first class post to the Service User's Bank branch.

8.6 Example of Bacs Unpaid Direct Debit report

Bacs Automated Return of Unpaid Direct Debits Reports are produced for each Service User. Separate sections are provided for unpaids returned on day 3 and day 4 respectively, with further sub-sections for each nominated account involved.

LIST OF AUTOMATED UNPAID DIRECT DEBITS RECEIVED FOR A N COMPANY LTD.

(1) SERVICE USER NUMBER 123456

ANY BANK
BRANCH NAME ANY BRANCH, ANY TOWN
(2) SORT CODE 83-99-99 ACCOUNT NUMBER 12345678

REFERENCE	AMOUNT	RETURNED FROM NAME	SORT CODE	ACCOUNT	TRANS CODE	REASON FOR RETURN	ORIGINAL BACS PROCESSING DATE
BAK/789/HC/3456	£15.00	BAKER E F	53-78-54	76543210	17	4199 - ADVANCE NOTICE DISPUTED	18 JUL 96
BEL/456/CI/8765	£10.00	BELL G	61-87-65	87654321	17	0199 - REFER TO PAYER	18 JUL 96
BRO/123/LP/9876	£15.00	BROTHERS C J	78-98-76	98765432	01	5199 - NO ACCOUNT	18 JUL 96
		TOTAL 3 ITEMS FOR £40.00					

This report, available for downloading via Bacstel-IP and the Bacs payment services website on day 4(5) of the unpaid cycle, details the Direct Debits that have been returned unpaid by the Paying Banks. The report lists all returned Direct Debits for each **Service User Number** for any one processing day. If the Service User submits Direct Debits for processing on consecutive working days this may result in some transactions for two consecutive days being displayed on one advice where the Paying Banks may have applied late returns.

An explanation of the report information is detailed below:

(1) Service User Number – Service User Number

Bank – Service User's Sponsoring Bank

Branch name – Name of Bank branch which holds the Service User's account.

(2) Sort code – The sort code number of the Service User's account.

Account number – The Service User's account number.

Reference	– The reference quoted by the Service User on the Direct Debit record.	
Amount	– Amount of Direct Debit.	
Returned from name	– The Payer's account name as quoted on the Direct Debit record.	
Sort code	– The sort code number of the Payer's account.	
Account	– The Payer's account number.	
Trans code	– The transaction code quoted on the Direct Debit record.	
Reason for return	– The first character will give the reason code for return, characters 2-4 is the original processing date of the Direct Debit record as date stamped by Bacs, followed by description of the reason for return.	See section 8.2 day one of cycle.
Original Bacs Processing day	– The original processing date is quoted and corresponds to the characters 2-4 of the reason for return.	

8.7 Example of a Manual Advice to the Service User of an Unpaid Direct Debit (most Paying Banks make Automated Returns but there are some exceptions)

Advice to Service User
of a manually unpaid Direct Debit

DIRECT Debit

From: The Manager _____ Bank/Building Society

Address _____

_____

_____ Postcode _____

Dear Sir,

Please credit us by return with the sum of **£** _____ in respect of an unpaid automated Direct Debit the details of which are shown below. Please use either: – the automated settlement system (quoting the sorting code, amount and serial number on the attached bank giro credit); or
– the attached bank giro credit

Details of unpaid automated Direct Debit:

Transaction Code _____

Date Processed
(business day before Debiting Day) _____

Payer's
Account Name _____

Payer's Account Number [| | | | | | | |]

Payer's Sort Code –
returning Debit [| | | | |]

Originating Account Details:

Service User's
Short Name _____

Service User's
Account Number [| | | | | | | |]

Service User's Reference
(as an automated entry) [| | | | | | | | | | | | | |]

Service User's SUN [| | | | | |]

Reason Code _____

Tick as appropriate

☐ **0** Refer to Payer	☐ **6** No Instruction
☐ **1** Instruction Cancelled	☐ **7** Amount Differs
☐ **2** Payer Deceased	☐ **8** Amount not yet due
☐ **3** Account Transferred to another Bank/Building Society	☐ **9** Presentation Overdue
☐ **4** Advance Notice Disputed	☐ **A** Service User Differs
☐ **5** No Account	☐ **B** Account Closed

Date _____

Branch Stamp

Yours faithfully _____ Manager

02/13 07/09/07 (part 1)

From: _____ Bank

_____ Branch

Date: _____

Re Settlement of:
Refund Request by: _____ (Service User)

bank giro credit

Bank and Branch	Branch Sort Code	Account Name and Number	Amount
Reference [ ]		Direct Debiting Supreme A/c Payer :	
	Sorting Code Number	Account Number	Amount
	[					]	[							]	£ [ ]

Please do not write or mark below this line or fold this voucher

9   RE-PRESENTATION OF AN UNPAID DIRECT DEBIT

Introduction

A re-presented Direct Debit is a debit which has been previously returned unpaid by the Paying Bank and is presented again by the Service User for collection.

See section 8 for full details.

9.1   Authority to re-present

The consent of the Payer to debit his or her account, as expressed in the DDI, also constitutes implied consent to the re-presentation of an unpaid Direct Debit originated under that authority. It does not arise from the existence of a debt owed by the Payer to the Service User.

Re-presentation must only occur when the Service User may reasonably assume that the conditions necessary for collection will be met.

9.2   Application

An unpaid Direct Debit must only be re-presented by the Service User if the following criteria are met:

– re-presentation takes place within one month of the date on which first presentation was made.

– the amount of the re-presented Direct Debit is the same as that originally dishonoured.

– it is identified by the use of transaction code 18.

If the final Direct Debit, in a series of payments, (transaction code 19) is returned unpaid by the Paying Bank, the Service User must re-present the Direct Debit with transaction code 18. If it is re-presented with a transaction code of 01, 17 or 19 it may not be accepted.

See section 7.2.2 for use of Transaction Codes.

9.3   Time scales

Re-presentation of an unpaid Direct Debit **may continue for one month** from the date on which first presentation was made. If payment has not been made within this period, the Service User must make other arrangements directly with the Payer for collecting the amount due or give Advance Notice of the new collection date and amount, or advice of collection amalgamation.

See section 4 for details of Advance Notice.

Best Practice Standards

If a Direct Debit is returned unpaid by the Paying Bank it is recommended that the Service User should liaise with the Payer to offer a new collection date. A Service User should give at least 5 working days notice to the Payer of the new collection date.

10   DIRECT DEBIT INSTRUCTION AMENDMENT AND CANCELLATION

Introduction

At any time the Payer can choose to amend or cancel his DDI by giving his Bank branch authority which will be effective immediately. In addition there are circumstances which require the Paying Bank to give advice to the Service User of a change to the DDI e.g. branch mergers.

The advice may be received in one of the following formats:

Paying Bank generated

* Automated or manual amendment / cancellation advice

* **Zero account number advice voucher**

* An unpaid Direct Debit advice.

Service User generated

* SUN / Reference Change.

Payer generated

* Advice of cancellation from the Payer to the Service User.

Service Users must apply DDI amendments and cancellations immediately or within 3 working days from receipt or as specified by the Payer to ensure the accuracy of the Direct Debit collection.

Where a Payer has given advice to the Service User to cancel the contract this will normally be taken as a cancellation advice for the DDI, however, where the Payer owes outstanding funds to the Service User in respect of the contract the Service User may, with the Payer's agreement, continue to use Direct Debit as the method of collection.

10.1 Paying Bank generated advices

Having received notification of a change to the DDI from the Payer, the Paying Bank will inform the Service User. This notification will be issued either electronically using the Automated Direct Debit Amendment and Cancellation Service (ADDACS) or by a manual advice. The majority of the Paying Banks use ADDACS. They send their DDI amendments / cancellations via Bacs who provide this information to the Service User either electronically or as a report, which is available to download via Bacstel-IP and the Bacs payment services website. Advice may also be given in the form of an **Unpaid Direct Debit** with the appropriate reason code.

Additionally where the status of the Paying branch has changed (e.g. branch closure / merger) and the Direct Debit is addressed to the old details, the Bacs system will provide advice of the new sort code and / or account number using the zero account number advice voucher or **ADDACS**.

The vouchers will be dispatched to the Service User with the correct account details as supplied by the Paying Bank.

Amendments to the DDI may arise as a result of:

– the cancellation of the DDI

– the transfer of the Payer's account to another branch of the same Bank

– cancellation of the DDI due to the Payer transferring his account to a branch of a different Bank

– written authorisation from the Payer to his branch of a change to details of his DDI e.g. change of account name or number, within the same Bank

– while not a permanent amendment to a DDI, the Payer may dispute the Advance Notice given which may result in a collection being suspended until the dispute has been resolved

– any one of the other reason codes shown in the ADDACS table below.

If a Paying Bank is live on ADDACS all advices issued must be via the automated method, unless there has been a system failure. However, in the case of some Paying Banks there is one circumstance, other than a systems failure, which can also result in a manual advice being issued. This occurs when the Paying Bank cannot locate an account from the information received and consequently its systems are unable to return an advice via the automated route.

Table of ADDACS reason codes

Code	Reason
0	Instruction cancelled - Refer to Payer
1	Instruction cancelled by Payer
2	Payer deceased
3	Account transferred to a new Bank or Building Society
B	Account closed
C	Account / Instruction transferred to a different branch of Bank / Building Society
D	Advance Notice disputed
E	Instruction amended
R	Instruction re-instated (maximum 2 months from original DDI cancellation date).

See Appendix 2 for information on how individual codes should be dealt with.

N.B. A Service User must note that its Payer's DDI can be terminated without his knowledge e.g. the appointment of a liquidator. This will involve statutory publicity thus providing constructive notice.

Paying Bank's responsibilities

Paying Banks will progress the Payer's instruction to amend / cancel a DDI. Failure to do so immediately (on day of receipt or within 3 working days) could result in liability for the Paying Bank. The potential liability is immediate and will relate to the period outstanding between the Bank receiving the Payer's instruction to amend / cancel the DDI and the Bank actioning that instruction.

Therefore if a debit is paid against the Payer's account before the cancellation advice is sent to the Service User the Paying Bank would be liable. Paying Banks will accept transaction code 19 as notification of the **expiry** of the DDI.

See section 7.2.2.

Service User's responsibilities

Service Users must action these advices immediately, or within 3 working days from receipt. Service Users must ensure that they keep an audit trail of ADDACS messages in order to respond to Indemnity Claims raised.

Cases will arise when the Service User receives notice of a cancellation but is unable to act on it before the next collection date. In this case they may receive an **Indemnity Claim**.

See section 11.1.
See section 7.6
Error Recovery.

Should there be a dispute over whether an advice was issued, the Paying Bank will provide a copy of the ADDACS record or proof that an automated ADDACS advice has been sent to Bacs.

A Service User must advise the Paying Bank by use of a covering note if it intends to use the same reference on a DDI which replaces a recently cancelled DDI.

Best Practice Standards

It is recommended that on receipt of an ADDACS advice, Service Users should match using the following:

- Payer Account Number

- Sort Code

- Payer Name

- Reference.

The ADDACS advices should be processed in sequence number order. In the event that any Service User is unable to apply an ADDACS advice, it should liaise with the Paying Bank.

10.2 Service User generated amendments

Notice of expiry shall be deemed to have been given if the Service User identifies the final collection under the expiring DDI by the use of transaction code 19.

Where there is a change to the status of the Service User which would lead to changes to (e.g.: reference / SUN) the Service User must obtain and lodge new DDIs with the Paying Banks. In exceptional circumstances, arrangements can be made to transfer DDIs from one SUN to another, and to a different legal entity, subject to strict safeguards. Service Users must refer to their Sponsor if they wish to make such arrangements.

10.3 Payer generated cancellations

The Payer may wish to advise the Service User direct by written or electronic form or orally of a cancellation to the DDI.

N.B. If notification has been accepted by the Service User, the Service User may subsequently be liable to an Indemnity Claim if the Payer disputes giving authority to amend / cancel a DDI.

- The Service User must apply the changes **and advise the Payer to notify the Paying Bank**. This will ensure that all parties involved are informed of the cancellation

- Request to a Paying Bank to stop collection of one Direct Debit in a series cannot normally be accepted from a Payer whose proper course of action is to cancel the DDI permanently. The only exception allowed is that a Payer may dispute Advance Notice given and request that the single collection advised be countermanded.

10.4 Example of a manual advice

A non-ADDACS Paying Bank will issue advice of a DDI amendment / cancellation to Service Users using the Manual Advice Form.

**Direct Debit Scheme
Advice of Instruction
Amendment/Cancellation**

DIRECT
Debit

From: The Manager _____ Bank/Building Society

_____ Branch

Sort Code No. _____ | | | | | | |

Dear Sir,

Please note the following amendment/cancellation with effect from _____

TICK AS APPROPRIATE

- **0** Instruction cancelled – Refer to Payer
- **1** Instruction Cancelled by Payer
- **2** Payer Deceased
- **3** Account Transferred to a new Bank or Building Society
- **B** Account Closed

- **C** Account/Instruction transferred to a different branch of Bank/Building Society (See part 2 below)
- **D** Advance Notice disputed
- **E** Instruction amended
- **R** Instruction re-instated

Section 1 Details of Instruction (To be completed in ALL cases)
Present details

Name of Service User _____

Your Reference (if any) _____

Name of Payer (Max 18 characters) _____

Payer's Account Number | | | | | | | | |

Section 1(a) Details of amendment (To be completed for reason code E and R)
Amended details

Name of Payer (Max 18 characters) _____

Payer's Account Number | | | | | | | | |

Section 2 Details of new branch of this Bank/Building Society

Branch Title _____

Sort Code Number | | | | | | |

Yours faithfully

Manager

Date _____

Service User Number (SUN)

| | | | | |

Payer's Account Number | | | | | | | | |

Branch Stamp

02/1308/09/07

10.5 Example of an Automated ADDACS report

The ADDACS report is the means by which amendments to and / or cancellation of DDIs is advised by Paying Banks to Service Users.

AUTOMATED ADDACS REPORT

Bacs

ADVICES OF DIRECT DEBIT AMENDMENT AND CANCELLATION FOR 04/01/99

DIRECT Debit

SUN : 156243   INCIDENTAL INSURANCE

Reference	Reason Code	Payer's Name	Sort Code	Account Number	Due Date	Freq.	Amount	Effective Date	Last Payment Due Date	ADDACS Sequence
A130/2450/2435RD	I	MORGAN-WHITE	40-31-28	59473324	03/05/99	M	£101.23	04/01/99	04/01/99	40000000
A131/2451/2435RD	C	WADE	30-22-28	76543324				05/01/99		40000001
		WADE	30-31-28	69174546						
A133/2453/2435FF	I	THOMAS	40-31-44	45353324	03/05/99	M	£77.23	04/01/99		40000002

Submissions Range of 40000000 - 40000002   Complete

Total Number of Advices   3

REASON CODE MEANINGS   0 = Instruction Cancelled Refer to Payer 1 = Instruction Cancelled by Payer 2 2 = Payer Deceased
3 = Account Transferred to a new Bank or Building Society B = Account Closed C = Account Transferred to different branch Bank / Building Society
D = Advance Notice Disputed E = Instruction Amended R = Instruction Re-instated

---

10.6 Example of an Advice of New Destination Account Number - Zero Account Number Voucher

The zero account number voucher may be generated by the Bacs system where the destination account number does not conform to the standard 8-digit code.

1		Bacs processing day
2	20-21-07	Payer's sort code
3	60-01-00	Service User's sort code
4	99997777	Service User's account number
5	A N COMPANY	Service User's name
6	2698543	Service User's Direct Debit reference
7	F. Rose	Payer's account name

10.7 Example of how to cancel a Direct Debit

A Service User may like to advise the Payer how to cancel a DDI.

How to cancel a Direct Debit

You can cancel a Direct Debit at any time.
Just write to your Bank or Building Society
and send a copy to us.

Tell them:

1. Our name

2. The name(s) of the account holder(s)

3. Your branch sort code

4. Your Bank or Building Society account number

5. Your reference with us

6. The amount of the collection (if you know it).

Postal address of your Bank or Building Society

Any Bank or Building Society
Any Street, Any Town
Pay

Sort code

00 - 11 - 22
Date   19

Amount Payee

£

Cheque Number   Sort Code   Account Number
¥000010¥   00 - 11 - 22¥   12345678   A.N.Other

Your Bank or Building Society account number

Name(s) of account holder(s)

11 INDEMNITY CLAIMS

Introduction

Paying Banks will refund the Payer in the event of an error by the Service User. Paying Banks use the Indemnity Claim process to recover the refunded payment from the Service User.

The Service User must settle an **Indemnity Claim** within 14 working days of the date of the claim. The Service User has the right to make a Counter Claim under certain conditions as detailed later in the Guide.

11.1 Valid Indemnity Claims

The Paying Banks will accept the word of the Payer concerning an error made by a Service User due to their obligations under the Direct Debit Guarantee and will raise an Indemnity Claim. The Service User must settle the claim within 14 working days. If the Service User disagrees as to the validity of the claim and the issue falls outside the **Counter Claim** criteria, the Service User must pursue the matter direct with the Payer. Direct Debit is the method of collecting payments and the Banks are not responsible for any underlying contract between the Service User and the Payer.

The Paying Bank will action the Payer's instruction to amend / cancel a DDI. Failure to progress a cancellation immediately will result in the Paying Bank being liable for any Direct Debits paid in error under the cancelled DDI unless the Payer has already notified the Service User.

Where the Service User has received an advice from the Paying Bank amending / cancelling the DDI, this must be processed immediately or within 3 working days of receipt. Where a Direct Debit collection quoting the old details is already in transit or if a debit is issued with the old details after the date of the cancellation advice, Service Users should be aware that the debit may be the subject of an Indemnity Claim.

See section 10.1 for further details.

In the case of an unresolved dispute in respect of an amendment / cancellation advice issued by the Paying Bank to the Service User, the Paying Bank will provide proof that the advice was issued.

