UK Domestic Rules

15 October 2015

Summary of Changes

This document reflects changes associated with recently published updates to the *UK Domestic Rules*. Rules for MasterCard, Debit MasterCard®, and Maestro® card programmes are included in this document.

Description of Change	Where to Look
Removed title pages for parts, and renamed chapters to better reflect applicability. For clarity, the document is now organized as follows: • Chapters 2-7 contain Rules applicable to MasterCard and Debit MasterCard • Chapters 8-12 contain Rules applicable to Maestro • Appendix A contains Compliance Zones applicable to MasterCard, Debit MasterCard, and Maestro	
As announced in *United Kingdom Operations Bulletin* No. 2, 15 July 2014, MasterCard will reduce the maximum number of declined authorizations on card-not-present transactions permitted in a 24 hour period to two (from four).	3.1.5 Multiple Authorisation Attempts on Card-Not-Present Transactions Multiple Authorisations 9.2 Multiple Authorisation Attempts on Card-Not-Present Transactions 11.2.1 Proper Use of Message Reason Code 4808
As announced in *United Kingdom Operations Bulletin* No. 3, 21 August 2014, all Expedited Billing Dispute Resolution Forms may be used for charging back UK domestic MasterCard transactions.	Removed Rule 6.0.2, so subsequent sections are renumbered

Description of Change	Where to Look
As announced in *United Kingdom Operations Bulletin* No. 5, 19 December 2014, MasterCard will extend the use of chargeback message reason code 4841 (Cancelled Recurring Transaction) in the United Kingdom.	Added new 3.5 Payday Loansfor MasterCard 9.13 Payday Loansfor Maestro Added additional use to chargeback message reason code 4841 in 6.1.4 Reason Code 4841 UK—Cancelled Recurring Transaction for MasterCard Added addtional use to chargeback message reason code 4841 in 11.4 Message Reason Code 4841—Cancelled Recurring Transactionfor Maestro. Modified 11.4.2 Proper Use for Acquirer's Second Presentment
As announced in *United Kingdom Operations Bulletin* No. 2, 2 February 2015, to encourage merchants and acquirers to reduce fraudulent transactions and other chargeback reasons, MasterCard is removing the minimum chargeback amount of GBP 10 that is currently applicable in the United Kingdom for certain reason codes.	Removed 6.0.1 Minimum Chargeback Amount; subsequent sections are renumbered In 6.1.6 Reason Code 4855 UK—Goods or Services Not Provided, removed GBP 10 minimum value

Contents

Chapter 1 Introduction

This section describes the use and applicability of this manual.

1.0 Applicability of the UK Domestic Rules

The *UK Domestic Rules* describes specific rules that are applicable to domestic transactions, in addition to the international rules.

Domestic transactions are defined as transactions that take place at a card acceptor located in the United Kingdom (UK) with a UK-issued card. For the purposes of these rules, the UK is defined as consisting of Great Britain, Northern Ireland, the Channel Islands, and the Isle of Man.

A card is issued in the UK if the BIN on the card has been allocated to the issuer in respect of its license for the United Kingdom.

Domestic transactions are subject to the international rules, except where there is a specific domestic rule that varies the international rule.

The domestic rules are contained in:

- This manual, which is organized as follows:
  - Rules applicable to MasterCard and Debit MasterCard appear in chapters 2–7.
  - Rules applicable to Maestro appear in chapters 8–12. These chapters do not apply to ATM transactions.
  - Compliance zones appear in Appendix A of this document.
- *MasterCard Rules*
- *Transaction Processing Rules*
- MasterCard Bulletins, or
- Other notifications to Customers.

The domestic rules are mandatory and enforceable for all domestic transactions in the UK.

Chapter 2 MasterCard and Debit MasterCard Card Requirements

This section describes card requirements.

2.1 Contactless Functionality—Debit MasterCard

All newly issued or re-issued Debit MasterCard cards must support contactless functionality and be enabled for contactless purchases.

This requirement does not apply to prepaid Debit MasterCard cards.

2.2 Limitation of Liability of Cardholders for Unauthorised Use—Debit MasterCard

The following rule variation for lost and stolen fraud applies in addition to the rules published in chapter 12 (Europe Region) of the *MasterCard Rules*.

The issuer must ensure that the cardholder's liability is zero for lost and stolen fraud occurring prior to the time of notification by the cardholder to the issuer of the loss or theft of the card, provided that the following conditions are met:

1. The cardholder has exercised vigilant care in safeguarding the card from risk of loss, theft, or unauthorised use;
2. The cardholder immediately and without delay notifies the issuer upon discovery of the loss, theft, or unauthorised use;
3. The cardholder has not reported two or more incidents of unauthorised use to the issuer in the immediately preceding 12-month period;
4. The account to which the transactions are posted is in good standing; and
5. The cardholder has complied with the terms and conditions of the corresponding cardholder agreement.

The above conditions do not apply for the cardholder to benefit from zero liability with respect to fraud types other than lost and stolen fraud, or with respect to lost and stolen fraud occurring after the cardholder has notified the issuer of the loss or theft of the card. For the rules applicable in these cases, refer to chapter 12 (Europe Region) of the *MasterCard Rules*. Except as specifically varied above, the Europe Region rules on limited cardholder liability apply in the United Kingdom.

This rule variation does not apply to prepaid Debit MasterCard cards, which are covered by the Europe Region rules.

Chapter 3 MasterCard and Debit MasterCard Acceptance Requirements

This section describes acceptance requirements when processing domestic MasterCard and Debit MasterCard transactions.

3.1 Purchases

3.1.1 CVM Fallback

CVM fallback is not permitted.

3.1.2 Cardholder Activated Terminal Requirements

Merchants may deploy unattended terminals provided that the terminals comply with the requirements set out in the international rules, supplemented by the requirements below.

A Cardholder Activated Terminal (CAT) that is not chip-capable must comply with the requirements for a CAT level 2 terminal.

A hybrid CAT that is capable of reading the chip on the card and verifying the cardholder's PIN offline is a dual capability CAT as described Appendix D of the *Transaction Processing Rules*.

CAT level 3 terminals that are chip-capable or non–chip-capable may be deployed and must comply with the international rules.

3.1.2.1 CAT Level 2 Terminals (No Chip Capability)

CAT Level 2 terminals must:

1. In the case of Automated Fuel Dispensers, the preauthorisation request may be for GBP 1 as the full transaction amount will not be known at the outset. Alternatively, a preauthorisation request for a pre-determined maximum amount may be submitted, followed by an advice message. Refer to the *Transaction Processing Rules*, (Chapter 4, Card-Present Transactions, Europe Region, Automated Fuel Dispenser Transactions) for the procedure to be followed in this case. Issuers must be able to receive preauthorisation requests for any amount, as well as advice messages, and must be able to send advice acknowledgements
2. Have a card capture facility that will be activated on receipt of a pick-up request from the issuer.
3. Be configured to issue a transaction receipt to the cardholder, with a truncated Primary Account Number (PAN).
4. Be configured so that the transaction amount is limited to a maximum value, dependent upon the applicable Merchant Category, as described in the table below.

Maximum Transaction Amounts at CAT Level 2 Terminals

MCC	Merchant Category	Maximum Transaction Amount (GBP)
30xx–32xx	Airlines with Specific Merchant Category Codes	300
35xx–37xx	Hotels with Specific Merchant Category Codes	600

MCC	Merchant Category	Maximum Transaction Amount (GBP)
4111	Ferries	300
4112	Passenger Railways	300
4131	Bus Lines	300
4511	Air Carriers, Airlines–not elsewhere classified	300
5542	Automated Fuel Dispensers	40 (if preauthorisation is for GBP 1)
6300	Travel Insurance	400
7011	Lodging–Hotels, Motels, Resorts-not elsewhere classified	600
7523	Car Parks	130
7832	Motion Picture Theatres	300
7922	Theatrical Producers (except Motion Pictures), Ticket Agencies	300
-	Other Categories	100

Magnetic stripe reading telephones (MCC 4814) may be deployed and must comply with the international rules.

Counterfeit card transactions at CAT Level 2 Terminals can be charged back by the issuer using Reason Code 4837 – Please refer to Section 6.1.3 for more information on Reason Code 4837.

3.1.2.2 Dual Capability Cardholder Activated Terminals

Dual Capability CATs must:

1. Have a single card slot for chip cards and non-chip cards, if the CAT accepts both types of card;
2. Support offline PIN and 'No CVM' as the CVM options for chip transactions;
3. Process a transaction involving a non-chip card as a CAT 2 magnetic stripe transaction;
4. Process a transaction involving a chip card without offline PIN verification as a CAT 2 chip transaction;
5. Process a transaction involving a chip card with offline PIN verification as a CAT 1 chip transaction;
6. In the case of Automated Fuel Dispensers, the preauthorisation request may be for GBP 1. Alternatively, a preauthorisation request for a pre-determined maximum amount may be submitted, followed by an advice message. Refer to the *Transaction Processing Rules*, (Chapter 4, Card-Present Transactions, Europe Region, Automated Fuel Dispenser

Transactions) for the procedure to be followed in this case. Issuers must be able to receive preauthorisation requests for any amount, as well as advice messages, and must be able to send advice acknowledgements.

