Chargeback Guide

Version: 1.1.1
13 July 2021

Copyright

(c) 2021. Global Processing Services All Rights Reserved.

The material contained in this guide is copyrighted and owned by Global Processing Services Ltd together with any other intellectual property in such material.

Except for personal and non-commercial use, no part of this guide may be copied, republished, performed in public, broadcast, uploaded, transmitted, distributed, modified or dealt with in any manner at all, without the prior written permission of Global Processing Services Ltd., and, then, only in such a way that the source and intellectual property rights are acknowledged.

To the maximum extent permitted by law, Global Processing Services Ltd shall not be liable to any person or organisation, in any manner whatsoever from the use, construction or interpretation of, or the reliance upon, all or any of the information or materials contained in this guide.

The information in these materials is subject to change without notice and Global Processing Services Ltd. assumes no responsibility for any errors.

Contents

1. About This Document

This guide describes the Chargeback process and how GPS supports chargeback management.

Document Scope

This guide describes chargebacks as processed and handled via GPS.

Target Audience

This guide is intended for GPS clients (Program Managers) who are interested in managing chargeback transactions.

What's Changed?

If you want to find out what's changed since the previous release, see the Document History section.

1.1. How to use this Guide

If you are new to chargebacks and want to understand how they work, see the Overview section.

To find out about the chargeback management options supported by GPS, see Chargeback Options.

To find out how to manage your chargebacks via Smart Client, see Managing Chargebacks on Smart Client

1.2. Related Documents

Refer to the table below for other documents which should be used in conjunction with this guide.

Document	Description
EHI Guide	Provides details of the GPS External Host Interface (EHI).
Smart Client Guide	Describes how to use the GPS Smart Client to manage your account.

2. Overview

2.1. What is a Chargeback?

A chargeback is a type of transaction dispute where a cardholder contacts their card issuer and requests their money back for an item or service purchased by using their card. The cardholder can only dispute a charge on their account and request a chargeback where they have a valid reason. For example:

- Goods or services not received
- Goods or services received not as advertised, faulty or of an unsatisfactory quality
- The amount charged is incorrect
- Fraudulent transaction – the cardholder did not make the transaction and their card details were obtained fraudulently

In all instances, the cardholder should first contact the merchant to attempt to resolve their issue, for example, by asking the merchant to issue a refund or resend a replacement item. Where the customer and merchant cannot agree on a resolution, the cardholder has the right to contact their card issuer and ask them to raise a chargeback.

The card schemes (i.e., Visa and Mastercard; also known as card networks) provide rules and processes, as well as systems to handle chargebacks. You can find out more about their rules at the following links:

- Mastercard Chargeback Guide
- Visa Chargeback Guidelines for Merchants (see Section 5 for issuer guidelines)

2.2. What is the Chargeback Process?

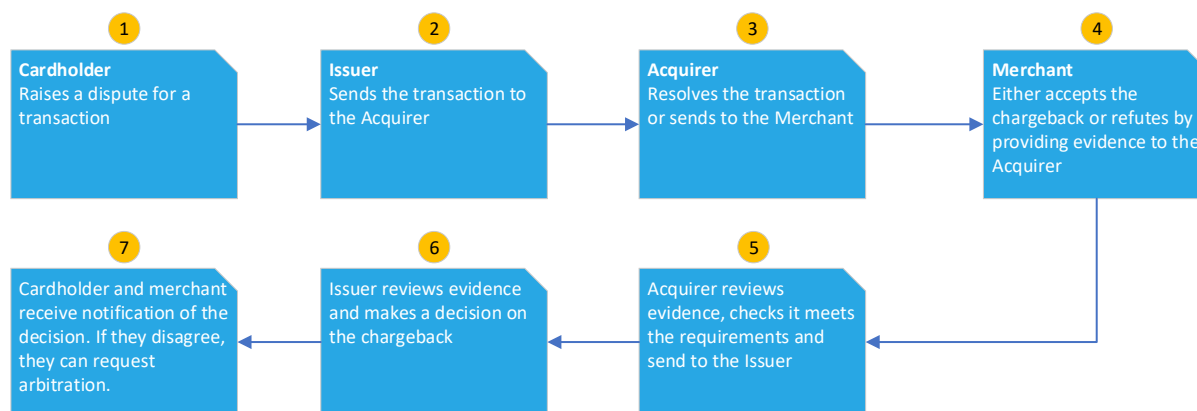*Figure 1* below provides a summary of the chargeback process.

Figure 1: Chargeback Transaction Flow -Simplified

Note that the communication between issuer and acquirer and the arbitration process is managed via the relevant card scheme (Mastercard or Visa), not shown in this figure.

The GPS Mastercard API development provides support for creating and managing the chargeback process described below, and includes new options such as arbitration and pre-arbitration case filings and bulk chargeback creation.