A valid Indemnity Claim must meet one of the following criteria:

1. The amount and / or date of the Direct Debit differs from the Advance Notice issued to the Payer by the Service User.

2. No Advance Notice was received by the Payer or the amount quoted is disputed by the Payer.

3. DDI cancellation by the Paying Bank – where there is proof that an ADDACS or paper cancellation advice has been sent by the Paying Bank to the Service User on or before the debiting day. All types of amendment / cancellation advices apply.

See section 10 for full details.

4. Where the Payer has cancelled the DDI direct with the Service User, notwithstanding the fact that the Payer may not have cancelled the DDI with the Bank.

5. No Instruction held. Payer disputes having given authority. In this case if the Service User can either produce a valid Instruction (e.g. one retained by the Service User in accordance with the AUDDIS requirements) or establish that one has in fact already been provided and that all other requirements have been complied with, a Counter Claim may be raised. A DDI shall not be regarded for this purpose as valid if it has not been signed by the Payer or is liable to be set aside e.g. mistake or misrepresentation.

6. Signature on DDI is fraudulent or not in accordance with the account authorised signature(s) held by the Paying Bank – **AUDDIS** Service Users only. No Counter Claim may be raised in this case.

7. An Indemnity Claim raised at the Service User's request. The request will not be accepted by the Paying Bank until after payment has been debited to the Payer's account. No action will be taken on any request until it has been confirmed in writing to the Paying Bank, by fax. A copy of the request must be submitted with the Indemnity Claim form.

8. Service User name disputed – where the Paying Bank is unable to identify and consequently action a Payer's request to cancel a DDI as a result of the Service User using one of the set-up exceptions in respect of trading names or facilities management.

9. Consequential loss.

N.B. Where a Service User has made an error which does not fall within the valid Indemnity Claim criteria, this will be referred to the **Direct Debit Scheme**, who will determine liability and give their authority for an Indemnity Claim to be raised. Where a Payer has received a refund under the Direct Debit Guarantee and also from the Service User, it is the Service User's responsibility to resolve this direct with the Payer or it's Payer's Agent.

11.2 Valid Counter Claims

There are five instances where a Service User may raise a Counter Claim:

1. Where the Paying Bank fails to send a cancellation advice to the Service User on or before the date the debit was presented against the Payers' account.

2. Where the Paying Bank has paid a Direct Debit with an 01 transaction code (in respect of a first collection on a new DDI) and has subsequently raised an Indemnity Claim for the reason 'No Instruction Held' – Rule to apply from 1.1.98; not available to AUDDIS Service Users.

3. Where the Paying Bank has returned a Direct Debit with an 01 transaction code 'Refer to Payer' and has subsequently raised an Indemnity Claim for the reason 'No Instruction Held' in respect of a representation with an 18 transaction code.

4. Where the Indemnity Claim is raised at the Service User's request and the Paying Bank fails to send a copy of the Service Users request.

5. Any claim which falls outside of the valid Indemnity Claim criteria as defined in 11.1 subject to any special provision for Counter Claims set out there.

If a Counter Claim is to be raised it **must** be raised by the Service User via its Sponsor after settlement of and within 14 **working days** of settlement of the Indemnity Claim.

A Counter Claim may only be raised where settlement of the original Indemnity Claim was made within 14 working days of the date of the original Indemnity Claim.

Where a Counter Claim has been raised, the Sponsor will respond within one month, confirming acceptance or rejection of the claim. The Paying Bank will either reject e.g. provide proof that an ADDACS or paper cancellation advice has been sent or settle the Counter Claim within 90 days of the claim being forwarded by the Sponsor.

The Service User should contact its Sponsor's Direct Debit Customer Services Department giving details of the settled Indemnity Claim including;

– amount

– date of claim

– Service User's account details

– SUN and the reference quoted on the **Direct Debit** record.

N.B. The Counter Claim is not the only route open to the Service User. The Service User retains its right to take action directly against the Payer. Direct Debit is the method of collecting payments and the Banks are not responsible for any underlying contract between the Service User and the Payer.

11.3 Refunding the Payer's account

Under the terms of the **Direct Debit Guarantee** a Payer is entitled to an immediate refund if an error has been made either by the Service User or the Paying Bank. This includes any errors relating to:

- the collection due date and frequency.

- the amounts to be paid.

- payments made after an instruction given to cancel a DDI.

The Paying Bank must, therefore, refund the Payer immediately and only raise an Indemnity Claim where there has been a Service User error. Where there has been an error by the Paying Bank a refund request may be raised.

If the Payer approaches the Service User direct regarding an error, the Service User must refer the Payer to the Paying Bank or contact the Paying Bank asking them to raise an Indemnity Claim.

See section 11.6 Refund Request and section 11.10 for an example of the Refund Request form.

11.4 Submission of the Indemnity Claim

All Indemnity Claims must be submitted by the Paying Bank using the Indemnity Claim form. The form will be dispatched direct to the Service User by first class post.

The form must provide details to the Service User of the reason for the claim along with the settlement account details and the date of any amendment / cancellation advice sent to the Service User. Only one reason must be given on an Indemnity Claim form. An Indemnity Claim can only be raised for the full amount of the original Direct Debit payment.

Invalid Claims

Where a Service User receives an Indemnity Claim which it believes does not conform to the valid Indemnity claim criteria as detailed in 11.1, it must nevertheless pay the claim, but may then immediately raise a Counter Claim in accordance with section 11.2. The Indemnity does not permit the rejection of any claim made by the Paying Bank.

11.5 Service User settlement of the Indemnity Claim – Time scales

An Indemnity Claim must be settled by a Service User to the Paying Bank without delay, and in any case within 14 working days from the date of the claim.

Settlement may be sent via Bacs but must be directed to the account specified on the Bank Giro Credit attached to the claim. This must also quote the reference detailed on the Bank Giro Credit. Alternatively the Service User may settle the claim by cheque, in which case it must either:

1. Attach the Bank Giro Credit to the cheque itself, as this will provide the Paying Bank with all the relevent details to ensure settlement of the outstanding claim in a timely manner and send to the Paying Bank branch by post to the address on the Indemnity Claim form; or

2. Pay in the Bank Giro Credit at its Bank branch.

If the Service User fails to settle the Indemnity Claim, the Paying Bank may claim settlement of the outstanding funds from the Service User's Sponsor who will settle the outstanding funds immediately. The Sponsor will debit all amounts to the Service User's account via Direct Debit or similar method. The Service User is deemed to have provided their Sponsor with the authority to make such debit by whatever method necessary by virtue of agreeing to abide by and operate within the set procedures as defined herein.

The Sponsors will be closely monitoring those Service Users who fail to settle their Indemnity Claims within the specified period and may at their discretion instigate a dispute process which may result in the Service User being requested to cease collecting Direct Debits.

11.6 Refund request

Where a Paying Bank has made a payment in error, a refund request may be sent to the Service User using the **refund request** form.

The Paying Bank must refund the Payer. The claim must not include a request for consequential loss.

Settlement of the claim is at the discretion of the Service User. If the Service User is in doubt as to the validity of the claim it must seek guidance from its Sponsor.

See section 11.10 for an example of the form.

11.7 Consequential loss

Where the Payer claims consequential loss as a result of an erroneous Direct Debit payment the Paying Bank will claim this from the Service User on a separate Indemnity Claim Form. **Consequential loss** must be fully justified by the Payer and this justification attached to the claim to the Service User. Paying Banks are **not** required to undertake immediate refunds in respect of consequential loss claims.

If the Payer raises a claim for consequential loss arising as a result of the Service User failing to collect a Direct Debit, the Payer must be directed to the Service User by the Paying Bank. It may be possible for Service Users to arrange insurance against consequential loss liability. Provision of such insurance is at the discretion of the insurer.

11.8 Example of prohibited practices

- Indemnity Claims for partial amounts are not allowed by the Scheme

- The Service User must not settle an Indemnity Claim by remitting direct to the Payer's account

- A Service User must not raise a Counter Claim where it has received cancellation advice direct from the Payer.

11.9 Example of a Direct Debit Scheme Indemnity Claim form

This form is raised by the Paying Bank for settlement of an Indemnity Claim.

DIRECT Debit

Direct Debit Scheme Indemnity Claim

Dear Sir,

Under the terms of the Direct Debit Indemnity, we request you to refund forthwith to this branch via Bacs, or by means of the attached bank giro credit, the sum specified below, in respect of the undermentioned Direct Debit(s). Our customer has already been reimbursed in respect of this claim.

Reason for Claim

☐	Amount and / or date of DD differs from Advance Notice
☐	*No Advance Notice received by Payer/or the amount quoted is disputed
☐	DDI cancelled by Paying Bank Date advice sent or copy enclosed / /
☐	Payer has cancelled DDI direct with Service User
☐	No Instruction held. Payer disputes having given authority
☐	**AUDDIS Service Users only** Signature on DDI is fraudulent or not in accordance with account authorised signature(s)
☐	Claim raised at Service User's request after DD applied to Payer's account. Date of Service User letter or Service User contact name: _____
☐	Service User name disputed. Payer does not recognise Service User collecting DD.
☐	Consequential loss. Supporting details attached.

*Delete as applicable

Details of Claim

Date(s) Processed
(working day(s) before Debiting Day) _____

Due Date and Frequency _____

Your Reference _____

Name of Payer _____

Amount of Direct Debit(s) £ _____

Total £ _____

Service User Number (SUN) [| | | | | |]

Yours faithfully

Manager

Date _____

Branch Stamp

DETAILS BELOW TO BE COMPLETED BY BRANCH CLAIMING PAYMENT

02/1309/09/07

From: _____ Bank

_____ Branch

Date: _____

bank giro credit

Re Settlement of Indemnity Claim by: _____ (Service User)

Bank and Branch	Branch Sort Code	Account Name and Number	Amount
Reference [ ]	Sorting Code Number	Direct Debiting Supreme A/c Payer : Account Number	Amount
	[					]	[							]	£ [ ]

Please do not write or mark below this line or fold this voucher

11.10 Example of a Refund Request form

A form used by the Paying Bank to request a refund from the Service User as a result of Paying Bank error.

DIRECT Debit

Direct Debit Scheme
Refund Request

From: The Manager _____ Bank/Building Society

_____ Branch

Dear Sir,

Due to an error by this branch which has affected our mutual customer could you please give consideration to refunding this Branch, by means of the attached bank giro credit, the sum specified below, in respect of the under mentioned Direct Debit.

Details of Request

Date(s) working day(s) before Debit Day
Processed _____

Due Date
and Frequency _____

Your
Reference _____

Name of
Payer _____

Service User
Number (SUN) | | | | | | |

Amount of
Direct Debit(s) £ _____

Total   £ _____

Yours faithfully

Manager

Date _____

Reason for Request

Date on which Payer instructed us to   /   /
cancel DDI _____

Other
Reason _____

_____

Additional
Notes _____

_____

_____

Branch Stamp

02/131I/09/07

From: _____ Bank

_____ Branch

Date: _____

Re Settlement of
Refund Request by: _____ (Service User)

bank giro credit

Bank and Branch	Branch Sort Code	Account Name and Number	Amount
Reference [ ]	Sorting Code Number	Direct Debiting Supreme A/c Payer :	
		Account Number	Amount
			£

Please do not write or mark below this line or fold this voucher

12 MONITORING OF THE SCHEME

Introduction

The Service User's Sponsor should satisfy itself that the Service User adheres to the requirements of the Scheme. A Service User must pass its Direct Debit communications literature to its Sponsor for approval. This approval will extend to the technical specification of the Service User's Bacs submissions, new / amended DDIs and other literature.

The Service User must advise its Sponsor of any changes to its status, communications literature or Bacs submissions. However, the Sponsor will monitor the operations within the Scheme to ensure the required standards are achieved and maintained by all Service Users.

The Sponsor reserves the right to withdraw its Sponsorship, limit the amount collected or refuse to accept a specific file of Direct Debits.

12.1 Monitoring of the Scheme

Sponsors will monitor operations within the Direct Debit Scheme to ensure that the required standard of documentation and procedure is achieved and maintained by all Service Users.

Monitoring of Direct Debits is undertaken to protect **Payers** using the Scheme. Failure to carry out these checks will not affect the validity of any claim under the Direct Debit Indemnity.

The following will be monitored:

The Direct Debit record

The Paying Banks will from time to time check a sample of Direct Debits presented by Service Users to ensure that operational standards set out in this Guide are met. The checks may also be applied to ensure the collected Direct Debits conform to the terms of the Instruction lodged by the Service User.

AUDDIS service

Bacs will provide a number of statistics to the Sponsors on a monthly basis as a means for them to gauge whether AUDDIS Service Users are operating effectively and efficiently. Where anomalies are identified by the Sponsors they will liaise with the Service User's Sponsor to establish the reasons why and identify an appropriate solution to be applied.

See section 15 for AUDDIS.

The Direct Debit Instruction and communications literature

Paying Banks have the right to refuse completed DDIs which are not legible or do not comply with the **DDI** regulations detailed in this Guide. These may be returned to the Service User by the Paying Bank marked 'lodgement refused' and the Paying Bank may request the Service User's Sponsor to investigate those DDIs which do not comply with the required standard.

See sections 3.2 and 5.3 for DDI design and lodgement refused.

Additionally, where the Sponsors receive notification of the use of non-standard communications literature (i.e. the Advance Notice and Direct Debit Guarantee issued to the Payer) the Sponsor will be required to liaise with their Service User and request them to change to the required standard.

Settlement of Indemnity Claims

A claim may be raised by the Paying Bank when the Payer disputes the validity of a debit applied against his account as a result of an error by the Service User. In all instances the Service User is required to settle the Indemnity Claim within 14 working days of the date of the claim.

The Sponsors will be closely monitoring those Service Users who fail to settle Indemnity Claims within the specified period and may at their discretion instigate a dispute process which may result in the Service User being requested to cease collecting Direct Debits.

Bacs account limit

A Sponsor may apply a limit against a Service User's **nominated account**. Overlimit referrals are raised by Bacs and issued to the Sponsor who will give their authority to process or extract the submission if appropriate. This facility is used by the Sponsors at their discretion.

The Sponsor reserves the right to withdraw its Sponsorship, limit the amount collected or refuse to accept a specific file of Direct Debits into the clearing.

12.2 Sponsor's role

The Sponsor is required to take proper steps to satisfy itself, and to confirm to Bacs Payment Schemes Ltd or other participants when called upon, that the Service User is adhering to the requirements of the Scheme.

Where the Sponsor has been advised of an instance where its Service User is operating outside of the required standards, the Sponsor must liaise with its Service User to clarify the requirements, set an appropriate time frame for the Service User to apply changes and monitor progress.

Where Service User's documentation / procedures impacts the integrity of the Scheme, the Sponsor must progress the issue.

12.3 Service User's responsibilities

It is the Service User's responsibility to ensure it advises its Sponsor of:

– any changes to its status. When this involves the Service User's business being carried on by a different legal entity (for instance by a company in place of a partnership) the new entity must itself become a Service User and take new DDIs before Direct Debiting may continue. In exceptional circumstances, arrangements can be made to transfer DDIs from one SUN to another, and to a different legal entity, subject to strict safeguards. Service Users must refer to their Sponsor if they wish to make such arrangements.

    – any change to its DDI and any other communications literature in respect of its Direct Debit operations or Bacs submissions.

Collecting and acting on Bacs Reports

Service Users must ensure that Bacs reports are downloaded via Bacstel-IP and the Bacs payment services website in a timely manner. In interpreting 'a timely manner' Service Users must be mindful of the requirements for actioning items on the report. Bacs will provide Management Information (MI) to Sponsors on a monthly basis to monitor those Service Users who fail to access reports or who fail to act on the information contained within.

Keeping contact details up to date

Communication details e.g. email address and telephone number are recorded for each contact i.e. Primary Security Contact and Additional Contact, registered to use Bacstel-IP. Each contact is responsible for ensuring that the information recorded is kept up to date. This includes the details recorded on the DDO database. Further information can be obtained from the Service User Guide – Bacstel-IP.

  Where the Sponsor has highlighted an instance where the Service User is not conforming to the requirements of the Scheme, the Service User must ensure it applies any changes requested by its Sponsor within an agreed time frame and provides evidence to support that the changes have been made.

  If Bank monitoring reveals an unacceptable level of error or substantial deviations from Scheme Rules, the Service User will be advised accordingly. If no subsequent improvement is made, the Service User may be required to withdraw from the Scheme.

Keeping Bacstel-IP software up to date

Service Users must ensure that their Bacstel-IP related software is kept up to date when provided with updates by their Solution Supplier. This includes updates to Modulus Checking and the ISCD

12.4 Customer/Payer complaint handling and timescales

When a Payer complaint or query is received at Bacs, the following action will be taken.

  Within 48 hours of receiving a complaint, Bacs will acknowledge receipt to the Payer with a holding letter detailing timescales for a response. Also within the same 48 hours, Bacs will forward details of the complaint to the Service User. This will enable any associated paperwork and information to be obtained from the Payer.

The Service User must acknowledge receipt of the complaint to Bacs within 48 hours. Within two weeks of receiving the complaint, the Service User must forward a written response to Bacs, detailing the findings of the investigation. If the Service User is not in a position to resolve the complaint, then it must advise Bacs of the timescales for the final resolution. Within 48 hours of receiving a response from the Service User, Bacs will advise the Payer. This will enable any queries with the response to be followed up.

Some sponsoring banks wish to raise complaints and queries received at Bacs direct with their Service Users. However, the timescales quoted above still apply.

13 EXIT FROM THE SCHEME

Introduction

There are three circumstances in which a Service User is required to withdraw from the Scheme.

- Voluntary termination

- Compulsory termination

- The contractual capacity of the Service User is terminated by legal process, for example, by bankruptcy or winding up or a merger or acquisition of or by another company.