7. In the case of Automated Fuel Dispensers, the Maximum Transaction Amount is GBP 100 if the preauthorisation is for GBP 1. The terminal must advise the cardholder of the Maximum Transaction Amount, prior to the PIN being entered, if the preauthorisation is for GBP 1, and the terminal must not allow a transaction for a value greater than the Maximum Transaction Amount. If a preauthorisation of a pre-determined maximum amount is submitted, the terminal must advise the cardholder of this amount, before the PIN is entered.
8. Be configured to issue a transaction receipt to the cardholder, with a truncated PAN.

3.1.2.3 Retained Cards

Cards retained by a CAT must be removed from the device within 24 hours and held within a secure environment in accordance with UK Industry guidelines and international Rules.

The CAT must not mutilate retained cards.

3.1.2.4 Restrictions on Use of CAT Level 2 Terminals

CAT Level 2 Terminals must not be used to dispense cash or foreign currency.

3.1.3 Mobile Phone Airtime Pre-Payment Transactions

3.1.3.1 Overview

The regulations in this subsection apply to purchases of pre-paid mobile phone airtime in 'Card Not Present' environments.

3.1.3.2 Acquirer Responsibilities

A MasterCard card or Debit MasterCard card can only be used for a Card Not Present transaction to purchase prepaid mobile phone airtime if the card has been previously registered with the merchant for this purpose.

3.1.3.3 Card Registration Restrictions

The acquirer must require that its merchants apply the following card registration restrictions.

1. No more than two cards can be registered for use on any mobile phone account with the merchant.
2. A card must not be registered for use on more than two mobile phone accounts with the merchant.

The acquirer must also require that its merchants, when registering a card, obtain the cardholder's name and home address and record them against the card's PAN on the register.

3.1.3.4 Transaction Restrictions

All prepaid mobile phone airtime transactions must adhere to the following restrictions.

1. All Transactions must

   a. Be authorised by the card issuer
   b. Be processed by the acquirer using Merchant Category Code 4814

   If a prepaid mobile phone airtime transaction is charged back as a result of fraudulent use, the acquirer must require that the merchant:

a. Immediately bar the mobile phone accounts for which the fraudulent payment was made, thus preventing further calls.
b. Deactivate the card for use on existing mobile phone accounts
c. Does not permit the compromised card to be registered for use on any other mobile phone account

2. Recurring Transactions

For recurring transactions, the following additional requirements apply:

a. The recurring transaction indicator must be used
b. The minimum transaction amount will be GBP 10, with a maximum transaction value of GBP 50
c. The acquirer must require that

i. The cardholder and card used have been registered with the merchant for at least 3 months; and
ii. The merchant has carried out transactions on the card where matching CVC 2 and AVS checks have been carried out.

NOTE: When the initial transaction is fully authenticated by MasterCard SecureCode, the requirement outlined in 2c, above, is waived, except for the AVS check which is retained as a best practice.

3.1.4 Contactless Transit Split Clearing

For the rules applicable to post-authorised aggregated contactless transit transactions refer to the *Transaction Processing Rules* (Chapter 4, Card-Present Transactions, MasterCard Contactless Transactions, MasterCard Contactless Transit Aggregated Transactions).

An authorised aggregated split clearing transaction occurs when all of the below conditions are met:

- The contactless enabled card or device must indicate that an M/Chip profile is supported.
- Tag 5F28 (Issuer Country Code) must have a value of 826.
- The denominated primary currency is GBP.
- The transaction is properly identified as defined in Appendix C of the *Transaction Processing Rules*.

3.1.4.1 First Authorisation Request

A transit card acceptor performing an authorised aggregated split clearing transaction may submit one or more First Presentment/1240 messages.

Each First Presentment/1240 message may combine one or more taps associated with one Authorisation Request/0100 message subject to all of the following:

- The first Authorisation Request/0100 message occurring in a 14 day period or immediately following a declined transaction must be for GBP 0.10.
- Offline Card Authentication (CAM) must be successful.
- The card acceptor must obtain authorisation of the transaction from the issuer.

- The combined amount of all First Presentment/1240 messages submitted against an Authorisation ID Response (DE 38) must be equal to or less than the chargeback protection amount as published in the *Chargeback Guide*, (Appendix C, CVM Limit and Contactless Ceiling Limit).
- The maximum time period from the first tap until the final First Presentment/1240 message is generated must be 14 calendar days.

3.1.4.2 Second and Subsequent Authorisation Requests

In addition to section 3.1.4.1 above:

- An Authorisation Request/0100 message occurring within 14 days of an Authorisation Response/0110 message reflecting an issuer's approval (without an intervening declined Authorisation Request/0100 message) must be for an amount other than GBP 0.10.
- The card acceptor must obtain authorisation from the issuer.
- The combined amount of all First Presentment/1240 messages submitted against an Authorisation ID Response (DE 38) must be equal to or less than the approved transaction amount plus the chargeback protection amount as published in the *Chargeback Guide*, (Appendix C, CVM Limit and Contactless Ceiling Limit Amounts).
- The maximum time period from the first tap (which resulted in the generation of the Authorisation Request/0100 message) until the final First Presentment/1240 message that is associated with said authorisation is 14 calendar days.

3.1.4.3 Declined Authorisation Request

If an issuer declines an authorisation request, the transit card acceptor may do one of the following:

3.1.4.3.1 Submit a First Presentment/1240 Message for GBP 6 or Less

When the issuer declines an authorisation request, the transit card acceptor may submit a First Presentment/1240 message within 48 hours of the decline response if all of the following conditions are met:

- The transaction amount in the Authorisation Request/0100 message was one of the following:
  - GBP 0.10
  - equal to or less than GBP 6
- The transaction was not effected with a commercial card as identified in DE 63 (Network Data) subfield 1 (Financial Network Code) of the Authorisation Request Response/0110 message.
- The previous Authorisation Request/0100 message on the same account was approved, or this was the first transit Authorisation Request/0100 message submitted by the transit card acceptor.

3.1.4.3.2 Submit a First Presentment/1240 Message for More than GBP 6

When the issuer declines an authorisation request, the transit card acceptor may continue to seek issuer approval for the declined amount.

The transit card acceptor may submit an Authorisation Request/0100 message a maximum of three times within thirty days of the initial decline response if both of the following conditions are met:

- The transaction amount is greater than GBP 6
- The Authorisation Request/0100 message must be coded as a key-entered transaction, not a contactless transaction.

3.1.4.4 Cardholder Request for Transaction Information

Upon the cardholder's request, the transit card acceptor must provide a list of the taps that were combined into a First Presentment/1240 message.

3.1.4.5 Substitute Draft for Contactless Transit Split Clearing

The requirements in the *Chargeback Guide* for a substitute draft for other contactless Transit transactions also apply for contactless Transit split clearing transactions.

3.1.5 Multiple Authorisation Attempts on Card-Not-Present Transactions

On Card-not-present Transactions, a Merchant is permitted a maximum of two declined authorisation attempts per calendar day on the same PAN. All authorisation attempts on the same PAN will count toward the maximum, regardless of the amount for which authorisation is requested.

The maximum applies per Merchant, regardless of the number of acquirers, Merchant names or Merchant IDs that the Merchant may have.

3.2 Face-to-Face Cash Advance Transactions

3.2.1 Cardholder Verification

CVM fallback is not permitted.

For all cash advance transactions, including those where the cardholder's PIN is checked, a personal identification of the cardholder must be requested and the normal procedures followed as set out in the rules.

It is not necessary for the address of the cardholder to be written on the face of the cash disbursement slip for face-to-face cash advance transactions.

3.3 Unique Transactions

3.3.1 Quasi-Cash Transactions

For all quasi-cash transactions in a face-to-face environment, including those where the cardholder's PIN is checked, a personal identification of the cardholder must be requested and the normal procedures followed, as set out in the rules.

It is not necessary for the address of the cardholder to be written on the face of the transaction receipt for face-to-face cash advance transactions.

3.4 Sales of Foreign Currency

MCC 6010 may be used only for face-to-face disbursements of sterling banknotes.

Sales of foreign currency notes, travelers cheques or other financial instruments denominated in foreign currency, whether carried out by a MasterCard licensee or by one of its authorised agents, must not be identified with MCC 6010.

3.5 Payday Loans

A chargeback right is available under reason code 4841 when the cardholder disputes any of the following fees related to payday loans (including payday loan brokers or other payday loan service providers):

- Fees or penalties associated with the agreement or the repayment; or
- Fees or penalties associated with a broker or other service.

This chargeback right is available for both recurring and non-recurring transactions related to payday loans.

Chapter 4 MasterCard and Debit MasterCard Processes and Fees

This section provides information about processes, documentation, and fees.