1. The cardholder disputes a transaction with their issuer (card issuing bank or their Program Manager).
2. Where required by scheme rules the card issuer sends a retrieval request to the merchant's acquirer (financial institute providing the merchant with a merchant trading account) to obtain additional information.
3. The acquirer and issuer attempt to resolve the dispute if possible (for example, by issuing a refund), otherwise the acquirer sends a chargeback notification to the merchant.
4. The merchant either accepts the chargeback or refutes it. If they refute the chargeback, they must submit the necessary evidence through representment.
5. The acquirer reviews the evidence, checks it meets the requirements and sends to the issuer.
6. The issuer reviews the new evidence and makes a final decision.
7. At this point, any party unhappy with the decision can either request further review, via pre-arbitration or go directly to the arbitration stage. If the acquirer and issuer cannot reach an agreement, the process enters arbitration. The card schemes will examine the evidence and make a final decision.

Note: The arbitration process can last for months and costs hundreds of pounds, which must be paid to the card schemes.

2.3. How does GPS Support Chargebacks?

As a Program Manager or card issuer, your cardholders should have a means to contact you directly to raise disputes about a transaction on their account. This is typically via a call centre number printed on their card or advertised on your website.

When a cardholder queries a transaction, you can use the GPS *Smart Client* application to view details of the transaction. Smart Client also provides a facility to enable you to raise and manage chargebacks (Note that this is only available for Mastercard issuers in Europe/UK at present). See *How to create and view chargebacks on Smart Client*.

Chargebacks are also supported via the relevant card scheme (e.g., MasterCard or Visa), which provide online systems where issuers and acquirers can view and respond to chargeback notifications.

If you are a card issuer, you will be able to respond directly to the card schemes. However, most GPS clients are Program Managers, who use an existing card issuer to provide their card service, and in this case, GPS can mediate on your behalf with your issuer's permission.

Note: Some issuers manage all chargebacks for their Program Manager clients, while others want their clients to raise their chargebacks directly with us and have enabled our Mastercom API to facilitate this.

> **Note**: If you are a Program Manager you will not have a direct relationship with the card scheme. You will need your issuer or GPS to provide you with information to help you manage your chargebacks.

2.4. Payment Authorisation Transaction Process

Figure 2 provides an overview of the transaction process and parties involved in a typical card payment scenario.
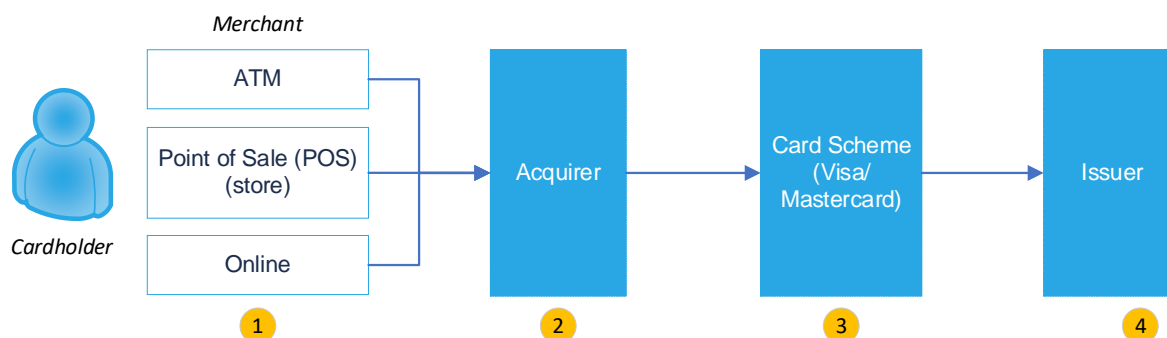

Figure 2: Card Payment Authorisation

Visa and Mastercard distribute Bank Identification Number (BIN) and sub BIN range tables to their customers (acquirers and issuers).

1. When a cardholder uses their card at a merchant store or website, or draws out money from an ATM, the acquirer Point of Sale (POS) terminal or Online PSP forwards the authorisation request to the merchant's acquirer.
2. The acquirer uses the BIN range tables to determine where to route the transaction.
3. The acquirer routes the transaction to the relevant card scheme (Visa or Mastercard).
4. Using the same BIN range, tables Visa and Mastercard identify the card issuer and route the transaction to the issuer.

> **Notes**:
> If the acquirer and issuer are the same bank, then the transaction is processed internally, and not sent to Mastercard or Visa.
> In some countries domestic transactions are routed via national switches, but not sent to Mastercard or Visa (e.g. BKM in Turkey).