The Service User's Sponsor will withdraw the Service User's SUN from the Scheme and advise all the Sponsors and Bacs of the termination of the Service User's participation. Even though the Service User has ceased to collect Direct Debits it is still liable for any **Indemnity Claims** which may be raised by the Paying Bank for Direct Debits applied to the Payers account during the period of the Service User's participation in the Direct Debit Scheme. In all cases this liability is not restricted in respect of time or amount.

13.1 Voluntary termination

A Service User must plan the withdrawal very carefully in close consultation with its Sponsor. This will normally entail the following actions:

- The cancellation of existing DDIs

- The progressive replacement of the Direct Debit by some other payment

- The Service User is required to give to its Sponsor one month's written notice from the processing date of the last Direct Debit collection file, of its intention to cease operating within the Scheme

- The Sponsor will co-ordinate the necessary documentation required to delete the SUN from the Bacs Reference Data and advise the Sponsors.

The Service User withdrawing voluntarily from the Direct Debit Scheme may consider it prudent to establish a contingency reserve for the purpose of meeting any claims which may be received in respect of any Indemnity liability which may arise subsequent to withdrawal of the Service User from the Scheme, in respect of Direct Debits originated prior to this event.

13.2 Compulsory termination

In the event of a Service User causing significant problems for the industry as a whole, leading for example to Paying Bank complaints to the **Direct Debit Scheme Steering Group**, it will be given two written warnings through its Sponsor. The first written warning will outline the general nature of the problem occurring detailing the requirements to conform and a time period for achieving conformity. Should the problem not be rectified within the agreed period, a second written warning will be given further specifying the nature of the problem, the requirements to conform and a further time period for achieving conformity. In setting the time period, the Direct Debit Scheme Steering Group will take into consideration the nature of the problem and the extent of the activity required to achieve conformity. Should conformity not be achieved within the time frames set out in the second written warning, the Sponsor will report to the Direct Debit Scheme Steering Group who will in turn report to the Bacs Payment Schemes Ltd Board who will have the right to instruct the Sponsor to terminate the Service User from the Scheme without further notice.

A Service User will be removed from the Scheme if the Bacs Payment Schemes Ltd Board reasonably believes that:

– Direct Debiting operations are being carried out in a manner which constitutes an abuse of the Scheme, affects the integrity of the Scheme or Direct Debiting operations are being carried out without due regard to the interest of Payers

– Where there is evidence that standards and procedures detailed in this Guide are being deliberately ignored.

In extreme cases, the Bacs Payment Schemes Ltd Board or the Sponsor reserve the right to terminate a Service User's participation in the Scheme at short notice, notwithstanding the disruption which may occur. Every effort will be made to give sufficient notice (minimum of 3 months) to enable a Service User to make alternative arrangements. However, the giving of notice in this context is not an obligation assumed by the Bacs Payment Schemes Ltd Board or the Sponsors and they cannot accept under any circumstances liability for any loss, which a Service User may suffer as a result of termination from the Direct Debit Scheme.

Should a Service User wish to appeal ("Appeal") its termination from the Direct Debit Scheme (howsoever caused), it must notify the Bacs Payment Schemes Ltd Board ("Notification") within 14 days of receiving notice of its termination from the Direct Debit Scheme.

Upon Notification, the Bacs Payment Schemes Ltd Board will, by written notice to the City Disputes Panel Ltd. ("the Appointer") request the Appointer to nominate an appeal panel ("Panel") to hear and determine the Appeal.

The Panel shall consist of three individuals who, in the opinion of the Appointer are suitably qualified members of or professional advisers to the banking and/or financial services industry in the City of London and who are also independent of the Service User, the Sponsor and the Bacs Payment Schemes Ltd Board. The Appointer may but shall not be obliged to consult the Service User, the Sponsor or the Bacs Payment Schemes Ltd Board before nominating a Panel. Within 14 days following their nomination, the Panel shall appoint one of their number to preside over the Appeal ("the Chair").

The Appeal shall be a re-hearing of the original determination of the Bacs Payment Schemes Ltd Board or the Sponsor (as applicable) and shall be conducted in accordance with such process as the Chair deems fair and appropriate, (and so far as he/she is advised, in accordance with the Human Rights Act 1998).

The Panel shall arrive at its decision by majority vote and the Panel's decision shall be final and binding on all parties to the Appeal. The Panel's decision may also include a ruling as to how the costs of the Appeal (including the remuneration of the members of the Panel) shall be borne between the parties.

13.3 Contractual capacity of the Service User is terminated by legal process

A Service User will be withdrawn from the Scheme if its contractual capacity is terminated by legal process, for example, by bankruptcy or liquidation. In particular, a Service User shall immediately cease to be entitled to participate in the Scheme, if any one or more of the following events ('the relevant insolvency event') occurs.

- When the Service User, being an individual, or where the Service User is a partnership, any partner in that firm, becomes bankrupt or makes any composition, conveyance or assignment or arrangement with or for the benefit of his creditors, or purports to do so

- When the Service User, being a company, passes a resolution or the court makes an order for the winding up of the Service User (otherwise than for bona fide reconstruction or merger) or a receiver, administrative receiver, administrator, trustee or similar officer is appointed in respect of all or any part of its undertaking or enters into a composition or voluntary arrangement with or for the benefit of its creditors.

- An event which is, under the law of a country outside the **United Kingdom**, equivalent to any of the events listed above.

The Service User must not raise any DDI or Direct Debit after the commencement of a relevant insolvency event. Service Users should note that the SUN will be withdrawn by the Sponsor as soon as possible after it has notice of the occurrence. The Sponsor will liaise with the Service User on this issue.

Where an administrative receiver is appointed for all or part of the undertaking of a Service User, it may be possible in some circumstances, and at the discretion of the Service User's Sponsor, to permit that Service User to continue as a participant in the Direct Debit Scheme. If a Sponsor decides to permit such a Service User to continue, then the Sponsor shall be liable for any loss or damage suffered by a Payer, Paying Bank or other Sponsor of the Direct Debit Scheme arising directly or indirectly from any Direct Debit raised by that Service User.

14   STANDING ORDER CONVERSION

Introduction

A number of Service Users also receive payment from some of its Payers by Standing Order. This is an automated payment initiated by the Payer's Bank on behalf of the Payer for a fixed amount on a pre-determined date.

Service Users can increase efficiency and reduce costs by converting customers to collection by Direct Debit.

14.1   Planning the conversion

Service Users should advise its Sponsors if they are planning a conversion exercise. Its Sponsor will provide it with marketing support covering:

– Payer incentives to sign up for Direct Debit

– design of literature and leaflets detailing the benefits of the Direct Debit Scheme

– advice on the most effective period to commence the campaign i.e. during a scheduled advertising campaign.

14.2   Design of the Direct Debit Instruction with Standing Order Cancellation request

The DDI must conform to the standard described in this Guide. In addition, Service Users must combine the Standing Order Cancellation request with the DDI.

Direct Debit Guarantee

Service Users must issue a copy of the Direct Debit Guarantee with the DDI, Advance Notice or other correspondence issued in respect of the application to the Payer, detailing the safeguards of the Scheme. Service Users are advised to print the Direct Debit Guarantee at the bottom of the combined DDI and Standing Order Cancellation request on a tear off portion to be retained by the Payer. In this way the Direct Debit Guarantee will be removed from the DDI by the Payer.

14.3   Completion and lodgement of Direct Debit Instruction and Standing Order Cancellation request

• Payers should be requested to complete the DDI and the Standing Order Cancellation request and return both to the Service User without detaching one from the other

• The completed DDI, when returned by the Payer, should be handled in the normal way

- The Standing Order Cancellation received with the DDI should be detached and forwarded to the Payers Bank. This step should be taken at a suitable time to ensure that payments are neither missed nor duplicated. Please allow the Paying Bank 5 working days to cancel the Standing Order authority
  - The Service User may wish to align the despatch of the completed Standing Order Cancellation Authority to the Payers Bank with the submission of the '0N' (in the case of AUDDIS Service Users) or the submission of the paper DDI (in the case of non AUDDIS Service Users), to the Payers Bank or Building Society

- Service Users may also wish to consider advising the Payer that the Standing Order Cancellation request has been despatched to the Payers Bank when the Advance Notice is issued. In this way the Payer can, if he so wishes, monitor his Bank account to ensure payments are not duplicated.

14.4 Example of a Recommended Direct Debit Instruction with Standing Order Cancellation request

This is a standard form for submitting DDI for lodgement and the Standing Order cancellation advice to Paying Banks. Please note non-AUDDIS Service Users will submit the whole form, AUDDIS Service Users only need to submit the Standing Order cancellation.

DIRECT Debit

A N Company
logo or name

Instruction to your Bank or Building Society to pay by Direct Debit

Please fill in the whole form including official use box using a ball point pen and send it to:

A N Company
Any Street
Any Town
Anywhere
AB1 2CD

Service User Number

Reference

Name(s) of Account Holder(s)

FOR (A N COMPANY) OFFICIAL USE ONLY
This is not part of the instruction to your Bank or Building Society.

Bank/Building Society account number

Branch Sort Code

Instruction to your Bank or Building Society
Please pay (AN Company) Direct Debits from the account detailed in this Instruction subject to the safeguards assured by the Direct Debit Guarantee. I understand that this Instruction may remain with (AN Company) and, if so, details will be passed electronically to my Bank/Building Society.

Name and full postal address of your Bank or Building Society
To: The Manager   Bank/Building Society
Address

Postcode

Signature(s)

Date

Banks and Building Societies may not accept Direct Debit Instructions for some types of account

---
✂

Name and full postal address of your Bank or Building Society
To: The Manager   Bank/Building Society
Address

Postcode

Standing Order Cancellation

Branch Sort Code

With immediate effect, please cancel my/our Standing Order authority payable to A N Company under:

Account reference No.

Bank/Building Society account number

Name(s) of Account Holder(s)

Signature(s)

Date

✂

This guarantee should be detached and retained by the Payer.

The Direct Debit Guarantee

DIRECT Debit

■ This Guarantee is offered by all Banks and Building Societies that take part in the Direct Debit Scheme. The efficiency and security of the Scheme is monitored and protected by your own Bank or Building Society.

■ If the amounts to be paid or the payment dates change (A N Company) will notify you (insert number of) working days in advance of your account being debited or as otherwise agreed.

■ If an error is made by (A N Company) or your Bank or Building Society, you are guaranteed a full and immediate refund from your branch of the amount paid.

■ You can cancel a Direct Debit at any time by writing to your Bank or Building Society. Please also send a copy of your letter to us.

DD+STAND ORD

15   AUDDIS – AUtomated Direct Debit Instruction Service

Introduction

AUDDIS (Automated Direct Debit Instruction Service) transfers DDIs electronically between Service Users and Paying Banks **via Bacs**.

With effect from 1 January 2008, the use of AUDDIS to submit DDIs is mandatory for all new Service Users that submit direct to Bacs.

Automating the transfer of the DDI brings significant benefits to all parties involved in the Direct Debit **Scheme**.

- Lower distribution costs for Service Users

- Easier identification of a DDI through the core referencing requirements

- Significant reduction in unpaids, particularly at the first collection

- The account details on the DDI are captured by the Service User and lodged electronically on the Payers account

- Direct Debit collections can only be made when a live DDI exists and the core reference used

- Better service quality from fewer processing delays

- Eliminates paper from the system

- Reduction of errors in the DDI set-up

- Improved image of the Direct Debit Scheme as a result of improved data quality.

How does it work?

AUDDIS automates the lodgement of DDIs from the Service User to the Paying Bank and all DDIs must be sent electronically to Bacs, without exception. The Paying Banks validate the DDIs, either accepting them or returning them to the Service User. This validation confirms that the technical requirements have been complied with; it does not provide confirmation that the Paying Bank's customer has authorised the DDI. A small number of Paying Banks are unable to receive electronic AUDDIS DDI output, in such cases they receive paper advices in the form of a report. If these are rejected the Paying Bank will advise the Service User directly by returning the paper advice marked 'lodgement refused'.

The paper DDI remains with the Service User. It is up to the Service User to decide how long to retain the paper and the method of storage. However the Service User must provide a copy of the DDI within 7 working days if requested by the Paying Bank. If a copy cannot be produced or the DDI is incorrect or fraudulent, then the Service User must accept liability under the terms of the Direct Debit Indemnity.

The receipt of a 0N AUDDIS transaction is sometimes used by the Paying Bank to inform the Payer that a new DDI has been set-up on his account.

Service Users must not collect Direct Debits from a Payer's account, earlier than 5 working days after lodgement of the DDI. With effect from the 19 November 2001 the lodgement period will be reduced from 5 working days to 2 working days, this will coincide with the launch of the Transfer of Direct Debits and Standing Orders Service. However where collection timescales allow, it is recommended 5 working days are left before the first collection to ensure that no 0N rejections are received. Service Users must take into consideration the rules pertaining to Advance Notice.

15.1 AUDDIS Service User set-up

A Service User wishing to join AUDDIS must apply to it's Sponsor for advice on the requirements of the Scheme. Service Users already using Direct Debit for an existing operation must allow at least 4 months between submission of their application form and the proposed joining date.

The Sponsor will establish the Service User's ability to meet the AUDDIS criteria before giving authority to allow the Service User to join the service.

A new Service User, or Service Users with new SUNs must allow a minimum of 8 weeks for their application to be processed before the intended 'live' date.

15.2 Making the switch

The Sponsors and Bacs will control and monitor Service Users on to the AUDDIS service to ensure a smooth transition. This can take place either by:

– setting up a new SUN.

   OR

– migrating all or some DDIs under an existing SUN.

All parties involved must conform to the following AUDDIS Rules, which are expanded upon in the AUDDIS Service Definition.

These Rules are in addition to the existing Direct Debit Scheme Rules, as detailed in this Guide, which otherwise apply except where varied by the AUDDIS Rules.

15.3 Conversion of existing Direct Debit Instruction records

A Service User using the service has the following options.

Convert all its existing DDIs to AUDDIS. This will be achieved by submitting all their existing DDIs with the Paying Banks via the AUDDIS Service. The DDI records will be submitted using transaction code '0S'.

Before conversion commences the Service User will be required to submit successful test files to Bacs.

- The Sponsor will liaise with the Service User on the requirement for AUDDIS test submissions. Full details of the requirements for testing and migration to AUDDIS are available in the booklet 'AUDDIS – A Migration Guide for Direct Debit Service Users' which can be obtained from the Sponsors.

The conversion of existing DDIs for a Service User joining AUDDIS will usually take place on one day. The Service User then has a month to obtain corrections for all rejected DDIs. At the end of this 'migration' period, the Service User's SUN will be set to live AUDDIS status.

Where Service Users do not wish to convert all DDIs to AUDDIS, the bulk-change procedure must be followed and the Sponsor will need to advise you of the requirements.

If a Service User wishes to merge two SUNs, the Service User must ensure that there is no duplication of core references. Before undertaking this exercise, the Service User must again liaise with the Sponsor who will need to advise you of the requirements.

Once a Service User becomes an AUDDIS user, either by using a new SUN or converting an existing SUN to AUDDIS, all DDIs must be submitted via AUDDIS for that SUN.

15.4 Direct Debit Instruction design

The current rules relating to the DDI design apply to AUDDIS Service Users.

In addition the following is also applicable.

- The preferred approach is for Service Users to preserve a one-to-one relationship between DDIs signed by the Payer, DDIs sent to the Paying Banks and Direct Debits to be collected. It is recognised the Service Users may not generate their reference until after the Payer has signed the DDI. In these circumstances where the Payer has signed a DDI without a reference, multiple references may be used providing each DD reference is quoted clearly on the Advance Notice to the Payer detailing which amounts relate to which reference. These must then be lodged on individuals 0Ns with the Paying Bank.

15.5 Lodgement of new '0N' Direct Debit Instruction

- A new DDI is lodged by submitting a '0N' record to the Paying Bank via Bacs (day 1) containing the DDI information.

- The Paying Bank receives the DDI on day 2 and validates the content.

- If accepted the DDI will be lodged on day 3. If rejected the Paying Bank will return the record to the Service User on day 3 via Bacs messaging or paper advice marked 'lodgement refused'. The Service User will receive details of the rejected and returned records on day 3 or 4 via Bacstel-IP and the Bacs payment services website.

Example of the DDI lodgement cycle. (4 working days)

Day 1	Day 2	Day 3	Day 4
Thursday	**Friday**	**Monday**	**Tuesday**
Service User transmits DDI input file to Bacs for processing.	Bacs output valid DDIs to Paying Bank.	Valid DDIs are lodged against Payer's accounts. Invalid DDIs are returned to Service User's via Bacs Messaging Service (ADDACS).	i) Bacs processes Paying Bank DDI returns. ii) Service Users access the returned DDIs by way of a report via Bacstel-IP and the Bacs payment services website. Note: Service Users can obtain details of the returned DDIs in a format to enable them to be applied directly to their systems. iii) Service User to reconcile.
Bacs validation of DDIs.	Paying Bank's validate DDIs.		

- Bacs also produce an Input Report for the DDI file, which details amended / rejected records resulting from Bacs validation. This is available to the Service User on day 1. The Input Report is available to the Service User via Bacstel-IP and the Bacs payment services website.

- In joining AUDDIS the Service User must satisfy itself of the Payer's identity and his capacity to authorise Direct Debits to be drawn upon the nominated account. The Service User must therefore ensure that it has adequate procedures in place to authenticate a Payer's identity and his authority to sign before submitting the DDI to the Paying Bank. This will help to prevent an Indemnity Claim being raised by the Paying Bank where the Payer disputes signing the DDI, since the Service User will retain the valid authenticated authority.

- The Paying Banks will store the core reference quoted on the DDI as part of the lodgement process and will use this to validate Direct Debit collections. The last collection reference or **core reference** will be quoted to Service Users by the Paying Bank when advising of amendment / cancellation of the DDI.

- It is the preferred standard practice that a Service User uses a one contract – one DDI approach. This will ensure that no DDI will be cancelled in error.