4.1 Expiry Date Checking by Issuers

4.1.1 Recurring Transactions

If on the Authorisation Request/0100 message, the recurring transaction indicator is set or the Merchant Category Code (MCC) is 5968 (Direct Marketing—Continuity/Subscription Merchants), the issuer must not check the expiry date and cannot decline the transaction for the reason that the expiry date quoted in the authorisation message is incorrect, or that the expiry date is missing from the message.

4.1.2 Non-Recurring Transactions

The issuer must verify the card expiry date on all authorisation requests by checking against the Cardholder Master File, with the exception of 'Recurring Transactions' as described in the above section.

In the event of a mismatch in the expiry date details, the issuer may either:

- Respond with a referral

OR

- Decline the transaction

4.2 Card Verification Code 2 (CVC2)

4.2.1 CVC2 at Bank-Owned Terminals

UK acquirers must ensure that merchants collect and transmit a CVC2 value on all card not present transactions at bank-owned terminals with the exception of properly processed no-show transactions, car rental addendum transactions, refunds and other similar transactions.

4.3 Address Verification Service

Acquirer and issuer participation in the Address Verification Service (AVS) is mandated for Card Not Present (CNP) domestic transactions.

4.3.1 Acquirer Requirements for AVS

Acquirers must register for AVS processing and meet the following requirements:

- They must transmit address information, when provided by their merchant, to the issuer in the Authorisation Request/0100 message for CNP domestic transactions;
- They must be able to receive the AVS response data from the issuer contained in the Authorisation Request Response/0110 message.

4.3.2 Issuer Requirements for AVS

Issuers must register for AVS processing and meet the following requirements:

- They must be able to verify AVS data contained in the Authorisation Request/0100 message for CNP domestic transactions,
- They must transmit a valid AVS response code to the acquirer in the Authorisation Request Response/0110 message.

With respect to newly assigned ICAs and BINs, an issuer is allowed six months from the date of assignment to come into compliance with this requirement.

Issuers that fail to register for AVS processing, or that do not provide a valid response code to acquirers, will not be eligible to charge back applicable transactions, using chargeback Reason Code 4837– No Cardholder Authorisation, where AVS data was provided by the acquirer.

4.3.3 AVS Response Codes

The following table describes the possible responses that an acquirer may receive to a request for an AVS check:

Response Code	Description
A	Address matches, postal code does not
N	Neither address nor postal code match
R	Retry–system unable to process
S	AVS currently not supported
U	No data from issuer/authorisation system
W	Postal code matches/address does not
X	Postal code and address match

4.4 Issuer's Right to Request a Transaction Information Document

Retrieval requests are not permitted where the clearing record (DE 055) shows that the transaction was a chip transaction verified by use of the cardholder's PIN.

4.5 Procedure for Correcting Duplicate or Erroneous Clearing Files or Batches

4.5.1 Notification to MasterCard

The submitting customer must inform Customer Operations Services, within **one working day** of becoming aware, that duplicate or erroneous clearing files or batches have been submitted to the Global Clearing Management System (GCMS).

This can be done via the telephone, followed immediately by fax or email confirmation of the incident.

The following information must be provided to identify the file or batch:

- The outgoing file ID (or GIDN) of the original file **and** the duplicate file;
- The processing class of the duplicate or erroneous batches;
- Any additional information to uniquely identify the file or batch.

4.5.2 Appointment of Incident Manager

The submitting customer must appoint an Incident Manager who can answer questions from MasterCard and/or the recipients of the data, until the incident has been resolved.

MasterCard will also appoint an Incident Manager who will use the information submitted by the customer provided in 4.5.1 to assess the impact of the incident.

4.5.3 Member Notification

MasterCard will inform affected customers within 1 working day of being notified of a duplicated or erroneous clearing file or batch being submitted to GCMS.

If all customers must be advised, MasterCard will send an *Operations Alert*, otherwise, individual faxes will be sent to each affected customer.

4.5.4 Duplication Generated by an Acquirer

If an acquirer generates a duplication of a clearing file or batch, correcting entries must be processed by the end of the third working day following the day that notification of the duplication was sent to MasterCard.

4.5.5 Duplication Generated by a Merchant

If a duplication is generated by a merchant, the acquirer is expected to use its best endeavours to resolve the situation as soon as possible and must advise MasterCard of the resolution date for communication to affected issuers.

The acquirer must advise MasterCard of the File IDs and the date when corrective action will be taken.

Customer Operations Services will forward this information to affected issuers.

The acquirer must then submit to MasterCard the correcting transactions on the date previously advised.

4.5.6 Penalties

Acquirers submitting duplicate or erroneous files into the Clearing System may be required to pay 0.50 GBP to affected issuers for every transaction on the duplicate or erroneous file payable after the incident has been fully rectified.

The fine will be paid to the issuers via Miscellaneous Fee records, with the legend 'File Duplication Fee', at a time agreed between the acquirer's Incident Manager and a representative of the issuer.

Refer to the *Chargeback Guide* in case of a dispute relating to Miscellaneous Fee Collection.

4.6 Automatic Billing Updater Programme and Recurring Payments Cancellation Service

4.6.1 Acquirers

Acquirers must participate in the MasterCard Automatic Billing Updater programme by completing the Member Enrollment Form available on MasterCard Connect™.

Acquirers must be able to send, receive and process ABU data.

Acquirers must ensure that their acquiring host processing system incorporates ABU functionality.

Acquirers are required to register their UK Recurring Payment merchants in the ABU programme.

Acquirers must submit card account number queries to the ABU programme on behalf of their Recurring Payment merchants before authorisation.

Acquirers must take appropriate action to inform merchants of the response code received from the ABU programme to support account validation as outlined in the *ABU Reference Guide* available on MasterCard Connect™.

Acquirers must participate in the Account Validation Service.

Acquirers have the option to submit brand flips to/from any competitor scheme to the ABU programme on behalf of their recurring payment merchants.

Acquirers must ensure that merchants correctly flag recurring transactions.

Acquirers must submit account inquiry updates on behalf of those merchants enrolled at a minimum of once every 180 days.

4.6.2 Issuers

Issuers must participate in the MasterCard Automatic Billing Updater programme by completing the Member Enrollment Form available on MasterCard Connect™. With respect to

newly assigned ICAs and BINs, an issuer is allowed six months from the date of assignment to come into compliance with this requirement.

Issuers must be able to send, receive and process ABU data. Issuers must maintain their entire active card portfolio in ABU and communicate all account changes via the ABU programme.

To support the Account Validation process Issuers must report new accounts and provide a one-time upload plus 6 months of historic data changes up to a maximum of 40 months data to the Issuer Account Change Database.

Account changes are classified as:

- New Accounts opened
- Account changes (BIN changes, upgrades, lost, stolen)
- Expired Account
- Closed Accounts
- Portfolio Acquisitions (MasterCard to MasterCard)
- Brand Flips from any competitor scheme to MasterCard (Optional)

Issuers must enroll and participate in the Recurring Payments Cancellation Service by either submitting the RPCS enrollment form or using the online RPCS enrollment process available on MasterCard Connect™.

With respect to newly assigned ICAs and BINs, an issuer is allowed six months from the date of assignment to come into compliance with this requirement.

4.6.3 Documentation Location

The ABU and RPCS documentation set can be found by following these steps:

1. Go to **www.mastercardconnect.com**.
2. Enter your **User ID** and **Password**.
3. Under **Library**, select **References**.
4. Select **Products & Services**, and then click **Recurring Payments**.
5. Select **Automatic Billing Updater** or **Recurring Payment Cancellation Service**.

4.6.4 Exemptions from the Requirement to Support Automatic Billing Updater (ABU)

Prepaid programmes are exempt from ABU reporting requirements, provided that the issuer does not allow the prepaid cards to be used to enter into recurring payment arrangements.

This exemption applies to both consumer and corporate prepaid programmes.

Single-use-only virtual account numbers are exempt from ABU reporting requirements.

4.7 Issuer Response on Recurring Transactions

If the Recurring Transaction indicator is set in the Authorisation Request/0100 message, the issuer must not generate a referral but needs to respond with either an 'approve' or with a 'decline'.

4.8 Merchant Rewards

An acquirer must pay a merchant who recovers a card an amount of 50 GBP. The amount paid to the merchant should be net of any tax payable on the reward.

For each card recovered in this way by a merchant, the acquirer has the right to charge the issuer for reimbursement of the reward paid for making the recovery, including the tax paid on the reward, together with a handling fee of 10 GBP, using the Fee Collection/1740 message.

NOTE: Please refer to the *IPM Clearing Formats* for information about completing the Fee Collection/1740 message.

Chapter 5 MasterCard and Debit MasterCard Settlement

This section provides information on settlement services and timeframes.

5.1 Domestic Settlement Service

Unless otherwise agreed between the Customers involved, all domestic transactions must be submitted to the Global Clearing Management System (GCMS) for clearing and settlement.

5.1.1 Settlement Timeframes

Transactions on cards that have sterling as the cardholder billing currency, which are submitted to GCMS for settlement in sterling and received by MasterCard by the clearing cut-off deadline, will be settled on the same day.