- A Service User should transmit a DDI to the Paying Bank within 10 working days of the customer signing the DDI, even if the Service User does not intend to commence collection immediately. A Service User who is unable to transmit the DDI within this timeframe must advise the Payer that the Direct Debit will not be set up on their bank account until XXXX (depending on when the Service User will lodge the DDI). However in all circumstances the Service User must transmit the DDI no later than 6 months from the date the DDI was signed. Failure to lodge the DDI within these timescales may result in the DDI being rejected.

- Service Users must not collect Direct Debits from a Payer's account earlier than 2 working days after lodgement of the DDI. i.e. if a DDI is lodged with the Paying Bank on Monday (day 3) of the Bacs cycle – then the first Direct Debit can be collected on Wednesday (day 5). However where collection timescales allow, and as shown in the table below, it is recommended 5 working days are left before the first collection to ensure that no 0N rejections are received.

Example of DDI lodgement and collection cycle

Day 3	Day 4	Day 5	Day 6	Day 7	Day 8
Monday	**Tuesday**	**Wednesday**	**Thursday**	**Friday**	**Monday**
Valid DDIs are lodged against Payer's accounts. Invalid DDIs are returned to Service User's via Bacs Messaging Service (ADDACS).	i) Bacs process Paying Bank DDI returns. ii) Service Users access the returned DDIs by way of a report via Bacstel-IP and the Bacs payment services website. Note: Service Users can obtain details of the returned DDIs in a format to enable them to be applied directly to Service Users systems. iii) Service User to reconcile.		Service User submits DD collection file to Bacs for processing.	Paying Bank receives and processes DD collection file.	Direct Debit applied to Payer's account or returned unpaid.

- Service Users must provide Advance Notice to the Payer before the first Direct Debit collection is made. Advance Notice must also be given to the Payer if the amount, collection due date or frequency is changed and the period given must agree with that quoted on the Direct Debit Guarantee.

15.6 Transaction codes

Service Users must use the following transaction codes for all DDIs and Direct Debits sent to Paying Banks via Bacs. Use of transaction codes is mandatory, no deviation from these codes is allowed.

Direct Debit Instruction

- 0N – for a new DDI, or to re-instate a Payer or Service User cancelled DDI

- 0C – to cancel an existing DDI

- 0S – to convert an existing non-AUDDIS DDI to AUDDIS (only used at conversion time)

- 0C/0N – by using these as a pair on the same day you can amend a DDI record.

Direct Debit

- 01 – for first collections, i.e. the first Direct Debit originated following receipt of a new DDI (0N), transferred DDI, amended or reinstated DDIs by the Payer's Bank

- 17 – for the collection of all Direct Debit payments. This code is used to indicate the collection of a standard Direct Debit, i.e. not a first, final or re-presented Direct Debit

- 18 – for a re-presented Direct Debit

- 19 – for a final Direct Debit collection.

15.7 Modulus Checking

Most Paying Banks operate a modulus checking facility within their systems which validates the sort code and account number combination of any DDI and Direct Debit applied to the Payer's account. It is preferred that Service Users apply the modulus checking routine within their own systems. Service Users may obtain details of the Paying Banks modulus checking validation requirements from www.vocalink.com/moduluschecking

Best Practice Standards

It is strongly recommended that AUDDIS Service Users apply modulus checking when applying the Direct Debit Instruction to their own system as this will highlight erroneous details and enable the Service User to correct any invalid information.

Service Users are also recommended to use the Industry Sorting Code Directory and information detailed in the 'Crediting and Debiting Building Society Accounts' booklet to validate sort code details.

Modulus Checking and the Industry Sorting Code Directory are available from your Bacs approved Software Supplier or direct from www.vocalink.com/moduluschecking or www.vocalink.com/iscd respectively.

15.8 Validation checks

Customer Validation

Know your customer – Best Practice Standards

It is highly recommended that Service Users verify and check the status of the Payer before processing any Direct Debits. **A list of verification measures to assist in verifying the Payer's details is available from www.bacs.co.uk/bacs/businesses/resources/subscriber+library/**

Some key areas to consider when validating a Payer are:

- Address verification against Royal Mail Postcode Address File (PAF)

- Telephone number verification

- National change of address processing

- Gone Away suppression files

- Electoral Roll Processing.

The following procedures can also be implemented to ensure the Payer and the account details provided are genuine.

Confirming account details –

- In a face to face enquiry Service Users should ask to see the Payer's cheque book, bank statement and / or debit card.

Confirming address details –

- Proof of address such as a driving licence or recent utility bill should be requested.

Additional Checks –

- Service Users should confirm if the Payer is new to its organisation. In certain markets such as utilities, mobile phones and subscriptions, Payers often switch suppliers and therefore may already exist on a database

- Ensure a system is in place, which is linked to address details, to intercept duplicate sorting code and account numbers

- Credit Checking.

DDI Validation

Bacs and Members perform validation checks on all DDIs and Direct Debits received. For full details see the AUDDIS Service Definition.

- DDIs failing Bacs' validation checks or returned by the Paying Banks with the appropriate reason will be advised to the Service User via its messaging electronic mailbox or paper advice.

- Any Direct Debit collection which is returned unapplied, shall be returned via the Automated Return of Unpaid Direct Debit system (ARUDD) or by 'Advice to Service User of a manually unpaid Direct Debit' form.

15.9 Core Reference

All AUDDIS Service Users must use core referencing. This reference must be quoted in field 10 of the Bacs data record and must be left justified.

15.10 Collection amalgamation

It is strongly advised that Service Users use the preferred standard practice of a one contract – one DDI approach. However, Direct Debit collections may be amalgamated under one DDI, providing that the Rules relating to Reference usage are applied. In the event, however, that there is any loss or damage caused to the Payer as a result of such amalgamation by a Service User, the Service User shall be responsible for such loss and damage, and shall indemnify the Paying Bank accordingly.

Multiple SUNs and multiple reference choices on a single DDI are only permitted for AUDDIS Service Users providing these are quoted on the DDI when the Payer signs. Any collections to be made under additional SUNs/reference not quoted on the original DDI requires the Service User to obtain a new DDI from the Payer.

Paying Banks strongly advise against the practice of amalgamated DDIs for different contracts into a single Direct Debit. Preferred practice is to maintain a one-to-one relationship between:

- the DDI signed by the Payer

- the DDI lodged with the Paying Bank

- the Direct Debits collected by the Service User.

One-off Direct Debits

The use of a DDI for the collection of a single Direct Debit is only permitted for AUDDIS Service Users providing the DDI is cancelled following the collection of the single Direct Debit i.e. the sequence of collections is 0N, 01 and 0C following AUDDIS lodgement rules. The 0C must only be sent once the collection has been received, this will ensure a re-presentation of the Direct Debit can be made if necessary. Payers must be advised that the narrative 'First payment' or an equivalent narrative may show on their bank statement; however this will be the only payment taken and the DDI will then be cancelled.

15.11 Direct Debit Instruction storage, retrieval and liability

The paper DDI remains with the Service User, who is responsible for authenticating the information on the form. It is up to the Service User to decide how long to store the paper and the method of storage. The Service User must provide a copy of the DDI within 7 working days if requested by the Paying Bank. If a copy can not be produced or the DDI is incorrect or fraudulent, then the Service User must accept liability under the terms of the Direct Debit Indemnity.

Storage

A Service User shall store the original DDI or an image thereof. If a Service User chooses only to store an image of the DDI, then it should store it in such a format as shall be admissible in evidence in any civil or criminal proceedings. The image stored shall be of such size and clarity as to ensure that the essential features of the DDI are clearly visible and legible, including but not limited to the customer's signature.

Retrieval

A Paying Bank may request a copy of a DDI from time to time by sending the Service User a 'Request for Copy DDI' form. This request may also be made even if the DDI has been cancelled. If the Service User is unable to provide a copy within 7 working days from the date of request, it will become liable for any Direct Debit collected under the DDI. A Paying Bank will not lose any rights if it does not remind the Service User to provide a copy DDI after 7 working days.

See section 15.20 for example of a form.

  A Paying Bank should include its fax number on the Request for copy of DDI form to allow the Service User to issue a copy within the 7 working day period.

Liability

A Service User shall be liable in cases where an AUDDIS DDI is signed fraudulently or not in accordance with the account operating mandate held by a Paying Bank.

See section 11.1 for details of Valid Indemnity Claims.

  N.B. It is advisable for Service Users to check with the Payer when a DDI is received under a business account or joint account. They should confirm the appropriate authority of the signatory or signatories.

15.12 Direct Debit Instruction amendment / cancellation

The Paying Banks will advise the Service User (via Bacs messaging service) of any amendment / cancellation advice received from the Payer. This service is also used to advise Service Users of any **AUDDIS DDIs** which have been rejected by Bacs or returned by the Paying Banks. It is strongly recommended that AUDDIS Service Users collect these advices electronically. It is also recommended that Service Users should then **apply these advices** directly to its systems **without manual intervention**.

- In the event of amendment / cancellation the Paying Banks will include in the advice, the last collection reference or core reference. Where no Direct Debit has been collected the core reference from the DDI will be used. To prevent a DDI being cancelled in error, it is recommended that a Service User adopts the one contract – one DDI approach to allow easy identification of the DDI.

- A cancelled / expired DDI may be reinstated by a Service User, in accordance with the customer's authority. This is not permitted where the DDI has been cancelled by the Paying Bank, the customer is deceased or the account is closed.

- A Service User may reinstate a cancelled DDI where the DDI has been cancelled in error because the Service User collects multiple payments under a single DDI. However, the Service User may be requested by the Paying Bank to produce a copy of the customer's signed authority within 7 working days. The customer's authority must be dated after the date of cancellation, which will provide evidence to the Paying Bank of the Payer's consent to reinstatement if collection is disputed. The Service User must be able to provide satisfactory evidence to the Paying Bank that it holds the necessary authority to collect Direct Debits from a Payer's account. A Service User failing to do so becomes liable for Direct Debits already submitted under that DDI.

The Paying Bank will confirm with the Payer that the evidence provided by the Service User is correct. Acceptable form of evidence is:

– copy of the new DDI.

– letter from the Payer confirming to the Service User that the cancelled DDI may be reinstated.

15.13 Dormancy

The Paying Banks operate a minimum 13 month dormancy period from DDI lodgement or last collection, i.e. length of time in calendar months after which a Paying Bank will drop details of a DDI because a Direct Debit has not been collected. If a Service User wishes to vary this period, it must apply to its Sponsor. The Sponsor will advise the Paying Banks of a Service User's extended dormancy period.

If a Service User does not present a Direct Debit against a DDI for 13 months, and has not requested an extended **dormancy period**, any subsequent Direct Debit must be preceded by a new DDI (0N), otherwise the Direct Debit shall be returned 'No Instruction'.

15.14 Changes to AUDDIS Direct Debit Instructions

- If a Service User wishes to change the SUN or the Reference of a DDI, it must ensure that the approval of its Sponsor has been received. The SUN / Reference can then be amended

- Once a Service User becomes an AUDDIS user, it is not permitted to revert to non-AUDDIS status.

- If an AUDDIS Service User is taken over by another Service User in the special circumstances where the new Service User is given a dispensation by the Sponsor to act on the DDIs given to the previous Service User, the new Service User must ensure that it has access to any paper DDIs, or images thereof (e.g. photocopy, digital scan, microfiche), submitted via AUDDIS by the previous Service User

- If a Service User wishes to merge two SUNs, the Service User must ensure that there is no duplication of core references across the two data files. Before undertaking this exercise the Service User must ensure it obtains the approval of its Sponsor

- If there has been a change to the reference, SUN or if the DDI has been cancelled and reinstated, the Service User must be able to provide proof that authority has been obtained to carry out the change. In the case of re-instatement this shall be in the form of a signed customer authority to reinstate.

Standing Order conversion

Where an AUDDIS DDI is intended to replace an existing Standing Order it is the Service User's responsibility to ensure that the Paying Bank is advised separately to cancel the Standing Order.

See section 14 for full details covering Standing Order conversion.

15.15 Monitoring of AUDDIS Service Users

A Service User should note that the Paying Banks will monitor the AUDDIS system and Service Users must ensure that they comply with AUDDIS rules. Failure to meet the level of performance expected will be referred to the Service User's Sponsor.

See section 12 'Monitoring the Scheme'.

Example of monitoring criteria:

- the appropriate use of each transaction code

- the production of a DDI or copy on request

- a Direct Debit claimed after cancellation

- the automatic rejection of a DDI and Direct Debit

- the number of Indemnity Claims

- a DDI presented against incorrect account detail

- the proper use of references.

15.16 Example of prohibited practices

- The Service User must not send a paper DDI to the Paying Bank under an AUDDIS SUN

- A Service User must not add additional SUN(s) or references to the DDI after it has been signed by the Payer

- Transaction code 17 must not be used for a first, final or re-presented Direct Debit

- A cancelled DDI may not be reinstated where the cancellation was instigated by the Paying Bank

- DDI information must not be telephoned through to a processing centre for input onto a Service User's Direct Debit database. Information must only be keyed from the original DDI or a complete image thereof.

15.17 Example of Multiple SUNs and Reference choices

Where a Service User chooses to use more than one SUN and reference on the DDI, these must be clearly displayed. These are examples of how this may be done.

Service User Number

1	2	3	4	5	6
2	3	4	5	6	7
3	4	5	6	7	8
6	5	4	3	2	1

References

123456789ABC
347945632DEF
973218443IXYZ
82239766FGHI

15.18 Example of a paper Advice of a new AUDDIS Direct Debit Instruction

This is for use by Paying Banks who are unable to receive electronic AUDDIS DDI output. In this case they receive paper DDIs in this format from Bacs; where the Paying Bank refuses to accept lodgement of the AUDDIS DDI the paper advice will be returned to the Service User marked 'lodgement refused'. Paper advices may be returned individually or with a Bank Bulk DDI Lodgement Referred/Rejected form.

See section 5.7 for an example of the Bank Bulk DDI Lodgement Referred/Rejected form.

1. Paying Bank

2. Payer

3. Payer's account details

4. The Service User

5. Service User's contact name and address

ADVICE OF NEW DIRECT DEBIT INSTRUCTION (AUDDIS)

Service User

Number: 9 9 1 2 3 4

1. To: The Manager ANY BANK

2. Name(s) of account holder(s)   D.R. HOWES

Name: A N COMPANY LIMITED   — 4

Reference   HOW02/67893/01

3. Branch Sort Code   7 0 - 0 9 - 2 0
   Account Number   8 7 6 5 4 2 3 9

If you have any queries on this Instruction, please contact:

RICHARD JONES   — 5

Telephone Number: 0161 735 4321 X3004

Fax Number: 0161 735 4325

Address: A N COMPANY LIMITED
ANY STREET
ANY TOWN
AB1 2CD

Bacs Processing Date: 23/11/05

15.19 Example of an AUDDIS returns report

This illustrates the use of reason codes on this advice on Bank returned DDIs.

ADDACS Advice of Bank Returned Direct Debit Instructions

Bacs

ADVICE OF BANK RETURNED DIRECT DEBIT INSTRUCTIONS FOR 17/01/95   17/01/95 10:15

DIRECT Debit

SUN : 156243   FRIENDLY FINANCE   Page 2

Record Type	Reference	Reason Code	Payer's Name	Sort Code	Account Number	A/C Type	Original Proc Date	Effective Date	Tran Code	Service User S/C Name	Details A/C	Note	ADDACS Sequence
D	A130/2450/2435RD	6	MORGAN-WHITE	40-31-28	59473324	0	15/01/95	16/02/95	0C	40-32-33	77677789	BACS	40000000
										FRIENDLY FINANCE			
D	A131/2451/2435RD	6	BROWN I.C.J.	40-31-28	52222324	0	15/01/95	16/03/95	0C	40-32-33	77677789	BACS	40000001
										FRIENDLY FINANCE			
D	A132/2452/2435EE	6	PENMAN Y.M	40-31-28	55555555	0	15/01/95	16/02/95	0C	40-32-33	77677789	BACS	40000002
										FRIENDLY FINANCE			
N	A133/2453/2435FF	B	EVANS J.E	40-31-28	59444224	0	15/01/95	16/02/95	0N	40-32-33	77677789	BACS	40000003
										FRIENDLY FINANCE			

Range of AUDDIS Advices   40000000 - 40000003   Complete   Total Number of Advices: 4

REASON CODE MEANINGS   1 = Instruction Cancelled by Payer 2 = Payer Deceased 3 = Account Transferred to a new Bank or Building Society 5 = No Account 6 = No Instruction B = Account Closed
C = Account Transferred to different Account / Branch of the Bank / Building Society F = Invalid Account Type G = Bank will not accept Direct Debits on Account
H = Instruction Expired I = Payer Reference is not unique K = Instruction cancelled by Bank

There are three 'Record Types':

D = Advises return of a 0C which is a cancelled DDI

N = Advises return of a 0N which is a new or re-instated DDI

S = Advises return of a 0S which is a converted DDI

15.20 Example of a Request for copy DDI form

Paying Banks will use form 15.20 when requesting sight of the original
(or copy of an AUDDIS DDI).

Direct Debit Scheme
Request for copy of
AUDDIS Direct Debit Instruction

DIRECT Debit

To:

Dear Sir,

Under the terms of the AUDDIS Rules we request you to forward a copy of the Direct Debit Instruction, detailed below, to this
branch within 7 working days of this request, for comparison with our records.

Details of Direct Debit Instruction

Service User Number (SUN)

Your Reference

Name of Payer

Payer Sort Code

Payer Account Number

Yours faithfully   Branch Stamp

Manager

Date

Fax Number

02/1478/11/06

16   PAPERLESS DIRECT DEBIT

Introduction

The Paperless Direct Debit service enables Service Users to sign up its customers for Direct Debit collections by telephone, the Internet, telephone keypad, face-to-face or interactive TV. Service Users can set up a Direct Debit Instruction (DDI) without the Payer having to sign a paper DDI. The Service User must obtain from the Payer details of his bank account, following the Script in this Guide, and the Service User shall lodge the DDI with the Paying Bank via **AUDDIS**. As such this service is only available to live AUDDIS Service Users. For full details of the AUDDIS service see section 15 of this Guide.