In order to ensure same-day settlement, issuers and acquirers must participate in the UK GBP Sterling Intra-currency Settlement Service (EU00082601) for all ICAs assigned for use in the UK. As an exception to this rule, issuers are not required to participate in the UK GBP Sterling Intra-currency Settlement Service for any ICA that has no GBP-denominated BINs.

Chapter 6 MasterCard and Debit MasterCard Chargeback Rules

This section describes chargeback rule variations for domestic transactions.

6.0 Introduction

Specific domestic rules apply to the following chargeback reason codes:

- 4808—Requested/Required Authorisation Not Obtained
- 4837—No Cardholder Authorisation
- 4841—Cancelled Recurring Transaction
- 4855—Goods or Services Not Provided
- 4860—Credit Not Processed
- 4863—Cardholder Does Not Recognise – Potential Fraud

For the above reason codes the domestic rule is a variance to part, or parts, of the international rule.

Detailed procedures for processing chargebacks are documented in the *Chargeback Guide*.

6.0.1 Cardholder Declarations

The issuer must ensure that the Cardholder's identity (for example, as stated on the original card) appears legibly on any cardholder declaration that is submitted in support of a cardholder dispute, unless these details appear elsewhere on other documentation submitted with the cardholder declaration.

6.0.2 Chargeback Time Frame for Cardholder Disputes on "Open-Ended" Contracts

The chargeback time frame for cardholder disputes is 120 days from the latest expected delivery date of the goods or services. **Effective for transactions processed on or after 17 October 2014**, for "open-ended" contracts which do not have a latest expected delivery date, the contract will be considered to be valid for 12 months from the transaction processing date. The chargeback reason codes affected by this change are:

- 4853—Cardholder Dispute—Defective/Not as Described
- 4855—Goods or Services not Provided

This extension of chargeback time frame only applies to situations where the merchant is still trading on the date of the first chargeback. The cardholder letter must stipulate that the contract is "open-ended" and the cardholder must have contacted or attempted to contact the merchant to resolve the dispute. The cardholder must specify how he attempted to contact the merchant and the result of that contact.

The chargeback time frame for undated vouchers or gift cards is unchanged and follows the global time frame which is 120 days from the date the cardholder attempts to use the voucher or gift card.

6.1 Specific Domestic Chargeback Rules

6.1.1 Reason Code 4808 UK—Requested/Required Authorisation Not Obtained

The issuer may use this reason code to charge back all non-chip-read transactions completed without authorisation, including non-face-to-face transactions, regardless of the transaction amount.

The following variances to the *Chargeback Guide* apply for domestic transactions.

A. Proper Use of Message Reason Code 4808

In addition, the issuer cannot chargeback under this reason code if the actual transaction amount does not exceed the authorised amount by more than 15 percent for transactions with MCC 5411 (supermarkets).

CAT Level 1 AFD Terminals
The issuer may not chargeback a transaction processed at a CAT level 1 fuel dispenser card acceptor for any amount less than or equal to GBP 100 if the transaction was identified in the authorisation request with MCC 5542 and CAT level 1, and authorised by the issuer for 1 GBP.

If the preauthorisation request was for GBP 1 and the transaction amount exceeds GBP 100, the issuer may chargeback only the difference between the transaction amount and the implied authorised amount of GBP 100.

CAT Level 2 AFD Terminals
The Issuer may not chargeback a transaction processed at a CAT level 2 fuel dispenser card acceptor for any amount less than or equal to 40 GBP if the transaction was identified in the authorisation request with MCC 5542 and CAT level 2, and authorised by the issuer for 1 GBP.

If the preauthorisation request was for GBP, and the transaction amount exceeds GBP 40, the issuer may chargeback only the difference between the transaction amount and the implied authorised amount of GBP 40.

For the chargeback rules applicable when a partial approval was given for a CAT Level 1 or CAT level 2 AFD transaction, refer to chapter 3 of the *Chargeback Guide*. When a partial approval is given, the amount for which preauthorisation is requested does not determine the level of chargeback protection; the issuer may chargeback any amount in excess of the partial approval amount.

Contactless Transit Split Clearing
The issuer cannot charge back a properly identified Contactless Transit Split Clearing transaction as a transit card acceptor, if:

- The sum of all First Presentment/1240 message amounts associated with the same authorisation is equal to or less than the sum of the approved transaction amount plus the chargeback protection amount
- The issuer approved the transaction and
- The maximum time period from the first tap until the final First Presentment/1240 message is generated was 14 calendar days or less.

If the sum of all First Presentment/1240 message amounts associated with the same authorisation exceeds the sum of the approved transaction amount plus the chargeback protection amount, then the issuer may charge back only the difference between these two sums.

In addition, the issuer may not charge back if:

- The issuer declined the authorisation request and
- The transaction amount is GBP 6 or less and
- The transaction was effected with a card that is not a commercial card as identified in DE 63 (Network Data) subfield 1 (Financial Network Code) of the Authorisation Request Response/0110 message Transactions above this amount may be charged back for the full amount. If the issuer declined the authorisation request and the transaction amount is more than GBP 6, the issuer may charge back the full transaction amount.

Multiple Authorisations
The issuer may charge back under this reason code if a card-not-present transaction was approved in Stand-In following two declined authorisation attempts on the same PAN by the same merchant on the same calendar day.

Time Frame	Retrieval Request	Supporting Documents	Data Record
90 Days	No	None	Multiple authorisation requests

B. Proper Use for Acquirer's Second Presentment
The acquirer may second present with the following information as proof of voice authorisation by the issuer:

Voice Authorisation

1. Card number
2. Expiry date
3. Transaction amount
4. Transaction date and time
5. Merchant number
6. MCC
7. Authorisation code
8. Whether or not CVC 2 was checked
9. Questions asked and answers supplied
10. Issuer Operator ID

Multiple Authorisations
The acquirer may second present if the transaction was authorised by the issuer and not in Stand-In, or if authorisation was obtained after fewer than two declined authorisation attempts on the same PAN by the same merchant in the same calendar day.

Second Presentment Conditions	Supporting Documents	Data Record
The transaction was authorised by the issuer, or was authorised after fewer than two declined authorisation attempts	None	"Issuer authorised" or "Fewer than 2 declined authorisation attempts"

C. Arbitration Chargeback
The issuer may raise an arbitration chargeback if the proof of voice authorisation provided by the acquirer does not match what the issuer has on file.

The issuer must supply the information showing the non-match.

6.1.3 Reason Code 4837 UK—No Cardholder Authorisation

The following variances/additional requirements to the *Chargeback Guide* apply for domestic transactions:

A. Proper Use of Message Reason Code 4837

The issuer may also use this chargeback reason code for counterfeit card magnetic stripe transactions that occurred at a CAT Level 2 terminal, provided that:

1. The cardholder states in writing that neither he/she, nor anyone authorised by him/her, engaged in the transaction, and
2. The issuer blocks the account number on their host, until card expiration, on or before the Central Site Processing Date of the first chargeback relating to the counterfeit card.

In addition, for counterfeit card transactions authorised in Stand-In, the issuer must have blocked the account number on it host and list the account number on the MasterCard Account File with a capture card response until expiration.

The issuer may not use this chargeback reason code for the following types of transactions:

- Card Not Present transactions where the acquirer transmitted AVS data in the Authorisation Request/0100 message in accordance with requirements, and the issuer is not registered for AVS processing;
- Card Not Present transactions where the acquirer transmitted AVS data in the Authorisation Request/0100 message in accordance with requirements, and the issuer did not respond in the Authorisation Request Response/0110 message in DE 48 using one of the indicators provided in section 4.3.3;

- Card Not Present transactions where the acquirer transmitted CVC 2 data in the Authorisation Request/0100 message in accordance with requirements, and the issuer is not registered for CVC 2 processing;
- Card Not Present transactions where the acquirer transmitted CVC 2 data in the Authorisation Request/0100 message in accordance with requirements, and the issuer did not respond in the Authorisation Request Response/0110 message in DE 48 using the following indicators: **M** = CVC 2 Match.
- For transactions authorised by the issuer following a referral request correctly fulfilled by the acquirer and where the issuer had issued a referral request in response to an authorisation request, processed in the preceding hour that showed that the transaction had been originally captured electronically at the merchant location.

B. Proper Use for Acquirer's Second Presentment

Second Presentment Condition	Supporting Documents	Data Record
The acquirer, who must be registered for AVS processing, can demonstrate that the issuer is not registered for AVS processing or did not respond in accordance with AVS processing requirements in respect of a CNP transaction.	Authorisation log reflecting an AVS response code of **S** or **U** or blank in DE 48 (Additional Date), PDS 83 of the Authorisation Request Response/0110 message.	NONE
The acquirer can demonstrate that the issuer did not respond in accordance with CVC2 processing requirements in respect of CNP transactions	Authorisation log reflecting a CVC 2 response code other than **M** in DE 48, PDS 87 of the Authorisation Request Response/ 0110 message.	NONE
The acquirer can substantiate that the passenger name on the airline ticket matches the valid cardholder name.	A copy of the ticket showing the same name as on the cardholder declaration.	Airline Ticket

C. Arbitration Chargeback

In respect of a dispute regarding the purchase of an airline ticket, the issuer must provide a progressive letter from the cardholder, dated after the second presentment, to re-confirm the cardholder's dispute.

For example, although the passenger name is the same as the cardholder, he/she did not make the transaction, nor took the flight.

Arbitration Chargeback Details	Supporting Documents
For airline transactions, the issuer can provide progressive documentation refuting the merchant documentation.	Progressive cardholder letter dated after the second presentment confirming that the cardholder did not purchase the ticket or take the flight.

6.1.4 Reason Code 4841 UK—Cancelled Recurring Transaction

The following variances/additional requirements to the *Chargeback Guide* apply for domestic transactions:

A. Proper Use of Message Reason Code 4841

Time Frame	Retrieval Request	Supporting Documents	Data Record
14 calendar days	No	None	CARDHOLDER DECEASED or ACCOUNT CLOSED or FACILITIES WITHDRAWN, or CARDHOLDER WITHDREW AUTHORITY, as appropriate.

In the event that:

1. The cardholder is deceased
2. The issuer or the cardholder has withdrawn or closed the account facilities
3. The cardholder withdrew his or her authority to bill a recurring transaction, regardless of any merchant Terms and Conditions

The issuer can initiate a chargeback, **within 14 calendar days** of the Transaction Processing Date, *without* having previously notified the merchant of cancellation.

No supporting documentation is required, but the issuer must identify the reason for the chargeback using appropriate text in the Data Record.

Beyond the 14-calendar day time frame, the standard international chargeback rule applies, including time frame and documentation requirements.

This chargeback reason code also applies to Installment and "Future Dated Transactions" and is restricted to cases where the cardholder has the regulatory right to stop payment on their card for this type of transaction.

B. Proper Use for Acquirer's Second Presentment

The acquirer may not second present referring to any merchant terms and conditions for cancellation.

6.1.6 Reason Code 4855 UK—Goods or Services Not Provided

The following variances/additional requirements to the *Chargeback Guide* apply for domestic transactions:

For disputes involving non-receipt of travel services from a bonded provider who has failed, the issuer or cardholder must attempt within **120 calendar days** from the date of failure, to obtain reimbursement from the relevant Bonding Authority prior to the issuer exercising a first chargeback, unless the issuer or cardholder has already been advised that the bond is insufficient. Where the issuer or cardholder has attempted to obtain reimbursement from the relevant Bonding Authority and subsequently received a negative response, the issuer has **60 calendar days** from the date of the Bonding Authority's response letter to exercise the chargeback.

A copy of the response from the Bonding Authority, or other notification stating that the bond is insufficient, must be sent to the acquirer with the cardholder's letter.

Refer to the *Chargeback Guide* regarding the overall time frame within which chargebacks must be processed.

6.1.7 Reason Code 4860 UK—Credit Not Processed

The following variances to the *Chargeback Guide* apply for domestic transactions.

A. Proper Use of Message Reason Code 4860

In case a credit was processed as a debit, issuers must provide evidence of the original debit transaction by supplying either the acquirer reference data (ARD) of the previous transaction if processed on a MasterCard card or Debit MasterCard card or other evidence of the original transaction if it was not processed on a MasterCard card or Debit MasterCard card.

Time Frame	Retrieval Request	Supporting Documents	DE 72
120 calendar days	No	If the original transaction was not processed on a MasterCard card or Debit MasterCard card, evidence of the original transaction	The ARD of the original transaction if processed on a MasterCard card or Debit MasterCard card

6.1.8 Reason Code 4863 UK—Cardholder Does Not Recognise—Potential Fraud

The following variance to the *Chargeback Guide* applies for domestic transactions:

A. Proper Use of Message Reason Code 4863

The issuer **may** use this chargeback reason code for face-to-face transactions.

The issuer may not use this chargeback reason code for the following types of transactions:

- Transactions where the clearing record (DE 55) shows that it was a chip transaction verified by use of the cardholder's PIN;
- Card Not Present transactions where the acquirer transmitted AVS data in the Authorisation Request/0100 message in accordance with requirements, and the issuer is not registered for AVS processing;
- Card Not Present transactions where the acquirer transmitted AVS data in the Authorisation Request/0100 message in accordance with requirements, and the issuer did not respond in the Authorisation Request Response/0110 message in DE 48 using one of the indicators provided in section 4.3.3;
- Card Not Present transactions where the acquirer transmitted CVC 2 data in the Authorisation Request/0100 message in accordance with requirements, and the issuer is not registered for CVC 2 processing;
- Card Not Present transactions where the acquirer transmitted CVC 2 data in the Authorisation Request/0100 message in accordance with requirements, and the issuer did not respond in the Authorisation Request Response/0110 message in DE 48 using the following indicators: **M** = CVC 2 Match.

B. Proper Use for Acquirer's Second Presentment

Second Presentment Condition	Supporting Documents	Data Record
The acquirer, who must be registered for AVS processing, can demonstrate that the issuer is not registered for AVS processing or did not respond in accordance with AVS processing requirements in respect of a CNP transaction.	Authorisation log reflecting an AVS response code of **S** or **U** or blank in DE 48 (Additional Date), PDS83 of the Authorisation Request Response/0110 message.	NONE
The acquirer can demonstrate that the issuer did not respond in accordance with CVC2 processing requirements in respect of CNP transactions	Authorisation log reflecting a CVC 2 response code other than **M** in DE 48, PDS 87 of the Authorisation Request Response/ 0110 message.	NONE

Chapter 7 MasterCard and Debit MasterCard Arbitration and Compliance

This section describes domestic variations to the arbitration and compliance rules.

7.0 Arbitration Cases

7.0.1 Pre-Arbitration

Prior to filing an arbitration case, the acquirer (for non-ATM disputes) or issuer (for ATM disputes) must submit a pre-arbitration request to the other party, in a good faith attempt to resolve the dispute. The pre-arbitration attempt must be sent using the Member Mediation service provided by MasterCom, allowing at least **30 calendar days** prior to the arbitration filing date.

If the requesting customer receives a rebuttal of the pre-arbitration letter, he may elect to file for arbitration immediately.

If the filed-against customer accepts responsibility for the disputed amount prior to the specified arbitration filing date, he must accept the Member Mediation request in Case Filing.

If the filed-against customer does not respond in Case Filing but only processes a credit via a Miscellaneous Fee Collection/1740 Message prior to, or on the specified case filing date, the credit will not be taken into consideration and a ruling will be issued.

If the filed-against customer accepts responsibility for the disputed amount, or is ruled responsible for the disputed amount in arbitration, the requesting customer may collect from the filed-against customer via a Miscellaneous Fee Collection/1740 message the amount of any Member Mediation Fees that it has been charged in connection with pre-arbitration.

The collecting party should use fee collection message reason code 7606 or 7607 and must clearly identify the MasterCom Case ID number in the Data Record DE 72.

If the pre-arbitration attempt fails and the dispute remains unresolved, then the acquirer/issuer may proceed to arbitration, as documented in the *Chargeback Guide*.

7.0.2 Arbitration

Refer to the *Chargeback Guide* for the arbitration procedures.

7.0.3 Filing Timeframe

The timeframe for filing arbitration cases is 75 calendar days from the arbitration chargeback processing date, or the second presentment processing date for ATM transactions.

7.1 Compliance Cases

Refer to the *Chargeback Guide* for the compliance procedures.

7.2 Arbitration and Compliance Fees

For arbitration and compliance cases relating to a UK domestic dispute, the following fees apply:

Filing Fee	EUR 200 (payable by the losing party)
Administration Fee	EUR 250 (payable by the losing party)
Technical violation fee	EUR 100

7.3 Appeals

Refer to the *Chargeback Guide* for the appeals procedure.

Chapter 8 Maestro Card Requirements

Please refer to section 5.13.1.1 of the Card Design Standards for specific UK Maestro card design requirements.

Chapter 9 Maestro Card Acceptance Requirements

This section describes acceptance requirements when processing domestic Maestro transactions.

9.1 Cardholder-Activated Terminal (CAT) Requirements

CATs must be configured so that the transaction amount is limited to the following maximum value, dependent upon the applicable merchant category.

MCC	Merchant Category	Maximum Transaction Amount (GBP)
30xx–32xx	Airlines with Specific Merchant Category Codes	300
35xx–37xx	Hotels with Specific Merchant Category Codes	300
4111	Ferries	300
4112	Passenger Railways	300
4131	Bus Lines	300
4511	Air Carriers, Airlines—not elsewhere classified	300
5542	Automated Fuel Dispensers	60 (if preauthorisation is for GBP 1)
7011	Lodging—Hotels, Motels, Resorts—not elsewhere classified	300
7523	Car Parks	130
7832	Motion Picture Theatres	300
7922	Theatrical Producers (except Motion Pictures), Ticket Agencies	300
—	Other Categories	50

Authorisation must be requested for the full transaction amount, with the exception of Automated Fuel Dispensers (AFDs), where the authorisation request may be for GBP 1. Alternatively, a preauthorisation for a pre-determined maximum amount may be submitted at an AFD, followed by an advice message. Refer to the international rules for the procedure to be followed in this case.