These Rules are in addition to the existing Direct Debit Scheme Rules and AUDDIS Rules, as detailed in this Guide. If a Service User fails to adhere to these Rules, they may be removed from the Direct Debit Scheme as detailed in section 13 of this Guide. **In joining the service, the Service User accepts liability in the case of a Payer disputing his authority had been given to set up a DDI**.

The use of a DDI for the collection of a single payment is only permitted for AUDDIS Service Users.

N.B. Whilst an outsourcing agent may complete the sign up process, the Service User will still be responsible for the actions of the organisation who are acting on its behalf.

If Paperless Direct Debit sign up is being outsourced, there must be an automated link between the Service User and the outsourcing agent. This will protect against incorrect re-keying of information and therefore go a long way towards eliminating discrepancies in key fields i.e. Payer's sort code, account number, name and ensuring compliance with the AUDDIS Rules.

Paperless Direct Debit encompasses the following sign-up methods:

Telephone

The Payer agrees to sign up for Direct Debit collection over the telephone by providing his account details to the Service User or its agent for completion of the DDI.

Internet

The Payer provides his authority for Direct Debit collections by completing an on-screen DDI which is sent to the Service User or its agent over the Internet.

Face-to-Face

The Payer in this instance must be offered a paper DDI to sign. If, however, the customer is given the option to have his details entered immediately into a computer without signing a DDI and agrees, the Service User may proceed following the rules and script in this Guide. If this information is being sent to a processing centre it must be fed electronically without re-keying.

Telephone Keypad

The Payer agrees to sign up for Direct Debit collection and his details are entered by depressing the telephone keypad following a series of pre-recorded operator directions which must follow the Script in this Guide.

Interactive TV

The Payer provides authority for Direct Debit collections by completing an on-screen DDI which is sent to the Service User or its agent by interactive TV. (Service Users should contact its Sponsor for script and example screen designs).

Other technologies for Paperless sign-up are not permitted without the Service User first obtaining the express approval of its Sponsor. Such approval is within the discretion of the Sponsor and may be refused. Seeking such approval will delay the application process.

16.1 Paperless Direct Debit Service User set-up

A Service User wishing to join the Paperless Direct Debit Service must apply to its Sponsor who will assess the application. The Service User must complete a separate application for each SUN.

Before commencing use of the Paperless Direct Debit Service, 2 Members of the Service User's staff must successfully complete the PDD e-learning training course. Further details will be provided to the Service User by its Sponsor.

Service Users must be aware of the associated additional risks involved in using the service, as follows:

- It is the Service User's responsibility to verify the customer and validate their details, i.e. identity; account details; customer address. (A number of software packages are available to assist in this process, details are available from the Bacs website at www.bacs.co.uk/bacs/businesses/resources/subscriber+library/).

- Service Users cannot Counter Claim following receipt of an Indemnity Claim for the reason 'Payer disputes having given authority'

- Service Users must be aware that there may be an impact on future business if Direct Debit ceases to be the preferred payment method for Payers

- The Service User must consider the wider reputational issues for the Scheme particularly with regard to the risk of fraud. Paperless Direct Debit may not be suitable for some transactions such as high value payments

Service Users may be subject to annual reviews of their Paperless Direct Debit process and procedures and failure to comply with the Scheme Rules may result in the removal of Sponsorship and exclusion from the Direct Debit Scheme.

Authority to begin Paperless Direct Debit sign-up will only be given when, and if, the Sponsor is satisfied that the Service User meets the requirements of these Rules. A Service User can only use the Paperless Direct Debit sign-up method authorised by its Sponsor. If additional methods are required the Service User must make a subsequent application to its Sponsor.

A Service User's application can be submitted at the same time as its application for AUDDIS. Alternatively a Service User may wish to apply for Paperless Direct Debit at a later date. The AUDDIS application timescales are applicable in all instances.

See section 15.1 for timescales

In order to participate in the Paperless Direct Debit Service, a Service User must have executed an Indemnity in one of the forms introduced with effect from 1.1.2004, a specimen of which is set out in Section 2.7. However, a Service User who was authorised before that date to participate in the Paperless Direct Debit Service, i.e. executed a specific Paperless Direct Debit Indemnity under the arrangements then in force may continue to do so.

See section 2 for full details on Indemnities

After execution, the signed Indemnity and accompanying authorising resolution must be returned by the Service User to its Sponsor.

A Service User wishing to carry out Paperless Direct Debit sign-up must comply with the following requirements on an ongoing basis:

• A Service User must have live status within AUDDIS before operating Paperless Direct Debit

• A Service User must only use their AUDDIS SUNs for Paperless Direct Debit applications

• No documentation for use within the Paperless Direct Debit Service shall be used by a Service User without prior approval from its Sponsor. This requirement covers all documentation to be used but particularly the following:

– The script for telesales staff, face-to-face, telephone keypad, interactive TV and Internet screens

– Direct Debit confirmation letter

– Advance Notice

– The Direct Debit Instruction.

16.2 Payer sign-up process

A Service User who has received approval for its documentation and acceptance into the Paperless Direct Debit environment, may then commence to sign up new Payers. However, it must use the approved script. A Service User's use of the script shall ensure the Payer is given a clear message and is left in no doubt that they have agreed to pay by Direct Debit and have set up a DDI.

The process must include the following steps:

Collection and validation of Payer's details

- The Service User must verify the identity of the Payer and his address, prior to the origination of any Direct Debits. It is recommended that this is achieved by using historical data from its records or for new customers by using a selection of registers e.g. electoral roll, post code list or credit rating list, which are available from Local Councils, the Royal Mail or other suppliers. **A list of verification measures to assist in verifying the Payers details is available from www.bacs.co.uk/bacs/businesses/resources/subscriber+library/**

- The Service User must obtain from the Payer details of his bank account including the sort code, account number and account name and confirm that the Payer is the only person required to authorise debits from the account. As business accounts often require more than one person to authorise debits to an account, this information will assist Service User's compliance with the AUDDIS Rules regarding the authentication of a Payer's identity and the authority to sign, before submitting the DDI to the Paying Bank.

If the customer is not the account holder and therefore not the Payer, or more than one person is required to authorise debits from the account, a paper DDI **must** be sent direct to the Payer(s) for completion, or be printable for completion by the Payer(s) in the case of the Internet service. The Direct Debit must not be set up until a completed paper DDI, duly authorised by the Payer(s) has been received.

- Service Users must validate the Payer's account details by applying 'modulus checking', at 'point of sale', when the Payer is still on-line. This will enable the Service User to correct any invalid information.

In addition Service Users shall also use the information details in the 'Crediting and Debiting Building Society Accounts' booklet to validate the Payer's sort code and account details. This is available from www.bacs.co.uk/bacs/businesses/resources/subscriber+library/

- During sign-up the Service User may confirm to the Payer the first Direct Debit collection date, frequency of the Direct Debit and amount. The Service User must also confirm to the Payer the Advance Notice period.

If at any stage the Payer does not wish to proceed with Paperless Direct Debit sign-up a paper DDI must be sent unless the Payer withdraws from requesting a Direct Debit completely. In such cases, the Direct Debit application must not be set up until a completed paper DDI, duly authorised by the Payer, has been received by the Service User.

Best Practice Standards

It is strongly recommended that the Service User also use the Industry Sorting Code Directory at point of sale when validating sorting codes. This is available from www.vocalink.com/iscd or your Software Supplier.

Confirmation of Payer sign-up

- Service Users must issue a written Direct Debit confirmation letter to the Payer within 3 working days from sign up. The confirmation letter must include the Payer's sort code, account number, account name, the Direct Debit Guarantee, and reference. This letter must be followed by the standard Advance Notice as described in section 4 of this Guide.

Alternatively, the confirmation letter incorporating the Advance Notice must be received by the Payer no later than 10 working days prior to the first collection date i.e. in advance of the account being debited (providing the first collection is made within a month from sign up). If the confirmation letter and Advance Notice are incorporated in one advice, then it must also include the amount to be debited, first collection date, frequency, and Advance Notice period.

For Internet Service Users the confirmation letter may be issued electronically providing it is formatted in the same way as the paper confirmation letter. However if electronic communication is used, the confidentiality of the customer's bank sort code and account number **must** be protected at all times. The Payer must be able to store and retrieve this letter for future reference. Use of electronic notification is at the Service User's risk as the Payer may dispute receiving such an advice.

16.3 The Direct Debit Indemnity and other liabilities

As one of the conditions of participation in the Direct Debit Scheme a Service User must execute the standard Direct Debit Scheme Indemnity ('the Standard Indemnity') which must be obtained from its Sponsor.

If the Service User participated in the Paperless Direct Debit Service before 1.1.2004 it will also have executed an additional Indemnity under the arrangements then in force. This Indemnity remains in full force and effect.

As no Counter Claim is permissible in the event of the Payer disputing they had given authority for the Service User's collection of Direct Debits under a DDI executed via Paperless Direct Debit, a Service User must pursue any action directly against the Payer. In order to do so the Service User must maintain appropriate archive records of DDI sign-up. Any such action takes place outside the Direct Debit Scheme. However, for the protection of Payers, the following minimum standards are required:

- Service Users shall maintain archive records of all communications with the Payer, i.e. Direct Debit confirmation letter and Advance Notice

- In the case of the Internet service, the Service User must have a method of confirming to the Payer that the Internet Instruction has been set up, such as a log of the DDI sign-up.

NB: Proof of despatch of a confirmation letter or confirmation letter incorporating Advance Notice is not proof of receipt by the Payer.

16.4 Paperless Direct Debit amendment/cancellation

Following advice from the Payer or Paying Bank that the Payer has closed the account or transferred to another bank the Service User must obtain the new account details from the Payer, as described in section 16.2 'Collection and validation of Payer's details'.

However, where the Service User has received an ADDACS advice with reason code 3, quoting both old and new paying bank details, a new authority is not required.

Some Service User's systems automatically generate standard letters and paper DDIs following receipt of an amendment/cancellation advice from the Paying Bank. In such circumstances, a Paperless Direct Debit Service User may continue with this process providing the new signed DDI is set up following the AUDDIS lodgement Rules.

16.5 Monitoring of Paperless Direct Debit Service Users

A Service User should note that the Paying Bank may monitor the service and Service Users must ensure that they comply with the Rules of the Direct Debit Scheme, AUDDIS and the Paperless Direct Debit service. Failure to comply will be referred to the Service User's Sponsor.

In addition to the AUDDIS monitors, the Paying Bank may also monitor the following:

– Confirmation letter conformity

– Compliance to the agreed script for telephone, face-to-face and keypad

– Compliance to the agreed Internet and interactive TV screens

– Use of the Service User's authorised Paperless Direct Debit sign-up method.
  e.g. telephone, Internet, telephone keypad and face-to-face.

16.6 Examples of Prohibited Practices

A Service User shall not:

- Operate Paperless Direct Debit sign-up without Sponsor authorisation

- Send a paper DDI for lodgement to the Paying Bank under an AUDDIS SUN

- Introduce any Paperless Direct Debit sign-up method which has not been previously authorised by its Sponsor

- Give only oral confirmation of a DDI set-up and/or future schedules of Direct Debit collections. Such information must be given to the Payer in written or electronic form

See section 4.3 for further details on Advance Notice

- Operate a Paperless Direct Debit service without the option to provide the Payer with a paper DDI if the Payer does not wish to proceed with Paperless Direct Debit sign-up.

- DDI information must not be re-keyed onto a Service User's Direct Debit database, there must be an automated link. Information must be fed electronically without re-keying from the point of DDI capture to the Service Users own system .

16.7 Mandatory layout of Confirmation Letter

Mandatory inclusions in italics

Mr A B Sample
1 Sample Street
Sample Town
AB1 CD2

<div style="border:1px solid">

Important: Confirmation of the
set-up of your Direct Debit Instruction

</div>

Dear Mr Sample

Thank you for buying goods and services from us. I hope you have found this new way of arranging your Direct Debit payment very convenient.

Having accepted your Direct Debit details, I would like you to confirm that they are correct.
Please can you check the details below.

- *Account name:*   • *Account number:*
- *Bank Sort Code:*

If any of the above details are incorrect please call us as soon as possible on 0123 456 7890. However, if your details are correct you need do nothing and your Direct Debit will be processed as normal. You have the right to cancel your Direct Debit at any time. A copy of the Direct Debit Guarantee is below.

For your information, the collections will be made using this reference.

- Service User Number:
- *Reference:*

Once again thank you for purchasing your goods from us, and I hope you continue to enjoy the benefits of buying goods and services over the phone by Direct Debit.

Yours sincerely

Name
Title

The Direct Debit Guarantee

- *This Guarantee is offered by all Banks and Building Societies that take part in the Direct Debit Scheme. The efficiency and security of the Scheme is monitored and protected by your own Bank or Building Society.*
- *If the amounts to be paid or the payment dates change (insert Company Name) will notify you (insert number of) working days in advance of your account being debited or as otherwise agreed.*
- *If an error is made by (insert Company Name) or your Bank or Building Society, you are guaranteed a full and immediate refund from your branch of the amount paid.*
- *You can cancel a Direct Debit at any time by writing to your Bank or Building Society. Please also send a copy of your letter to us.*

NB: The Direct Debit Guarantee must be included with or on this letter.
Please amend this letter to reflect the Paperless Direct Debit application used
e.g. telephone, Internet.

16.8 Mandatory layout of Confirmation Letter, incorporating Advance Notice

Mandatory inclusions in italic

Mr A B Sample
1 Sample Street
Sample Town
AB1 CD2

DIRECT Debit

> *Important: Confirmation of the set-up of your Direct Debit Instruction, including future payment schedule*

Dear Mr Sample

Thank you for buying goods and services from us. I hope you have found this new way of arranging your Direct Debit payment very convenient.

Having accepted your Direct Debit details, I would like you to confirm that they are correct. Please can you check that the list below including your payment schedule is correct.

- *Account name:*
- *Day of the month to be debited:*
- *Date of first collection:*
- *Frequency of collection:*

- *Account number:*
- *Bank Sort Code:*
- *Amount to be debited:*

If any of the above details are incorrect please call us as soon as possible on 0123 456 7890. However, if your details are correct you need do nothing and your Direct Debit will be processed as normal. You have the right to cancel your Direct Debit at any time. A copy of the Direct Debit Guarantee is below.

For your information, the collections will be made using this reference

- Service User Number:
- *Reference:*

Once again thank you for purchasing your goods from us, and I hope you continue to enjoy the benefits of buying goods and services over the phone by Direct Debit.

Yours sincerely

Name
Title

The Direct Debit Guarantee

DIRECT Debit

- *This Guarantee is offered by all Banks and Building Societies that take part in the Direct Debit Scheme. The efficiency and security of the Scheme is monitored and protected by your own Bank or Building Society.*
- *If the amounts to be paid or the payment dates change (insert Company Name) will notify you (insert number of) working days in advance of your account being debited or as otherwise agreed.*
- *If an error is made by (insert Company Name) or your Bank or Building Society, you are guaranteed a full and immediate refund from your branch of the amount paid.*
- *You can cancel a Direct Debit at any time by writing to your Bank or Building Society. Please also send a copy of your letter to us.*

NB: The Direct Debit Guarantee must be included with or on this letter.
Please amend this letter to reflect the Paperless Direct Debit application used
e.g. telephone, Internet.

16.9 Suggested Outline of Paperless Direct Debit Script

This script is a guide for Paperless Direct Debit transactions. It can be adapted to suit a business or an organisation's needs, but it must be approved by the Service User's Sponsor prior to use. It is to be used for telephone, telephone key pad and face-to-face applications. The following are mandatory inclusions:

- Verification that the customer is the account holder and therefore the Payer. If the customer is not the account holder a paper DDI must be sent to the Payer for completion. **A list of verification measures to assist in verifying the Payers details is available from www.bacs.co.uk/bacs/businesses/resources/subscriber+library/**

- Taking the Payer's Bank or Building Society account number, sort code and account name; and confirm that the person entering into the transaction is the only person required to authorise debits from the account. If more than one person has to authorise debits from the account a paper DDI must be sent to the Payer for completion

- Advice of the Advance Notice period

- Confirmation of bank details back to the Payer

- An explanation of the Direct Debit Guarantee

- Advice of the company name that will appear against the Direct Debit on the Payer's bank statement

- A Service User who is unable to lodge the DDI within 10 working days of the Direct Debit set-up must advise the Payer that the Direct Debit will not be set up on their bank account until XXXX (depending on when the Service User will lodge the DDI). However in all circumstances the Service User must transmit the DDI no later than 6 months from the date of set-up. The Payer must still be sent confirmation of the Direct Debit details in the post within 3 working days. Failure to lodge the DDI within these timescales may result in the DDI being rejected.

Best Practice Standards

It is recommended that branch address details are confirmed back to the Payer.

  NB. Branch address details in Service User software may differ to those provided by the Payer e.g. Service Centre details.

  Assuming the Payer has agreed to buy and asks, for example, to pay by monthly Direct Debit and the monthly amount to be debited has been agreed.

EXAMPLE – SCRIPT A

> *OK thank you. To avoid delay and to save you having to fill in any paperwork I can set up your Direct Debit Instruction right now over the phone. Would that be helpful?*

Payer agrees.

> *OK that's great. Now all I need to do is record your bank details. Is the account to be debited in your name?*

Payer says yes.

> *Can you please confirm your account name*

If the account is not in the payers name, arrange to send paper DDI as unable to set up telephone Instruction. Close call.

> *Is this a personal or business account?*

Confirm that the person entering into the transaction is the only person required to authorise debits from the account. If not, a paper DDI must be sent to the Payer for completion.

> *And what is the account number? And the branch sort code? This will be on your bank statement or along the bottom of your cheque book.*

If unknown go to script B.

Ask if they have used this account to make Direct Debit payments before as some Banks or Building Societies may not accept Direct Debits for certain types of account.

> *Now, we've agreed that the monthly amount will be £ _____ , but is there a particular day of the month you would like the money to come out of your account, for instance just after you're paid?*

If no preference given, agree on most suitable day for the Service User.

> *And the first collection will come out of your account next month, which will be the Xth of month and on the same day each month (depending on the frequency agreed) thereafter. The company name which will appear on your bank statement against the Direct Debit will be XXXXXXXX. That's it, you have set up your Direct Debit Instruction with us. You will be sent confirmation of this agreement in the post within 3 working days of this phone call (or not later than 10 working days before the first collection).*
>
> *All Direct Debits are protected by a guarantee. I can read it to you now or you can read it in our confirmation letter. Which would you prefer?*

If answer is 'read it now', read the Direct Debit Guarantee below. If the answer is no, go to confirming the account details.

> *In future, if there is a change to the date, amount or frequency of your Direct Debit, we will always give you X working days notice in advance of your account being debited. In the event of any error, you are entitled to an immediate refund from your Bank or Building Society. You have the right to cancel at any time and this guarantee is offered by all the Banks and Building Societies that take part in the Direct Debit Scheme. A copy of the safeguards under the Direct Debit Guarantee will be sent to you with our confirmation letter.*

> *Let me just confirm your Bank or Building Society account details back to you. Your account name is XXXXX XXXXXX, your account number is XXXXXXXX and your branch sort code is XX XX XX. Is that correct?*

If answer is yes.

> *That completes the setting up of your Direct Debit Instruction. Thank you very much for your time today. Goodbye.*

EXAMPLE – SCRIPT B

If the Payer does not know his account number and/or his sort code.

> *OK that's fine, do you have your cheque book handy?*

Once the Payer has his cheque book, ask if he has used this account to make Direct Debit payments before as some Banks or Building Societies may not accept Direct Debits for certain types of account.

> *Is this the account you want to make payments from? Do you see the three sets of numbers running along the bottom of each cheque, the first set of numbers is the number of the cheque, the second is your branch sort code could you read that to me?*

Record, check it is 6 digits. (NB: Many accounts have the sort code and account number at the beginning of the cheque book. If in doubt ask them to contact their bank).

> *And the third number is your account number, could you read that to me too please?*

Record, check it is 8 digits (NB: Some Bank or Building Society accounts can have 7 or 9 digits). Confirm the details back to the Payer and finish the call with advice of the Direct Debit Guarantee and Advance Notice period from Script A.

EXAMPLE – SCRIPT C

If the Payer already has a DD with you or is buying multi products i.e. Gas and Electricty, then the script does not have to be repeated. However, it must be made clear to the Payer, how many DDs are being set up, the references and the fact that the DDs will be taken from the same account.

> *OK that's fine. We can use those details.*

Confirm the details back to the Payer and finish the call with advice of the Direct Debit Guarantee and Advance Notice period from Script A.

RESPONSE TO POSSIBLE QUESTIONS

(to be used with Example Scripts A, B and C)

If the Payer asks how is it possible to set up a DDI over the phone.

> *We have recently started using an enhanced service provided by the banking industry so we are able to set them up over the telephone. All the normal safeguards of the Direct Debit Scheme still apply and we will always confirm the content of these calls to you in writing.*

If the Payer would prefer to use the post and receive a paper Instruction for completion and return.

> *I can do that for you. Is there a particular concern that you have with setting up the Direct Debit over the phone now?*

If the Payer would still prefer to use the post.

> *I can send you the forms in the post or, if you prefer, you can call back later. All the information you need to set up a Direct Debit Instruction is on your cheques.*

If the Payer is not the account holder.

> *As you are not the account holder, we will need to send the account holder a Direct Debit Instruction to complete and return. Can I confirm the address to send this to?*

If the Payer says he is concerned over the security of information.

> *I can understand that, but I can assure you that all information is retained in the strictest confidence. In the event that you have any queries or dispute an entry on your bank account you can of course rely on the Direct Debit Guarantee. Does that ease your concerns enough to want to go ahead now?*

Yes – continue with SCRIPT A.

No – Payer wants information in the post, check details and close politely.

If the Payer says he is concerned over mistakes being made.

> *I understand your concern and to reduce customers' concerns a number of measures are in place to safeguard against genuine mistakes. There is the Direct Debit Guarantee. Firstly, if at any time money is debited from your account incorrectly the Banks and Building Societies guarantee to refund it. Secondly, no changes to the date, frequency or amount debited can be made without notifying you normally at least XX working days in advance of your account being debited. And finally, you have the right to cancel any Direct Debit at any time simply by writing to your Bank or Building Society, with a copy to us. A copy of these safeguards will be included in our confirmation letter.*

Does that answer your concerns sufficiently for you to want to go ahead with the Direct Debit set-up now?

Yes – continue with SCRIPT A.

No – Payer wants information in the post, check details and close politely.

16.10 Suggested Outline of Internet Direct Debit Script

The following are suggested screen prompts for customers accessing an Internet site for Direct Debit sign-up. Service Users may be working with Internet agencies or other experienced Web professionals, but if not, they should use these scripts verbatim. All Service Users must include the following mandatory items within their screens.

- SSL Server Security must now be present and be a minimum of 128 bit

- A postal and email address must be provided to the Payer

- A general enquiries / customer service contact number must be given to assist the Payer if he has any urgent issues or a complaint to raise

- The information required to complete the on-screen DDI does not need to be captured directly onto the on-screen DDI, but once completed a copy of the DDI complying with the mandatory format in section 16.11 must be available for printing by the payer

- Verification that the customer is the account holder and therefore the Payer. If the customer is not the account holder a paper DDI must be sent to the Payer for completion or a copy must be available for printing, see section 16.12. **A list of verification measures to assist in verifying the Payers details is available from www.bacs.co.uk/bacs/businesses/resources/subscriber+library/**

- Taking the Payer's Bank or Building Society account number, sort code and account name; and confirm that the person entering into the transaction is the only person required to authorise debits from the account. If more than one person has to authorise debits from the account a paper DDI must be sent to the Payer for completion or a copy complying with the mandatory format in 16.12 must be available for printing by the payer

- Advice of the Advance Notice period

- Confirmation of bank details back to the Payer

NB. Branch address details in Service User software may differ to those provided by the Payer e.g. Service Centre details.

- An explanation of the Direct Debit Guarantee

- Advice of the company name that will appear against the Direct Debit on the Payer's bank statement

- A Service User who is unable to lodge the DDI within 10 working days of the Direct Debit set-up must advise the Payer that the Direct Debit will not be set up on their bank account until XXXX (depending on when the Service User will lodge the DDI). However in all circumstances the Service User must transmit the DDI no later than 6 months from the date of set-up. The Payer must still be sent confirmation of the Direct Debit details in the post within 3 working days. Failure to lodge the DDI within these timescales may result in the DDI being rejected.

Assuming the Payer has agreed to buy and asks, for example, to pay by monthly Direct Debit and the monthly amount to be debited has been agreed.

STAGE ONE: OPENING

Direct Debits can now be set up on-line or over the telephone in addition to the original postal method.

All the normal Direct Debit safeguards and guarantees apply. No changes in the amount, date or frequency to be debited can be made without notifying you at least XX working days in advance of your account being debited. In the event of any error, you are entitled to an immediate refund from your Bank or Building Society. You have the right to cancel a Direct Debit Instruction at any time simply by writing to your Bank or Building Society, with a copy to us.

STAGE TWO: SIGN UP OF BANK DETAILS

In order to set up your Direct Debit Instruction on-line you will need to provide the following information through the setting up procedure (your cheque book contains all the bank details that you require):
Bank or Building Society name and account number, sort code and branch address.

- If you are not the account holder, a paper Direct Debit Instruction will be sent for completion. Please click to end

- If this is a personal account continue with the set-up procedure

- If it is a business account and more than one person is required to authorise debits on this account, a paper Direct Debit Instruction will be sent to the Payers for completion. Please click to end.

Alternatively you can print off your on-screen Direct Debit Instruction and post it to us. If you are unable to print please contact us on XXXXXX (tel no) and we will post you a paper Direct Debit Instruction.

If you do not wish to proceed any further please click to END.

The details of your Direct Debit Instruction will be sent to you within 3 working days or no later than 10 working days before the first collection.

Click the mouse on YES or NO to confirm details:
YES (onto next stage)
NO (redo form)
CANCEL to stop the set-up procedure (go back to start page).

STAGE THREE: RECONFIRMING THE DETAILS TO THE CUSTOMER

These are the details that you have entered to set up the
Direct Debit Instruction:

> Name of Account Holder
> Branch Sort Code   /__ __/__ __/__ __/
> Bank Account Number /__/__/__/__/__/__/__/__/
> Amount to be debited from Bank Account (if known)
>   £__/__/__/__/__/__/__/__•__/__/
> Date each month for collection (or other collection frequency) /__/__/
> The company name which will appear on your bank statement against the
> Direct Debit will be XXXXXXXX.

Click mouse on YES or NO to confirm details:
YES (onto next stage)
NO (redo form)
CANCEL to stop the set-up procedure (go back to start page).

STAGE FOUR: ADDRESS FOR THE LETTER OF CONFIRMATION

Your Direct Debit Instruction will be confirmed to you by e-mail within
3 working days. Alternatively the confirmation letter incorporating your
Advance Notice will be received by you no later than 10 working days prior
to the first collection date. If you prefer to receive this by post please indicate
the address you would like this to be sent to.

> _____
> _____
> _____
> _____

Click for next stage (stage five)

STAGE FIVE: COMPLETING THE SIGN-UP

That completes the setting up of your Direct Debit Instruction and the
confirmation of the Instruction will be sent to you within 3 working days or be
received by you no later than 10 working days before the first collection.

  Thank you very much for your Direct Debit Instruction details. Here is the
Direct Debit Guarantee for your information. (Direct Debit Guarantee
appears on-screen).

16.11 Example of Screen for Internet Direct Debit

Company Name

Company Address

DIRECT Debit

Instruction to your Bank or Building Society to pay by Direct Debit

Name(s) of Account Holder(s)

Service User Number

Bank/Building Society Account Number

Reference

Branch Sort Code

Instruction to your Bank or Building Society

Please pay (insert Company Name) Direct Debits from the account detailed in this Instruction subject to the safeguards assured by the Direct Debit Guarantee. I understand that this Instruction may remain with (insert Company Name) and, if so, details will be passed electronically to my Bank/Building Society.

Name and full postal address of your Bank or Building Society

To : The Manager   Bank/Building Society

Address

Postcode

Date

Day   /   Month   /   Year

Banks and Building Societies may not accept Direct Debit Instructions for some types of account

SUBMIT   **CLEAR**

Example of Direct Debit Guarantee

Please print off and retain

DIRECT Debit

The Direct Debit Guarantee

■ This Guarantee is offered by all Banks and Building Societies that take part in the Direct Debit Scheme.
The efficiency and security of the Scheme is monitored and protected by your own Bank or Building Society.

■ If the amounts to be paid or the payment dates change (insert Company Name) will notify you (insert number of) working days in advance of your account being debited or as otherwise agreed.

■ If an error is made by (insert Company Name) or your Bank or Building Society, you are guaranteed a full and immediate refund from your branch of the amount paid.

■ You can cancel a Direct Debit at any time by writing to your Bank or Building Society.
Please also send a copy of your letter to us.

Refer to section 3.8.1 for alternative Direct Debit Guarantee wording

16.12 Mandatory Screen for Internet Direct Debit for printing as a Paper Direct Debit Instruction

To be printed off by customer, completed and returned to the Service User.

Direct Debit Guarantee to be retained by Payer.

DIRECT Debit

Please fill in the whole form using a ball point pen and send it to:

Company Name

Company Address

Instruction to your Bank or Building Society to pay by Direct Debit

Service User Number

Reference

Name(s) of Account Holder(s)

Bank/Building Society account number

Branch Sort Code

Name and full postal address of your Bank or Building Society

To: The Manager   Bank/Building Society

Address

Postcode

Instruction to your Bank or Building Society
Please pay (insert Company Name) Direct Debits from the account detailed in this Instruction subject to the safeguards assured by the Direct Debit Guarantee. I understand that this Instruction may remain with (insert Company Name) and, if so, details will be passed electronically to my Bank/Building Society.

Signature(s)

Date

Banks and Building Societies may not accept Direct Debit Instructions for some types of account

16.13 Automated Voice System Script

The text includes a number of break out points should the caller experience difficulties.

	Main Prompt	Help Prompt
Introduction	In order to set up a Direct Debit you will need to provide your bank account details. All the normal safeguards of the Direct Debit Scheme still apply and we will confirm the content of this call together with a copy of the safeguards to you in writing within <x> days[6]. Please be assured that the information will be held securely.	
Fixed rate *(optional)*[1]	We will be setting up a Direct Debit, which will take equal monthly payments from your bank account. Do you wish to go ahead with this?	If you wish to set up a Direct Debit, an agreed amount of money will be paid directly to us each month enabling you to spread the annual cost of your account. Do you wish to go ahead with this?
Caller is account holder	Is the name we have on your account the same as the name that appears on your bank account?	Please confirm that the name on the bank account from which you wish to make payments is the same as the name that appears on your <company> account
	[If caller is not account holder & agent is available] **Thank you. Please hold whilst we transfer you to an agent** **[If caller is not account holder & agent is not available]** Thank you. A paper Direct Debit Instruction will now be sent to the account holder for authorisation[2].	
Sole Authoriser	Are you the sole authoriser for the bank account to be debited?[3]	Does anyone else need to authorise debits from this account?
	[If caller is not Sole Authoriser & agent is available] **Thank you. Please hold whilst we transfer you to an agent** **[If caller is not Sole Authoriser & agent is not available]** Thank you. You will now be sent a paper Direct Debit Instruction to be signed by the account authorisers.	

Introduction	Main Prompt	Help Prompt
Collection amount	The suggested amount for your monthly Direct Debit is <amount>; this includes your outstanding balance (as well as a Direct Debit discount). Do you want to continue?	The amount suggested would be the amount taken each month from your bank account. It includes any outstanding balance as well as a direct debit discount. Please confirm that you wish to go ahead with this.
Bank account details	The next step will be to collect your bank account details. What is your bank account number?	What is the account number for the bank account that the Direct Debit will be taken from?
	Thank you. Now what is your branch sort code, which is a 6 digit number?	You should read the number as a series of digits including any zeroes.
	Thank you. Please wait whilst we verify your sort code and account number.	
Collection date	OK. What is the day of the month that you would prefer the collection to be made on; (it must be between 1 and 28).	In order to set up a Direct Debit you need to choose the day on which the collection will be made. What is your preferred day of the month which must be between 1 and 28.
	For the date given, the first collection will be due on <first_collection_date>.	
Confirmation	So to confirm, you would like to pay your account by direct debit. We will be claiming <amount> in the name of <company> 4 on the <day> of each month from account number <acc_number> and sort code <sort_code>. If the date, amount of frequency of your Direct Debit changes, we will always give you at least 10 working days notice in advance of your account being debited.[5]	
	Do you want to go ahead with this?	Please confirm that you wish to set up this Direct Debit.

	Main Prompt	**Help Prompt**
Guarantee	Thank you. Your Direct Debit set up is now complete. Because this Direct Debit was set up over the telephone you will now hear the Direct Debit Guarantee. If in future there is a change to the date, amount or frequency of your Direct Debit, we will always give you at least 10 working days notice in advance of your account being debited. In the event of an error you are entitled to an immediate refund from your bank or building society. You have the right to cancel your debit at any time. A copy of the Direct Debit Guarantee will be sent to you in the post with a confirmation of the agreement and first collection date.	
Set up on other accounts	Do you want to set up a Direct Debit on any of your other accounts?	You have more than one account with us and can set up a Direct Debit on each of them during this phone call. Do you wish to set up a Direct Debit on any other of your accounts?

1. **Fixed rate – now made optional**
2. **Caller is account holder – if negative response then inform caller that a DDI will be sent out**
3. **Bank account details – is caller sole authoriser**
4. **Confirmation – include name that will appear on caller's bank statement**
5. **Confirmation – prior to this include advance notice period**
6. **Confirmation – prior to this include timescale for receipt of confirmation letter.**

17 INTER BANK TRANSFER OF DIRECT DEBIT INSTRUCTIONS AND STANDING ORDERS SERVICE (ToDDaSO)

Introduction

Where a Payer transfers his account from one Paying bank ("the old Paying Bank") to another ("the new Paying Bank") then he is able to take advantage of the Inter-Bank Transfer service to transfer his DDIs and Standing Orders. The Payer's Bank as the new Paying Bank will give advice to the Service User of the change to the DDI. This section sets out details of the Inter Bank Transfer service relating to Direct Debits. The process for Standing Orders is not covered in these Rules.

How does it work?

The new Paying Bank will request from the old Paying Bank, on the Payer's behalf, a list of DDIs and Standing Orders paid from his account at the old Paying Bank. The following details must be provided for each DDI: Service User's name, SUN and reference. The old Paying Bank is required to provide the information in full in accordance with timescales detailed in the Banking Code. This practice ensures that the new Paying Bank has current information.

For each DDI the customer wishes to transfer, the new Paying Bank will notify the Service User.

N.B. Not all customers will take advantage of this service. Some may still choose to advise the Service User directly therefore Service Users must have procedures in place to handle these requests.

17.1 Lodgement

For each change to the DDI the new Paying Bank will inform the Service User. This notification will be issued either electronically, using the Automated Direct Debit Amendment and Cancellation Service (ADDACS) reason code 3 message containing both the old and the new Bank details or by manual advice. If a Paying Bank is live on ADDACS all advices issued must be via the automated method, unless there has been a systems failure.

See section 17.6 for an example of a report.

See section 17.7 for an example of a manual advice.