AFDs must check the limit for each transaction and advise cardholders of the maximum transaction amount, if the preauthorisation is for GBP 1, before the PIN is entered. If the preauthorisation is for a pre-determined maximum amount, the AFD must advise cardholders of this amount, before the PIN is entered.

Issuers must be able to receive preauthorisation requests for any amount as well as advice messages, and must be able to send advice acknowledgements.

For the chargeback rules applicable when a partial approval was given for an AFD transaction, refer to chapter 11 of the present manual. When a partial approval is given, the amount for which preauthorisation is requested does not determine the level of chargeback protection; the issuer may chargeback any amount in excess of the partial approval amount.

9.2 Multiple Authorisation Attempts on Card-Not-Present Transactions

On card-not-present transactions, a merchant is permitted a maximum of two declined authorisation attempts per calendar day on the same PAN. All authorisation attempts on the same PAN will count toward the maximum, regardless of the amount for which authorisation is requested.

The maximum applies per merchant, regardless of the number of acquirers, merchant names or merchant IDs that the merchant may have.

9.3 Smart Card Loading CAT Devices

The smart cards to be loaded must be issued by the merchant that operates the device, and only to holders whose names and addresses are known to the merchant

They must bear a means to verify the smart card holder on each occasion that she or he uses the smart card, not be capable of being used to obtain cash and not bear any detail of the smart card holder's Maestro cards.

If the smart card has its own PIN, the merchant must discourage the holder from using the same PIN for her/his card and not store details of the PIN with card details.

The loading device may use stored details of a card for transactions providing they are derived from a transaction in which the card itself was used.

The Card Acceptor Name/Location data provided in a transaction interchange file for a transaction performed at a loading device must contain the words "value load" and the merchant's name.

9.4 Telephone Pre-payments (Mobile Phones and Unspecified Phones)

A transaction is permitted only if the PAN has previously been registered with the merchant for pre-payments as per the following rules.

No more than two (2) cards may be registered (per phone in the case of mobile phones).

Where registration is for mobile phones, no more than two (2) phones may be registered per card.

The merchant must obtain and verify the cardholder's name and home address by one of the following methods:

1. Obtaining from the cardholder address or details from the address and either
   - Providing details from the address (for example, AVS data) to the issuer for verification; or
   - Verifying the address/details against a utility bill and or bank statement; or
2. Obtaining details for the address from the user

Authorisation must be obtained for every purchase transaction.

Transactions must be processed using merchant category code 4814.

If a transaction is charged back on grounds of fraudulent use, the acquirer must inform the merchant and the merchant must:

- If a mobile phone has been used, disconnect the phones for which the card is registers;
- If an unspecified phone has been used, not permit the cardholder to make any more calls;
- Cancel registration of the card used to perform the transaction;
- Not re-register a card with the same details.

This type of transaction must not be performed using contactless technology.

9.5 Transit Auto Top-Up Payments

Cardholders issued with a pre-pay card from a transit company offering the auto top-up service may auto-top-up their cards with set amounts when the amount held on the card falls below an agreed level using their Maestro card, under the conditions described below.

All cards must be registered for the service. This includes any cards new to the cardholder subsequent to the initial registration and opt-in process.

A maximum of two (2) debit cards only may be registered per auto top-up card.

Any one debit card can be registered against a maximum of two (2) auto-top-up cards only.

Cardholders can register for this auto-top-up service via the Internet and formally opt-in by use of email before this method of topping up their cards is enabled. When this service is offered via the Internet, some form of fraud screening must be undertaken. The initial transaction, classed as an e-commerce transaction, must be conducted using SecureCode. Subsequent transactions will be classed as MO/TO and must be flagged accordingly. If any checks fail, the transaction must not proceed.

MO/TO registration for this service is also permitted, whereby a cardholder contacts the call center, is supplied with an authority form for completion, which includes name and address, card number, expiry date, top-up amount and signature. On receipt, the transit company telephones the customer to undertake a CVC 2/AVS check. The registration is not progressed if the cardholder authority is not returned.

Cardholders can register for this service in a face-to-face environment. For POS transactions, the initial transaction must be conducted using the chip with no possibility of fallback. Subsequent transactions may be undertaken as MO/TO and must be flagged accordingly.

All transactions must be authorised and if approved autoload is set up. In the case of a decline, the cardholder will be contacted to verify payment details. If the outcome is unsatisfactory, the transit card must be hot-listed.

Standard liability applies to the initial transaction and for subsequent transactions, the acquirer is liable in all cases.

Two merchant IDs are required: one for the initial transaction and one for the subsequent transit auto top-up payments.

MCC 4111 must be used to allow accurate monitoring. The acquirer must monitor transaction and chargeback volumes in comparison to the card-not-present (CNP) average as follows:

1. The number of chargebacks should not exceed 1% of total Auto Top-Up transactions.
2. Total gross fraud to turnover must not exceed scheme average CNP fraud to turnover.
3. Total gross fraud to turnover must not exceed the average fraud to turnover ratio in MCC 4111 by 10% in any one month.
4. Monitoring must be based on fraud transaction data, therefore, be reviewed three months in arrears.

If a transaction is disputed, the following procedures should be followed:

1. Where a transaction goes through after a cardholder has cancelled his auto-top-up arrangement, compliance procedures may be initiated as documented in the *Chargeback Guide*; or
2. Where a transaction is fraudulent, chargeback code 4837 – "No Cardholder Authorisation" should provide a right of chargeback.

All fraud may be charged back with the exception of the initial transaction where standard liability applies.

9.6 Purchase with Cash Back Transactions

A maximum cashback amount of GBP 100 must be observed.

9.7 Quasi-cash Transactions (MCC 6051)

For a mail order/telephone order (MO/TO) transaction for currency and/or travelers cheques that are to be delivered:

1. The cardholder authority must include the cardholder's telephone number.
2. A name and address check or a CVC 2/AVS check must be performed.
3. Authorisation must be obtained.
4. The total amount of such transactions must not exceed GBP 3,000 per cardholder per day.

For electronic commerce transactions for currency and/or travelers cheques that are to be delivered, the total amount of such transactions must not exceed GBP 3,000 per cardholder per day.

Purchases of sterling are not permitted, except at merchants on board ships that have no other banking facilities. If sterling is purchased at such merchants, secondary identification must take the form of a passport, full driving license, or Armed Forces ID, and the amount of the transaction must not exceed GBP 500.

9.8 Gambling Transactions (MCC 7995)

For a mail order/telephone order (MO/TO) transaction, cardholder authorities must contain a personal registration number given to the cardholder by the merchant, before the cardholder performs the first transaction.

Although the authority for a first transaction at a merchant must conform to normal UK Maestro rules, authorities for subsequent transactions need not include the card's PAN; cardholder's name; expiry date; or cardholder's home address.

Name and address checks are not permitted.

A Merchant must not give a cardholder a personal registration number unless:

- It has obtained the cardholder's name and address;
- A POS terminal at one of its outlets has accepted the following details from the cardholder's card: PAN and expiry date.

If the cardholder uses a card other than the card whose details have been accepted by the merchant's POS terminal (for example, following the issue of a new card):

- Details of the other card must also be accepted by a POS terminal at one of the merchant's outlets;
- A personal registration number must be provided to the cardholder for use with the other card.

Authorisation must be performed for every purchase and purchase with cash back transaction and the cardholder must be advised of the outcome before a bet is accepted.

9.8.1 Gaming Payment Transactions

Face-to-face gambling merchants may use the Gaming Payment Transaction to transfer winnings in accordance with all applicable rules. Gambling merchants that are legally required to transfer winnings to the same card that was used to place the bet or purchase gambling value must use the Gaming Payment Transaction for this purpose.

9.9 Mail Order/Telephone Order (MO/TO) Transactions

MO/TO transactions must not be performed using contactless payment functionality or include purchase with cash back.

A MO/TO transaction must have its own unique cardholder authority. Manual key entry of the PAN is the normal method of performing a MO/TO transaction. There is no cardholder verification procedure.

A zero floor limit is applicable for all MO/TO transactions.

If an issuer's response to an authorisation request is incorrectly supplied as call referral, this must be translated into a decline.

The merchant must collect and transmit CVC 2 for all MO/TO transactions. In addition, AVS checking is mandatory at merchants that deliver foreign currency or travelers' cheques. AVS checking is optional for all other MO/TO transactions.

The merchant must not present the transaction until the products or services are ready to be dispatched.

If the merchant does not give the cardholder the transaction receipt or the products and/or services upon completion of the transaction, then they must be either delivered to the cardholder by a method chosen at the merchant's discretion or collected by the cardholder.

9.10 Cardholder Authorities

A cardholder authority must contain:

1. The card's PAN, expiry date, and CVC 2 as positioned in a white panel adjacent to the signature panel on the card;
2. The cardholder's name and home address (including postcode);
3. The transaction amount (including postage and packaging);
4. For a mail order transaction: a document signed by the cardholder or a document which the acquirer considers to be acceptable in lieu of a signed document (for example, an authority sent by facsimile transmission);
5. For a telephone order transaction:
    a. Either
        1. instructions given over the telephone by the cardholder to the merchant, either to the merchant's staff or to equipment operated by the merchant (for example, an interactive voice system), or
        2. instructions given over the telephone by means of a text message from the cardholder to the merchant, via equipment operated by the merchant; and
    b. The date on which the Cardholder gave her/his authority; and
6. If goods/services are to be delivered, the delivery address, and if the goods/services are to be delivered to or collected by a third party, the third party's name.

9.11 CVC 2/AVS Checks

The following applies where the merchant carries out AVS checking and for CVC 2 checks.

The cardholder authority must include the CVC 2 shown on the cardholder's card.

When entering the transaction, the merchant must key in the CVC 2 and numeric data in the cardholder's address and postcode.

Online authorisation must be sought for the transaction.

The acquirer must attempt to send the authorisation request to the issuer accompanied by the CVC 2/AVS data.

When the issuer's response to the authorisation request is approved, the issuer must accompany its response with an indication as to whether, for each of the CVC 2, the address numerics and the postcode numerics:

1. The data matches information held in its own records; or
2. The data does not match information held in its own records; or
3. The address numerics and postcode numeric have not been checked; or
4. The data has not been supplied.

When the acquirer sends a response to the authorisation request to the merchant's POS terminal, the message must include the issuer's CVC 2 and AVS responses.

The merchant must not re-use the CVC 2 or retain the CVC 2 in any manner for any purpose. The CVC 2 on a cardholder authority for a mail order transaction must be rendered unreadable prior to storage.

9.12 CVC 2 Mismatches

If an issuer receives CVC 2 data in the authorisation request and it is invalid (for example, the CVC 2 field is not blank and the data does not match the data held on the issuer's records), the authorisation request must be declined.

If an authorisation request is approved when the CVC 2 data submitted is invalid, the issuer cannot charge the transaction back for a fraud-related reason.

9.13 Payday Loans

A chargeback right is available under reason code 4841 when the cardholder disputes any of the following fees related to payday loans (including payday loan brokers or other payday loan service providers):

- Fees or penalties associated with the agreement or the repayment; or
- Fees or penalties associated with a broker or other service.

This chargeback right is available for both recurring and non-recurring transactions related to payday loans.

Chapter 10 Maestro Card Processes

This section provides information about processes, documentation, and fees.

10.1 MATCH

Acquirers must refer and report to Merchant Alert to Control High-Risk Merchants (MATCH™), as set forth in the *Security Rules and Procedures* manual.

Before signing a merchant agreement with a potential merchant, an acquirer must check whether or not the potential merchant, or any of its outlets, appears on the MATCH files. If an entry appears, any resulting contact with another acquirer must be performed by the acquirer itself (that is, must not be delegated to agents).

10.2 Address Verification Service

Acquirer and issuer participation in the Address Verification Service (AVS) is mandated for UK Maestro CNP domestic transactions.

10.2.1 Acquirer Requirements for AVS

An acquirer must register for AVS processing and meet the following requirements:

1. The acquirer must transmit address information, when provided by the merchant, to the issuer in the Authorisation Request/0100 message for CNP domestic transactions;
2. The acquirer must be able to receive the AVS response data from the issuer contained in the Authorisation Request Response/0110 message and forward it to the merchant.

10.2.2 Issuer Requirements for AVS

An issuer must register for AVS processing and meet the following requirements:

1. The issuer must be able to verify AVS data contained in the Authorisation Request/0100 message for CNP domestic transactions;
2. The issuer must transmit AVS response code to the acquirer in the Authorisation Request Response/0110 message.

With respect to newly assigned ICAs and BINs, an issuer is allowed six months from the date of assignment to come into compliance with these requirements.

An issuer that fails to register for AVS processing, or that does not provide a valid response code to acquirers, will not be eligible to charge back applicable transactions using message reason code 4837—No Cardholder Authorisation, where AVS data was provided by the acquirer.

10.2.3 AVS Response Codes

The following table describes the possible responses that an acquirer may receive to a request for an AVS check.

Response Code	Description
A	Address matches, postal code does not
N	Neither address nor postal code match
R	Retry–system unable to process
S	AVS currently not supported
U	No data from issuer/authorisation system
W	Postal code matches/address does not
X	Postal code and address match

10.3 Automatic Billing Updater Programme and Recurring Payments Cancellation Service

10.3.1 Acquirers

Acquirers must participate in the MasterCard Automatic Billing Updater programme by completing the Member Enrollment Form available on MasterCard Connect™.

Acquirers must be able to send, receive and process ABU data.

Acquirers must ensure that their acquiring host processing system incorporates ABU functionality.

Acquirers are required to register their UK Recurring Payment Merchants in the ABU programme.

Acquirers must submit card account number queries to the ABU programme on behalf of their Recurring Payment Merchants before authorisation.

10.3.2 Issuers

Issuers must participate in the MasterCard Automatic Billing Updater programme by completing the Member Enrollment Form available on MasterCard Connect™.

Issuers must be able to send, receive and process ABU data. Issuers must maintain their entire active card portfolio in ABU and communicate all account changes via the ABU programme.

With respect to newly assigned ICAs and BINs, an issuer is allowed six months from the date of assignment to come into compliance with this requirement.

To support the Account Validation process issuers must report new accounts and provide a one-time upload plus 6 months of historic data changes up to a maximum of 40 months data to the Issuer Account Change Database.

Account changes are classified as:

- New Accounts opened
- Account changes (BIN changes, upgrades, lost, stolen)
- Expired Account
- Closed Accounts
- Portfolio acquisitions (Maestro to Maestro)
- Brand flips from any competitor scheme to Maestro (optional)

Issuers must enroll and participate in the Recurring Payments Cancellation Service by either submitting the RPCS enrollment form or using the online RPCS enrollment process available on MasterCard Connect.

10.3.3 Documentation Location

The ABU and RPCS documentation set can be found by following these steps:

1. Go to **www.mastercardconnect.com**.
2. Enter your **User ID** and **Password**.
3. Under **Library**, select **References**.
4. Select **Products & Services**, and then click **Recurring Payments**.
5. Select **Automatic Billing Updater** or **Recurring Payment Cancellation Service**.

10.3.4 Exemptions from the Requirement to Support ABU

Prepaid programmes are exempt from ABU reporting requirements, provided that the issuer does not allow the prepaid cards to be used to enter into recurring payment arrangements.

This exemption applies to both consumer and corporate prepaid programmes.

Single-use-only virtual account numbers are exempt from ABU reporting requirements.

Chapter 11 Maestro Card Domestic Chargeback Rules

This section describes chargeback rule variations for domestic transactions.

11.1 Specific Domestic Maestro Chargeback Rules

Specific domestic rules apply to the following chargeback reason codes:

- 4808—Requested/Required Authorisation Not Obtained
- 4837—No Cardholder Authorisation
- 4841—Cancelled Recurring Transaction
- 4870—Chip Liability Shift

For the above reason codes the domestic rule is a variance to part, or parts, of the international rule.

Detailed procedures for processing chargebacks are documented in the *Chargeback Guide*.

11.2 Message Reason Code 4808—Requested/Required Authorisation Not Obtained

11.2.1 Proper Use of Message Reason Code 4808

- **Multiple Authorisation.** The issuer may chargeback under this reason code if a card-not-present transaction was approved in stand-in following two declined authorisation attempts on the same PAN by the same merchant on the same calendar day.

Time Frame	Retrieval Request	Supporting Documents	Data Record
90 days	No	None	Multiple authorisation requests

- If a transaction is processed at a CAT dispensing fuel for an amount in excess of GBP 60 and the transaction was identified in the authorisation request with MCC 5542, and authorised by the issuer for GBP 1, the issuer may process a partial chargeback for the amount exceeding GBP 60. If the transaction amount is less than or equal to GBP 60 the issuer may not invoke the chargeback.
- Partial Authorisation of Automated Fuel Dispenser (MCC 5542) transactions If an authorisation request/0100 message indicates that an automated fuel dispenser card acceptor supports partial authorisation, and the transaction amount exceeds the partial approval amount in DE 6 of the authorisation request response/0110 message, the issuer may charge back the difference between the transaction amount and the partial approval amount. This rule applies even if the authorisation request was for GBP 1.

11.2.2 Proper Use for Acquirer's Second Presentment

Multiple Authorisation. The acquirer may second present if the transaction was authorised by the issuer and not in Stand-in, or if authorisation was obtained after fewer than two

declined authorisation attempts on the same PAN by the same merchant in the same calendar day

Second Presentment Conditions	Supporting Documents	Data Record
The transaction was authorised by the issuer, or was authorised after less than two declined authorisation attempts	None	"Issuer authorised" Less than 2 authorisation attempts"

11.3 Message Reason Code 4837—No Cardholder Authorisation

11.3.1 Proper Use of Message Reason Code 4837

This message reason code may be used for mail order/telephone order (MO/TO) transactions and non–face-to-face fraudulent mobile phone prepayment transactions.