Service Users must action these advices immediately, or within 3 working days from receipt. The Service User must not contact the Payer to obtain a new DDI; the advice is the Service User's authority to debit the new account.

- For Non AUDDIS Service Users the Payer's authority given to the new Paying Bank taken with the list provided by the old Paying Bank shall constitute the DDI for the purposes of the rules, without lodgement of any new DDI by the Service User. Therefore the Service User is not required, in this instance, to follow the normal DDI completion and lodgement process as detailed in Section 5. Service Users must however apply the change to their datafile and continue with Direct Debit collections.

- AUDDIS Service User's must send a '0N' to lodge the new Instruction within 10 working days. Collections can then continue providing the necessary 5 working day period following lodgement has elapsed. The lodgement period has been reduced from 5 working days to 2 working days to ensure the collection of the Payer's Direct Debit is not delayed by more than 3 working days from that specified in the Advance Notice. However where collection time scales allow, it is recommended 5 working days are left before the first collection to ensure that no '0N' rejections are received.

Should the Service User fail to collect the Direct Debit as specified further notification must be given to the Payer of the new collection date.

If any Direct Debit collections have been sent to Bacs in advance of the input day or a Service User collects Direct Debits from the old Paying Bank after receipt of a transfer advice, there is a possibility that the old Paying Bank may reject them.

17.2 New Paying Bank's responsibilities

- The new Paying Bank shall:
  - Obtain details of all Direct Debits collected from the old Paying Bank account
  - Obtain Payer's agreement to the list of the DDIs which will be transferred
  - Advise the Service User of the new account details in time for the transfer date
  - Advise the old Paying Bank, under advice to the customer, to cancel the DDIs and close the account (if required)

- In carrying out an Inter Bank Transfer under these provisions, the new Paying Bank shall comply with these Rules

- Should there be a dispute over whether the Payer has authorised the transfer of any DDI, or whether an advice was issued the new Paying Bank will produce a copy of the ADDACS record or proof that an automated ADDACS advice has been sent to Bacs.

17.3 Service User's responsibilities

- Service User's must action advices immediately or within 3 working days from receipt

- All AUDDIS Service Users must send a '0N' transaction using the new bank details within 10 working days

- Service User's must collect the first Direct Debit following transfer using transaction code 01

- Service User's must ensure that they keep an audit trail of ADDACS Code 3 messages in order to respond to Indemnity Claims raised

- If the Inter Bank Transfer of Direct Debit Instruction delays the Payer's Direct Debit collection by more than 3 working days from that specified in the Advance Notice a further notification must be given to the Payer of the new collection date

See section 4.2 for details.

- It will be regarded as best practice for Service Users not to issue a letter to the customer confirming the new account and Direct Debit collection details

- Subsequent to the Inter Bank Transfer the old Paying Bank will cancel the DDIs, held on their systems, which are no longer valid and an ADDACS advice will be produced (as detailed in section 10.1). In the event that a Service User receives an ADDACS advice from the old Paying Bank in respect of any Direct Debits included in the Inter Bank Transfer then the Service User shall disregard the ADDACS advice as it has been superseded by the Inter Bank Transfer.

There maybe occasions when, (see examples below) following the generation of an ADDACS advice, you may wish to speak to the Payer's Bank or the Payer's bank may wish to speak to you (the Service User) to query or check the details contained in the advice. Discussions should be restricted to information pertinent to the Direct Debit:

- Query cancellation of a DDI – discussion should be restricted to the date of cancellation, the reference and the cancellation reason code, because this will be shown on the ADDACS advice

- Query amended DDI – discussion should be restricted to the date of amendment, the reference, and the reason code used, because this will be shown on the ADDACS advice

- Query transfer of a DDI – discussion should be restricted to the date of transfer, the reference, and the reason code, because this will be shown on the ADDACS advice.

In summary, neither you nor the Payer's bank should volunteer or divulge any personal information regarding the customer or their personal circumstances, limiting discussions to details known to both you and the Payer's bank e.g.

  - The Direct Debit reference

  - Date of last displayed amount claimed

  - The ADDACS reason code as mentioned above.

Dialogue should be restricted to information pertinent to the Direct Debit as above.

17.4 Suppression facility at Bacs

As detailed in section 17.1 those new Paying Banks who use ADDACS will send their DDI amendments via Bacs. On receipt of the reason code 3 ADDACS advice Bacs will create a list of DDI transfer messages based on the following:

- Old Paying Bank sort code and account details

- New Paying Bank sort code and account details

- Service Users Number (SUN)

- The reference information provided by the old Paying Bank (this will be either the **last used reference** or the **core reference**).

Bacs will then match all subsequent ADDACS cancellation and closures messages i.e. ADDACS codes 1, 3 or B from the old Paying Bank to the details in the DDI transfer list. Where an exact match is found, the ADDACS advice will be suppressed and not sent to the Service User.

However there may be occasions where the reference detailed on the ADDACS reason code 3 from the new Paying Bank does not match with the reference quoted in the ADDACS cancellation advice provided by the old Paying Bank and therefore suppression will not occur. In the event that a Service User receives such an ADDACS advice from the old Paying Bank having already been notified by the new Paying Bank of the new account details, then the Service User shall disregard the ADDACS advice from the old Paying Bank.

This may occur where a Service User uses variable references for collecting Direct Debits (i.e. the reference changes for each collection) therefore this may not be the same reference as the one notified to the new Paying Bank by the time the DDI's are cancelled at the old Paying Bank.

See section 17.7 for an example of manual advice

Bacs will be unable to suppress any advices which are received manually by the Service User, as these are not processed via Bacs.

17.5 Example of prohibited practice

- Service Users must not request the Payer to sign a new DDI upon receipt of a transfer advice.

17.6 Example of an ADDACS report

Bacs ADVICES OF DIRECT DEBIT AMENDMENT AND CANCELLATION FOR 20/12/01 20/12/01 10:15

SUN: 756243 COINCIDENTAL INSURANCE Page 2

Reference	Reason Code	Name	Sort Code	Account Number	Due Date	Freq	Amount	Effective Date	Last Payment Due Date	ADDACS Sequence
A134/2453/2435RD	1	MORGAN-WHITE	40-31-28	59473324	03/12/01	M	£101.23	20/12/01	02/01/02	40000000
B/2/243	C	ANGELA WADE	30-22-28 30-31-28	76543324 69174546				20/12/01		40000001
B134/2492/2435RE	1	MISS D.THOMAS	40-31-44	45353324	03/12/01	M	£77.23	20/12/01		40000002
D123/2553/2435RD	B	MR A. RODGERS	40-25-32	69170012				20/12/01		40000003
E229/2653/2435RD	B	ALAN EMERY	40-25-28	69173324				20/12/01	02/12/01	40000004
M786/2777/2435MN	E	SHEILA WHITE MRS. S BROWNSLOW	20-18-28 20-18-28	39463324 39463324	03/12/01 03/12/01	M M	£37.83 £37.83	20/12/01	24/12/01	40000005
M546/2853/2435EF	3	JAMIE JOHNSON	60-16-87 30-22-28	15379603 55254756				20/12/01		40000006
R122/2855/2435EF	3	TOM ENGLISH	40-13-56 30-22-28	78538023 69174545				20/12/01		40000007
X111/4526/2435MN	E	IAN HEMMINGWAY	30-22-28 30-22-28	85452324 85453972				20/12/01		40000008

Submission Range of 40000000 - 40000008 Complete

Total Number of Advices : 9

REASON CODE MEANINGS: 0 = Instruction cancelled refer to Payer 1 = Instruction Cancelled by Payer 2 = Payer deceased
 3 = Account transferred to a new Bank or Building Society B = Account Closed
 C = Account/Instruction transferred to a different branch of Bank/Building Society D = Advance Notice Disputed
 E = Instruction Amended R = Instruction Reinstated

17.7 Advice of Transfer of Direct Debit Instruction

Advice of Transfer of Direct Debit Instruction to (AN Bank)

DIRECT Debit

Service User's name and address	From: The Manager (AN Bank)

This document is your authority to change your records. If clarification is needed please consult section 17 of the Service User's Guide and Rules to the Direct Debit Scheme.

Service User Number ☐ ☐ ☐ ☐ ☐ ☐

Date

Dear Sir,

Your customer, named below, has instructed us that the Direct Debit Instruction(s) listed should in future be collected from us. Please collect future Direct Debits using the new account details, as specified below.

AUDDIS Service Users – **Please submit a '0N' transaction quoting the new sort code, account number and core reference. Please arrange to collect the first payment using the '01' transaction code.**

Non AUDDIS Service Users – **The DDI has been set up on your customer's new account with us, please amend your records to quote the new sort code and account number. Please arrange to collect the first payment using the 01 transaction code.**

Customer name

Reference Number (Multiple reference numbers are detailed on an attached sheet)

Old Bank sort code ☐ ☐ ☐ ☐ ☐ ☐

Old Bank account number ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

NEW BANK DETAILS

Sort Code ☐ ☐ ☐ ☐ ☐ ☐

Account Number ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

If you have any queries, please call ( )

NB   1. There is no need to verify these new account details with your customer.
     2. Please ensure that this newly set up instruction is not affected when the old instruction is cancelled.

TO BE RETAINED BY SERVICE USER

02/1430/10/07

APPENDIX 1: GLOSSARY OF TERMS

Abbreviated Service User's Identity

Shortened version of the Service User's name as annotated in field 9 of the Bacs record. (See also Field 9).

Acknowledgement (DDI)

Additional section to the Direct Debit Instruction (DDI) that the Paying Bank / Building Society completes and returns to the Service User to confirm lodgement of the DDI. (To be discontinued, see section 6.2.)

ADDACS

The service allowing banks/building societies to advise Direct Debit Service User via Bacs of any amendments to or cancellations of Direct Debit Instructions. The message is sent either electronically or on paper.

Advance Notice

The notice period (normally 10 working days plus postal time) given to the Payer in respect of the date of debiting and the amount to be debited, in accordance with section 4.

Agency Bank

A type of sponsored institution. An agency bank participates in clearing and can nominate to sponsor service users but must have an agency relationship with a scheme member for purposes such as settlement and has limited liability. Sometimes referred to as an indirect clearer.

Amalgamation of Collections

Multiple or combined payments relating to more than one contract collected under a single DDI.

APACS

The Association for Payment Clearing Services.

Arrestment

A legal warrant lodged by a Sheriff Officer or a Messenger-at-Arms with a person, owing money to or holding goods on behalf of another, who is being sued by a third party for payment of a debt or performance of an obligation.

ARUDD

The service allowing banks/building societies to return to the Service User any Direct Debit payment instructions they could not apply. The debit is returned to the Service User's account and Bacs generates a report for the Service User detailing the Direct Debit that is being returned unpaid and the reason for the return.

AUDDIS

The service enabling Direct Debit Instructions to be transferred electronically from Service Users to the paying banks and building societies via Bacs.

AUDDIS (DDI)

For the purpose of AUDDIS the AUDDIS DDI is either the Instruction itself or any subsequent written communication from the customer to the Service User amending the terms of the original AUDDIS DDI.

Bacs Cycle (This is also known as 'Processing Cycle')

The Bacs 'operational' cycle (minimum 3 English Bank working days) comprises:
Day 1 (Input Day) – Service User submits data to Bacs as per timetable laid down in the Service User Guide – Bacstel-IP.
Day 2 (Processing Day) – All data accepted is processed through Bacs and passed onto the Paying Banks.
Day 3 (Entry Day) – The Payer's account is debited and the funds are credited to the Service User's account.

Bacstel-IP

A service providing a highly secure access channel into Bacs. It uses internet technologies and public key infrastructure (PKI) security to allow access to Bacs payment services including payment file processing, report accessing etc. Bacstel-IP carries out some online validation of submissions.

Bureau

A type of service user. Submits payment files to Bacs on behalf of a number of other service users. A bureau is a type of direct submitter but a bureau cannot originate payment instructions. There are different types of bureau:
a) Commercial – submits payment files on behalf of third parties and must be certified as a Bacs approved bureau.
b) In house – submits payment files on behalf of other service users that are all part of the same company or group of companies as the bureau.
c) Other – any bureaux that do not fit into the other two categories, e.g. a sponsor service operated by another organisation on the sponsor's behalf.

Bureau Service User Number

A number allocated to a bureau to uniquely identify it to Bacs. A bureau Service User Number starts with a B followed by five digits.

Commercial Computer Bureaux

A bureau is an organisation that is authorised by a Sponsor to make submissions to Bacs on behalf of one or more Service Users. It is identified by a 6-digit Bureau Number (Bureau Format).

A bureau may also be an organisation which submits to Bacs on behalf of third parties in non-bureau format or under its own SUN.

Consequential Loss

A loss incurred by a Payer which is a consequence of the direct loss suffered as a result of an erroneous Direct Debit transaction.

Core Reference

A minimum of six alpha-numeric upper case characters that is allocated by a Service User to identify a Direct Debit Instruction. This reference is quoted in all subsequent Direct Debit collections to allow the paying bank to match the payment instruction to the original DDI.

Counter Claim

A claim raised by the Service User against the Paying Bank following settlement of an Indemnity Claim which the Service User believes to be unjustified.

Direct Debit Instruction (DDI)

Sent by the Service User to the payer's bank/building society as the authority to pay Direct Debits from the payer's account. These can be sent electronically through Bacs.

Direct Debit

The collection of an agreed amount from a bank/building society account by a Service User, on request. The amounts and dates may vary from payment to payment. The payment request is sent via Bacs.

Direct Debit Guarantee

The guarantee offered by paying banks to payers in respect of the Direct Debit Scheme specifying the rights and safeguards of payers.

Dormancy Period

The time after which a bank/building society will drop details of a DDI from a payer's account if no collections have been made in that time. The period is normally 13 months and is recorded against a Direct Debit Service User Number (SUN) on the Direct Debit Service Users database.

Due Date

The date on which a Direct Debit payment is due to be taken. The payment can actually be taken up to and including 3 working days after the due date – see payment date.

Electronic Funds Transfer – File Structures

The document, which details the technical specification for file submission to Bacs.

Entry Day (Day 3)

(See 'Bacs cycle'.)

Expiry

When a Direct Debit Instruction has expired. (The process of a Direct Debit authority running out). See dormancy period.

Facilities Management

In the context of the Direct Debit scheme, a Service User or bureau that takes responsibility for the collection or administration of Direct Debits on behalf of another institution/company that may not be a Service User in its own right.

Field 9, 10 and 11

Field 9 of the data record.
The 'short name' of the Service User (max 18 characters) which appears in the Direct Debit payment record and may appear on the Payer's bank statement.

Field 10 of the data record.
The 'reference number' (max 18 characters) applied to the DDI by the Service User when it is lodged with the Paying Bank. This must also appear in the Direct Debit payment record.

Field 11 of the data record.
The Payer's account name (max 18 characters). This must be the name of the person who is paying the Direct Debit and has signed the DDI.

Fixed Amount or Date DDI

A DDI where the amount to be collected is fixed with respect to amount and / or date. These are no longer allowed by the Scheme.

Garnishee Order

(See Third Party Debt Order)

Indemnity

A document under the Direct Debit scheme that contains a legally binding undertaking to make payment to a paying bank in response to an Indemnity Claim. An Indemnity, in standard form, is an essential requirement of the Direct Debit scheme.

Indemnity Claim

A claim made by the Paying Bank in respect of an incorrect Direct Debit being applied to an account.

Industry Sorting Code Directory (ISCD)

A directory that combines a number of key databases. It contains information about all banks/building societies connected to any of the UK clearing systems: Bacs, CHAPS and Cheque and Credit Clearing. The directory contains a record for each bank/building society branch and other financial institutions involved in the UK payment systems. It includes the sorting code, branch details and details of the bank that settles transactions for the branch in each of the clearings.

Inter Bank Transfer of Direct Debits and Standing Orders

A service to assist customers when moving their bank/building society accounts by electronically transferring Direct Debit and standing order information between banks/building societies.

Irregular Payments

A Direct Debit that is not collected on a regular basis, but that is collected more than once in a 13-month period.

Input Day (Day 1)

(See 'Bacs cycle'.)

Instruction

See DDI (Direct Debit Instruction)

Legal Entity

A Service User must be either a legal person (natural or corporate or, in Scotland only, a partnership) or exceptionally a collection of persons governed by a defined legal framework (such as a partnership or unincorporated association). These are referred to in this Guide as legal entities. A group of companies is not a legal entity, unless they are formally constituted as a partnership.

Letter of Nomination

A formal letter by an Agency Bank to its Sponsor nominating one of its customers as a Service User. (See section 2.1.)

Lodgement (Lodged)

The process of the Paying Bank accepting the DDI.

Management Administration

A Service User may contract an organisation to manage its Direct Debit application. However, the Service User must take full responsibility for the actions of the other organisation on their behalf.

Mandate

This term, as used in previous editions of this Guide, has been replaced by Direct Debit Instruction. (See also DDI [Direct Debit Instruction]).

Migration (AUDDIS)

The process by which a Service User transfers non-AUDDIS DDIs to the automated AUDDIS system. (See section 15.3.)

Modulus Check

An arithmetic process to determine if there is a valid link between a sorting code and an account number range, i.e. whether a particular account number could exist at a specified sorting code.

Nominated Account

A bank/building society account from which a service user can originate payment instructions. The nominated account can be an individual account or a group individual account.

Notice of Expiry

Shall be deemed to have been given if the Service User identifies the final collection under the expiring DDI by use of transaction code 19.
(See also Expiry.)

'On or immediately after'

On or within 3 Bank working days of the specified payment date given in the Advance Notice.

Originator

A service user who originates payment instructions, whose bank/building society account details make up the originating account information in a payment instruction, and who is responsible for those payment instructions. An originator can be either a direct or an indirect submitter.

Originator's Identification Number (OIN)

A unique six-digit number allocated to each service user who is authorised to use the Direct Debit scheme. For Direct Debit scheme Service Users, this number is the same as the service user number.

Paper Vouchers

Paper Direct Debit collections processed through the paper clearing system. This service is no longer allowed, only automated collections via Bacs are acceptable.

Participants of the Direct Debit Scheme

These are:
– The Sponsor; The Service User and the Paying Banks / Building Societies.

Payer

The person that, by authorising a Direct Debit Instruction, allows a Service User to collect Direct Debits from their account.

Payer's Branch

The Paying Bank branch holding the Payer's account to be debited.

Paying Bank

The bank/building society at which a Direct Debit Instruction is lodged for a payer and that raises messages to advise of amendments or cancellations in relation to the Direct Debit Instruction.

Payment Date

The date on which a Direct Debit payment is made. This can be done up to or including three working days after the due date.

Processing Cycle

The minimum time taken for a payment instruction to be submitted to Bacs for processing and the time it reaches the destination account. The processing cycle has four stages: arrival, input, processing and entry. See also three-day cycle.

Processing Day (Day 2)

See 'Bacs cycle'.

Public Key Infrastructure (PKI)

A system to verify the validity of parties involved in electronic communications and to secure electronic data transmissions. PKI involves digital certificates, certificate authorities and other registration authorities. PKI security is used by Bacstel-IP. PKI uses two "keys"; a public and a private key. A message encrypted with a private key can only be decrypted with the associated public key (and vice versa).

Reference

The reference allocated by the Service Users to each individual DDI and Direct Debit. (See also 'Core Reference'.)

Refund Request

A claim made by a paying bank for a refund from the Service User that is not covered by the valid indemnity claim criteria. This would occur following an error on the part of the paying bank (the paying bank fails to action a Direct Debit cancellation and makes the payment).

Registered Name

The name of the company as registered at Companies House.

Registered Trading Name

A trading name registered at Bacs for use under the Direct Debit Scheme.

Re-presentation

A Direct Debit, that was returned to the Service User as unpaid, being resubmitted for collection.

The Scheme

The Direct Debit Scheme defined and described in this document.

Service Names

A generic name used by an organisation which describes the service offered. This name may differ from the Service User's registered name or trading name, e.g. 'Budget Plan'.

Service User

A company, group of companies, charity etc. that is sponsored to use one or more Bacs service.

Service User Number

A six-digit number allocated to a service user to uniquely identify it to Bacs.

Single Payment

A single payment can be defined as a Direct Debit, which will only be collected once.

Solution Suppliers

Third party companies or in-house sections that provide Bacstel-IP related software packages to facilitate the transmission of payment files from a service user to Bacs.

Sponsor

Any financial institution that can authorise service users to use Bacs. Also referred to as sponsoring bank.

Standing Order

A credit payment instruction as detailed in the standing order mandate.

ToDDaSO

Transfer of Direct Debit and Standing Orders (see Inter Bank Transfer of Direct Debits and Standing Orders).

Third Party Debt Order (Formally Garnishee Order)

An order of an English, Welsh or Northern Irish court addressed to a Bank to pay money from a debtors account to a judgement creditor in satisfaction of a judgement debt.

Three-day Cycle

The service offered by Bacs where the minimum time taken for the processing cycle is three processing days. Input, processing and entry occur on consecutive processing days. See also processing cycle.

Trading Name

A name under which a company conducts its business. This name may differ from the Service User's registered name.

Transaction Code

A two-character code used in each payment instruction, specifying the type of payment instruction (e.g. debit, credit, DDI).

United Kingdom (UK)

For the purpose of the Scheme, the United Kingdom (UK) comprises England, Wales, Scotland, Northern Ireland, the Channel Islands and the Isle of Man.

Unpaid Direct Debit

A Direct Debit that is returned to the Service User as the funds could not be collected from the destination account, e.g. insufficient funds, or no DDI set up on the account. See also automated return of unpaid Direct Debits.

Unpaid Direct Debit Reason Codes

A series of codes used to denote the reason for returning a Direct Debit unpaid either by automated means via Bacs (ARUDD) or by manual advice.

Variable Amount Instruction

A DDI which does not specify the amount to be debited. These are the only Instructions now acceptable.

Working Days

For the purposes of the Scheme, working days is defined as English Bank working days excluding Saturdays, Sundays and Bank Holidays.

Zero Account Number Advice Voucher

A paper advisory slip generated by Bacs and completed by the destination bank/building society to inform a Service User of the correct destination account number to use in the future. It is produced if a payment instruction fails validation of the destination account number and is in turn set to all zeros by Bacs.

APPENDIX 2: DIRECT DEBIT REASON CODES AND THEIR MEANING

The following tables for Unpaid Direct Debits, ADDACS and AUDDIS have been expanded to give additional information on how individual codes should be dealt with:

Unpaid Direct Debit reason codes

Unpaid Code	Reason	Circumstances	Special Instruction/ Information
0	Refer to Payer	A Payer's Bank is not in a position to pay the Direct Debit; (for some reason other than the exception below). OR The service of a Garnishee Order or Arrestment on the Payer's account, his bankruptcy, liquidation or appointment of receiver	Service User may represent up to one month from original processing day - it is recommended that the Payer is notified of this 5 working days in advance of the representation. Service User will need to establish from the Payer the reason for non-payment and likelihood of payment upon representation
1	Instruction cancelled	Instruction cancelled by Payer or his bank	Service User must liaise with Payer to agree the payment method for collection of any outstanding funds
2	Payer deceased		
3	Account transferred	Account transferred to a new Bank or Building Society	First check you have not been notified of the new Bank details, if not you must obtain a new DDI from the Payer. Collection must be suspended until a new DDI set up and Advance Notice is issued to the Payer
4	Advance Notice disputed	Payer disputes time, amount or frequency of Advance Notice and has requested single payment to be countermanded	Service User should not collect further Direct Debits until it has resolved the dispute with the Payer
5	No account (OR wrong account type)	Account Number is not recognised at the Paying Bank	Service User should check DDI information and/or liaise with Payer
6	No Instruction	No Instruction held with Paying Bank	Service User should check DDI information and/or liaise with Payer and if appropriate obtain new Instruction
7	Amount differs	Payer states the amount of the Direct Debit differs from the amount in any existing fixed Instruction or Advance Notice to Payer	Service User should not collect further Direct Debits until it has resolved the dispute with the Payer
8	Amount not yet due	Payer states date of debiting is in advance of the due date specified in any existing fixed DDI or Advance Notice to the Payer AUDDIS Service Users only - It is less than 5 working days since the DDI was lodged	Service User should not collect further Direct Debits until it has resolved the dispute with the Payer
9	Presentation overdue	Payer states date of presentation is more than 3 working days after due date on fixed DDI or Advance Notice to Payer OR Re-presentation of Unpaid Direct Debit is more than one month from original Direct Debit processing day	Service User must give further Advance Notice to the Payer before Direct Debit is collected
A	Service User differs	Identity of Service User differs from DDI	
B	Account closed	Payer has closed their account for an unknown reason	If the Direct Debit is to continue the Service User must obtain a new DDI for a different/new account

Direct Debit Instruction Amendments and Cancellations (ADDACS)

Code	Reason	Circumstances	Special Instruction/Information
0	Instruction cancelled - Refer to Payer	Paying Bank has cancelled Instruction	Service User cannot collect via Direct Debit on this account. If Direct Debit is to continue the Service User must obtain a new DDI for a new account
1	Instruction cancelled by Payer	Payer has instructed Paying Bank to cancel DDI	Service User must liaise with the Payer to agree the payment method for collection of any outstanding debts
2	Payer deceased		
3	Account transferred to a new Bank or Building Society	Account transferred to a new Bank or Building Society	If both old and new Bank details are quoted you will need to amend your records accordingly. AUDDIS Service Users only - A 0N must be sent to lodge the new instruction. If only the old Bank details are quoted first check you have been notified of new account details. If new account details have not been advised you must obtain a new DDI from the Payer. Collection must be suspended until a new DDI set up and Advance Notice issued to the Payer.
B	Account closed	Payer has closed their account for an unknown reason	If the Direct Debit is to continue the Service User must obtain a new DDI for a different/new account
C	Account transferred to a different branch of Bank/Building Society	New account details supplied to the Service User	Service User must apply change to data file and continue with Direct Debit collections AUDDIS Service Users only - An 0C/0N pair must not be sent on receipt of this message
D	Advance Notice disputed	Payer disputes time, amount or frequency of Advance Notice	Service User should not collect further Direct Debits until it has resolved the dispute with the Payer
E	Instruction amended	Paying Bank will advise amendment via ADDACS message	Service User should collect Direct Debits using new details AUDDIS Service Users only - An 0C/0N pair must not be sent on receipt of this message
R	Instruction re-instated	Paying Bank may re-instate a cancelled DDI up to two months from cancellation	Service User may resume direct debiting under the reinstated Instruction. However, a new DDI must be obtained and lodged if re-instatement is identified after the two month period

AUDDIS reason codes

Code	Reason	Circumstances	Special Instruction/ Information
1	Instruction cancelled by Payer	Payer has instructed Paying Bank to cancel DDI	Service User must liaise with Payer to agree the payment method for collection of any outstanding funds
2	Payer deceased		
3	Account transferred	Account transferred to another Bank/Building Society	First check you have not been notified of the new Bank details, if not you must obtain a new DDI from the Payer. Collection must be suspended until a new DDI set up and Advance Notice is issued to the Payer
5	No account	Account number is not recognised at the Paying Bank	Service User should check Direct Debit information and/or liaise with Payer
6	No Instruction	Does not exist on Paying Bank's database	Service User should check the DDI and/or liaise with Payer and send an 0N when resolved
B	Account closed	Payer has closed his account for an unknown reason	If the Direct Debit is to continue the Service User must obtain a new DDI for a different/new account
C	Account transferred to a different branch of the Bank/Building Society	New account details supplied to the Service User by Paying Bank	Service User should apply change to data file and continue with Direct Debit collections An 0C/0N pair must not be sent on receipt of this message
F	Invalid account type	Paying Bank does not allow Direct Debits on this type of account	Service User will need to obtain new account details from the Payer The Direct Debit cannot be applied
G	Bank will not accept Direct Debits on account	Paying Bank does not allow Direct Debits on this account	Service User must liaise with Payer and obtain a new DDI for a different/new account
H	Instruction has expired	Occurs when a Service User attempts to convert a DDI which is shown as expired on the Paying Bank's database	A 0N DDI will be required to re-activate this DDI if collections are to resume Service Users must ensure they have the Payer's authorisation to collect under expired Instruction
I	Payer Reference is not unique	Paying Bank has matched the DDI to an existing DDI with a similar reference that has more or fewer characters	Service User should allocate a different reference and lodge DDI, again using 0N
K	Instruction cancelled by Paying Bank	Paying Bank has cancelled the DDI	Service User cannot collect via Direct Debit on this account If Direct Debit is to continue the Service User must obtain a new DDI for a new account

Please note that the reasons quoted overleaf are AUDDIS reason codes used by Bacs only.

AUDDIS reason codes (continued)

Code	Reason	Circumstances	Special Instruction/ Information
L	Incorrect Payer's Account Details	Either: • the sort code / account number has failed the modulus check • the sort code does not exist • the account number is not all numeric or is all zeros • the account type is invalid.	Service User should undertake sort code validation and modulus checking prior to sending the DDI transactions to Bacs or, if already doing this, should ensure that they are using the latest version
M	Transaction Code / User Status incompatible	Transaction codes which are not allowed whilst in this status have been sent	Service User has sent '0S' DDI transactions after being given 'LIVE' status on the Bacs masters files. Service User should re-submit transactions with 0N as the transaction code
N	Transaction disallowed at Payer's branch	This code will be returned where paying banks have expressly disallowed the set-up of DDIs at the branch in field 1 of the transaction	Service User should refer back to their payer and obtain a DDI for a different/ new account
O	Invalid reference	The reference in field 10 of the DDI record does not comply with the AUDDIS rules	Service User should ensure that references meet the rules of the AUDDIS Service (see Appendix 3 of this document)
P	Payer's Name not present	Validation has detected field 11 is blank. A Payer's name should always be entered	Service User should correct the record and re-submit
Q	Service User's name blank	Validation has detected field 9 is blank. The Service User's company or trading name should always be entered	Service User should correct the record and re-submit

Reason Codes L to Q are only generated by Bacs and occur as a result of its validaton of DDI records

APPENDIX 3: AUDDIS CORE REFERENCE REQUIREMENTS
(FOR CORE REFERENCE TECHNICAL REQUIREMENTS SEE AUDDIS SERVICE DEFINITION ANNEX D)

This Appendix describes the criteria used for setting up the AUDDIS **core reference**. It is split into two sections with the first section giving information on the basic requirements for Service Users, followed by more detailed information on the technical requirements of Paying Banks in setting up Direct Debit Instruction (DDI) information. In addition it gives basic information on single versus multiple DDIs.

AUDDIS introduces standardised automated checks by Paying Banks to ensure that, for every DD received, they have a DDI set up on the customer's account containing a matching reference.

All AUDDIS Service Users must use core referencing and the reference must always be quoted in **field 10** of the DDI.

Core Reference Rules

- A core reference may be up to 18 characters long and must be a minimum of 6 characters

- Although any of the allowed **Bacs** characters may be included in the core reference*, only upper case alpha and numeric characters will be considered in checking for the minimum length of 6 characters

- It **must not** consist of all the same characters e.g. all zeros

- It **must be** left justified within field 10 of the Bacs DDI and debit record. This requires the first alpha/numeric character of the reference to appear in character position one of this field

- It **must be** lodged with the Paying Banks exactly as it appears on a signed DDI

- It **must be** unique for the sort code, account number and SUN to ensure that the Paying Banks can accurately match Direct Debits to DDIs. It must not be possible to match the core reference quoted in the DDI wholly or in part to the core reference of any other DDI already held by the Paying Bank for the same sort code, account number and SUN

*Other allowed characters are space, ampersand (&), hyphen, full stop and solidus (/).

Single versus multiple DDIs – advice on reference formatting

It is recognised that Service Users may have a number of different contracts with a particular customer and may therefore wish to collect several DDs from the same customer bank account. The guidelines are aimed to ensure that direct debiting proceeds at lowest cost and with minimum complexity for all parties involved.

There are two key issues i.e.

- whether the Payer has to sign one or several instructions and hence whether Paying Banks holds details of one or several DDIs; and

- whether the Service User amalgamates the various amounts due into a single DD.

1. Multiple DDIs signed by the Payer

The preferred approach is for Service Users to preserve a one-to-one relationship between DDIs signed by the Payer, DDIs sent to the Paying Banks and Direct Debits to be collected. It is recognised that Service Users may not generate their reference until after the Payer has signed the DDI. In these circumstances where the Payer has signed a DDI without a reference, multiple references may be used providing each DD reference is quoted clearly on the Advance Notice to the Payer detailing which amounts relate to which reference. These must then be lodged on individual '0N' transactions with the Paying Bank.

Using this one-to-one relationship allows Paying Banks to readily identify which DDI to cancel if the Payer wishes to cancel some but not all of his DDs.

Reference on the DDI signed by the Payer	Reference quoted in the '0N' transaction and held by the Paying Bank	References in the subsequent DDs
MC/1234AB - 1	MC/1234AB - 1	MC/1234AB - 1 JAN MC/1234AB - 1 FEB MC/1234AB - 1 MAR
MC/1234AB - 2	MC/1234AB - 2	MC/1234AB - 2 JAN MC/1234AB - 2 FEB MC/1234AB - 2 MAR
MC/1234AB - 3	MC/1234AB - 3	MC/1234AB - 3 APR MC/1234AB - 3 MAY MC/1234AB - 3 JUN

2. Single DDI signed by the Payer

The alternative approach is for the Payer to sign a single DDI against which the various DDs are collected. The optional element of the DD reference is used by the Service User to distinguish between the different contracts. This approach may be appropriate where there are many different contracts with a single Payer, a fleet of hire cars for instance.

Reference on the DDI signed by the Payer	Reference quoted in the '0N' transaction and held by the Paying Bank	References in the subsequent DDs
MC/1234AB	MC/1234AB	MC/1234AB - 1 JAN MC/1234AB - 1 FEB MC/1234AB - 2 JAN MC/1234AB - 2 FEB MC/1234AB - 3 APR MC/1234AB - 3 MAY

In using this approach, Service Users must accept the consequences of a Payer advising their Bank that they wish to cancel one of the contracts. As the Paying Bank only has details of the one DDI this is all the Bank can cancel even if the Payer only wants some of the contracts cancelled. In this circumstance, when the Service User receives the ADDACS cancellation report, it should contact the Payer to determine whether all contracts are to be cancelled or just some and where appropriate obtain and lodge a new DDI.

3. Alternative Single DDI method

A variation to the above approach is for the Service User to still have only a single master DDI signed by the Payer, but to advise the Paying Bank about each of the contracts by supplementing the reference with some additional differentiating information.

Reference on the DDI signed by the Payer	Reference quoted in the '0N' transaction and held by the Paying Bank	References in the subsequent DDs
MC/1234AB	MC/1234AB - 1	MC/1234AB - 1 JAN MC/1234AB - 1 FEB
	MC/1234AB - 2	MC/1234AB - 2 JAN MC/1234AB - 2 FEB
	MC/1234AB - 3	MC/1234AB - 3 APR MC/1234AB - 3 MAY

The advantage of this approach is that it allows better control in terms of the Payer being able to cancel individual components of the DDI. This approach may also be appropriate in circumstances when the Service User is not able to complete the reference until after the DDI has been signed by the Payer.

Amalgamation of Direct Debits

All Paying Banks strongly advise against the practice of amalgamating the DDs for different contracts into a single DD because of the problems that tend to occur when the Payer wishes to cancel some but not all of the amounts being paid. If Service Users insist on amalgamating several DDs, then the single DDI method previously described, should be used, so that there is still a one to one relationship between the DDI signed by the Payer, the DDI details held by the Paying Bank and the DD collected.