11.3.2 Improper Use of Message Reason Code 4837

An issuer may not raise a chargeback under this message reason code for a cardholder not present transaction where it has been provided in an authorisation request with the CVC 2 on the card and numeric data in the cardholder's address and postcode and one of the following.

1. The issuer fails to perform a check on any of this information, or
2. The CVC 2 does not match the CVC 2 held by the issuer.

11.3.3 Proper Use for Issuer's First Chargeback

Where a chargeback is being raised as a result of multiple fraudulent mobile phone pre-payment transactions performed with the same card, the issuer may combine the transactions in question into a single First Chargeback/1442 message, providing supporting documentation including a schedule showing dates and amounts of each transaction.

11.3.4 Proper Use for Acquirer's Second Presentment

The following lists show what the acquirer should provide to process a second presentment following the chargeback of a MO/TO transaction and following the chargeback of a non–face-to-face fraudulent mobile phone prepayment transaction.

1. The acquirer may process a second presentment following the chargeback of a **MO/TO** transaction by providing one of the following:
    a. A cardholder authority or receipt which, in either case, bears the cardholder's signature and shows correct details of the transaction, including correct details of the cardholder's card.; or
    b. A cardholder authority (for example, an email message, a facsimile document); or

c. An invoice quoting the cardholder's name; or
d. A delivery receipt signed by the cardholder and quoting a billing address; or
e. A document indicating a different merchant name than the one shown in the clearing record; or
f. Proof that the delivery address contained the same numerics as those with which the issuer had been provided, but only where a "full match" response to the AVS check was given; or
g. For airline tickets purchases, a copy of the boarding pass showing the cardholder's name; or
h. Details of a long-standing account/customer relationship between the merchant and the cardholder: (such as account opening information); or
i. If proof of death or incapacitation on the day a transaction was performed is provided by the issuer, evidence that the transaction took place earlier than death or incapacitation.

2. The acquirer may process a second presentment following the chargeback of a non–face-to-face fraudulent **mobile phone pre-payment** transaction by providing the following:

a. Evidence that the transaction was initiated by the cardholder.
b. If proof of death or incapacitation on the day a transaction was performed is provided by the issuer, a second presentment is permitted only if evidence can be provided that the transaction took place earlier than death or incapacitation.

11.3.5 Arbitration Case Filing

The issuer may continue the dispute providing a progressive cardholder letter refuting the compelling evidence received from the card acceptor in the second presentment. Before filing for arbitration the issuer must process a member mediation (pre-arbitration) granting the filed-against member 30 days to respond.

After the 30 days have elapsed or the acquirer has rejected the pre-arbitration attempt, the issuer may escalate the case to arbitration within 75 days of the second presentment. All cases, including member mediations must be filed in MasterCom Case Filing or via the Case Filing Hub Site.

11.4 Message Reason Code 4841—Cancelled Recurring Transaction

The following variances/additional requirements to the Chargeback Guide apply for domestic transactions.

11.4.1 Proper Use of Message Reason Code 4841

Time Frame	Retrieval Request	Supporting Documents	Data Record
14 calendar days	No	None	CARDHOLDER DECEASED or

Time Frame	Retrieval Request	Supporting Documents	Data Record
			ACCOUNT CLOSED or FACILITIES WITHDRAWN or CARDHOLDER WITHDREW AUTHORITY, as appropriate
120 calendar days	No	Cardholder letter disputing any fees related to Payday Loans.	Payday Loan Fee

In the event that:

1. the cardholder is deceased.
2. the issuer or the cardholder has withdrawn or closed the account facilities.
3. the cardholder withdrew his or her authority to bill a Future Dated Transaction or recurring Transaction, regardless of any merhcnat terms and conditions.

The issuer can initiatate a chargeback, within 14 calendar days of the Translaction Processing Date, without having previously notified the merchant of the cancellation.

No supporting documentation is required, but the issuer must identify the reason for the chargeback using appropriate text in the Data Record. Beyond the 14-calendar day time frame, the standard international chargeback rule applies, including time frame and documentation requirements.

This chargeback reason code also applies to Installment and "Future Dated Transactions" and is restricted to cases where the cardholder has the regulatory right to stop payment on their card for this type of transaction.

This chargeback reason code also applies when the cardholder disputes any of the following fees related to Payday Loans (including payday loan brokers or other payday loan service providers).

- Fees or penalties associated with the agreement or the repayment; or
- Fees or penalties associated with a broker or other service. The chargeback timeframe in this scenario is 120 days from the transaction processing date. This chargeback right is available for both recurring and non-recurring transactions related to payday loans.

This chargeback right is available for both recurring and non-recurring transactions related to payday loans.

11.4.2 Proper Use for Acquirer's Second Presentment

When the issuer used one of the above mentioned options, the acquirer may not second present referring to any merchant terms and conditions for cancellation or on the grounds that the cardholder consented to the charge in any of the scenarios described in Rule 11.4.1 of these rules.

11.5 Message Reason Code 4870—Chip Liability Shift

11.5.1 Proper Use for Message Reason Code 4870

- For counterfeit fraud this reason code may be used for transactions taking place at a magnetic-stripe-reading-only cardholder-activated terminal.
- For lost, stolen, or never-received fraud, this reason code may be used for transactions taking place at a non–PIN-capable cardholder-activated terminal.

Chapter 12 Maestro Card Arbitration and Compliance

For the rules applicable to arbitration and compliance cases relating to a domestic Maestro dispute, please see Section B.4.1 of the *Chargeback Guide* with the exception of section 11.3.5 of this manual.

Appendix A Compliance Zones

This appendix provides the noncompliance category assigned to the rules contained this manual.

Noncompliance Categories

The following table provides the noncompliance category assigned to the rules contained in this manual. These noncompliance categories are assigned for the purposes of imposing assessments when warranted under the compliance framework described in the *MasterCard Rules*. A minimum of 30 days will be allowed to remedy noncompliance.

Number	Rule Title	Category
3.1	Purchases	A
3.2	Face-to-Face Cash Advance Transactions	A
3.3	Unique Transactions	A
3.4	Sales of Foreign Currency	B
4.1	Expiry Date Checking by Issuers	C
4.2	Card Validation Code 2 (CVC 2)	A
4.3	Address Verification Service	A
4.4	Issuer's Right to Request a Transaction Information Document	C
4.6	Automatic Billing Updater and Recurring Payments Cancellation Service	B
4.7	Issuer Response on Recurring Transactions	C
4.8	Merchant Rewards	B
5.1	Domestic Settlement Service	C
9.1	Cardholder Activated Terminal	A
9.2	Multiple Authorisation Attempts on Card-not-present Transactions	A
9.3	Smart Card Loading CAT Devices	A
9.4	Telephone Pre-Payments (Mobile Phones and Unspecified Phones)	A
9.5	Transit Auto Top-Up Payments	A

Number	Rule Title	Category
9.6	Purchase with Cash Back Transactions	B
9.7	Quasi-cash Transactions (MCC 6051)	A
9.8	Gambling transactions (MCC 7995)	A
9.9	Mail Order/Telephone Order (MO/TO) Transactions	A
9.10	Cardholder Authorities	A
9.11	CVC 2/AVS checks	A
9.12	CVC 2 Mismatches	A
10.1	MATCH	A
10.2	Address Verification Service	A
10.3	Automatic Billing Updater Programme and Recurring Payments Cancellation Service	B

Notices

Following are policies pertaining to proprietary rights, trademarks, translations, and details about the availability of additional information online.

Proprietary Rights

The information contained in this document is proprietary and confidential to MasterCard International Incorporated, one or more of its affiliated entities (collectively "MasterCard"), or both.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of MasterCard.

Trademarks

Trademark notices and symbols used in this document reflect the registration status of MasterCard trademarks in the United States. Please consult with the Global Customer Service team or the MasterCard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

Disclaimer

MasterCard makes no representations or warranties of any kind, express or implied, with respect to the contents of this document. Without limitation, MasterCard specifically disclaims all representations and warranties with respect to this document and any intellectual property rights subsisting therein or any part thereof, including but not limited to any and all implied warranties of title, non-infringement, or suitability for any purpose (whether or not MasterCard has been advised, has reason to know, or is otherwise in fact aware of any information) or achievement of any particular result. Without limitation, MasterCard specifically disclaims all representations and warranties that any practice or implementation of this document will not infringe any third party patents, copyrights, trade secrets or other rights.

Translation

A translation of any MasterCard manual, bulletin, release, or other MasterCard document into a language other than English is intended solely as a convenience to MasterCard customers. MasterCard provides any translated document to its customers "AS IS" and makes no representations or warranties of any kind with respect to the translated document, including, but not limited to, its accuracy or reliability. In no event shall MasterCard be liable for any damages resulting from reliance on any translated document. The English version of any MasterCard document will take precedence over any translated version in any legal proceeding.

Information Available Online

MasterCard provides details about the standards used for this document—including times expressed, language use, and contact information—on the Publications Support page available on MasterCard Connect™. Go to Publications Support for centralized information.