If you are a Program Manager, the card scheme will route the transaction to GPS, who then forwards on to your card issuer. Depending on your External Host Interface (EHI) mode, in cases where the GPS External Host system holds the balance on the card, GPS may perform the payment authorisation and then forward to the issuer. You will receive real-time transactional data via your EHI data feed or overnight as transactional XML reports. See *Figure 3* below.
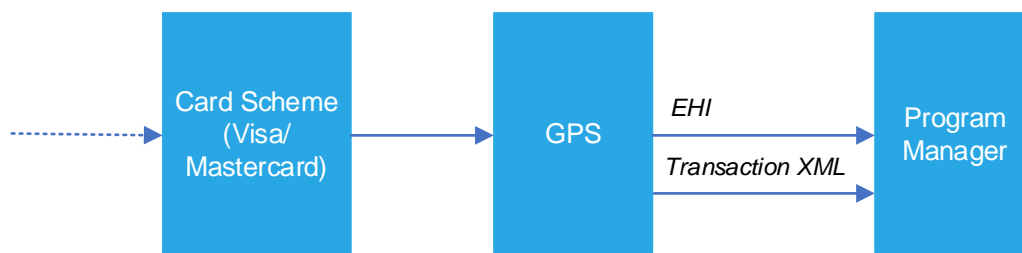
Figure 3: Role of GPS in Transaction Authorisation

At a transactional level, issuer BINs are routed to GPS. However, issuers still settle the funds between Mastercard and Visa, as GPS does not hold the funds on the card.

Mastercard and Visa both provides online systems to enable acquirers and Issuers to raise and manage disputes. Issuers have different preferences as to how they want to manage chargebacks for their Program Managers:

- Some issuers prefer to handle chargebacks on behalf of their Program Managers.
- Some issuers provide their Program Managers with access to Mastercard (Mastercom UI) and Visa (Visa VROL) online systems to enable them to directly raise and respond to chargebacks
- Other issuers want GPS to manage this at a programme level for the Program Manager, which we do via Smart Client.

Please refer to your issuer in the first instance for details.

2.5. Chargeback Processes – Transaction Status View

Figure 4 below shows the typical transaction status changes during the life cycle of a transaction, from authorisation through to presentment and chargeback. This is a simplified view and does not show all the steps involved.

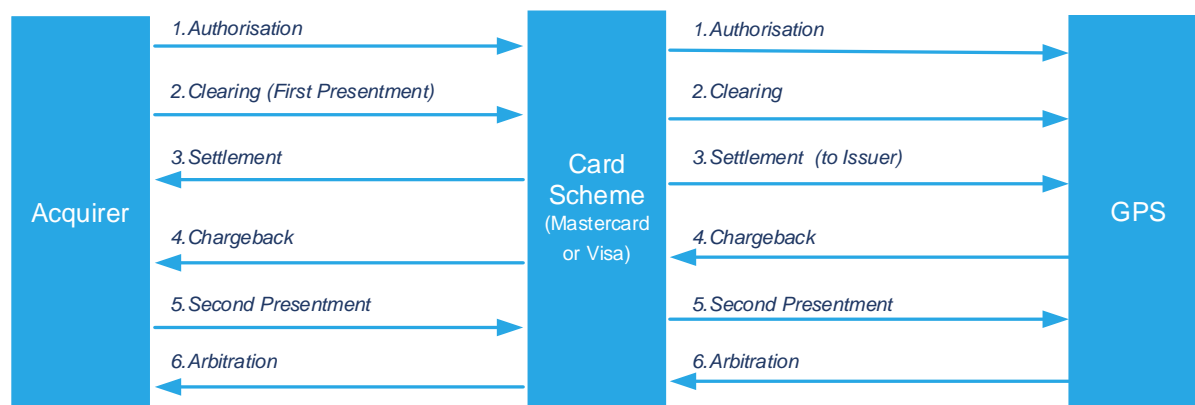*Figure 4: Transaction Life Cycle (Simplified)*

1. The cardholder uses their card to make a purchase and the transaction is Authorised. This step involves checking the balance on the account to ensure there are sufficient available funds for the transaction. At this stage the authorised amount may be reserved on the cardholder's account or the merchant may want to take it immediately.

2. When the merchant is ready to take the funds, the transaction is submitted for clearing, where the authorised amount is debited from the cardholder's account. This stage is known as Clearing or First Presentment. In Smart Client, this is shown as a Presentment status.

3. Settlement is the process where actual funds are exchanged between the issuer and acquirer (the acquirer implements a separate settlement process with their merchant).

> **Note**: GPS receive settlement reports from the scheme and pass it to our clients without any checks or additional processing. Actual settlement (funds transfer) is between the schemes and our issuers. This stage is shown in *Figure 4* for completeness and is not recorded as a transaction status within Smart Client.

4. A chargeback request can only be initiated on a transaction that has reached the *Presentment* stage. (Prior to this, you can use a reversal to reverse the authorisation.)

5. Once a chargeback is raised, it is sent to the card scheme (Mastercard or Visa) who forwards it on to the merchant's acquirer. At this stage the acquirer can accept the chargeback. If the acquirer does not agree with the chargeback, they can refute the chargeback, and the transaction goes into the Second presentment stage.

6. If the chargeback cannot be resolved, the card issuer can decide to proceed with case filing and case the transaction enters the Arbitration stage. The card scheme reviews and make a final decision.

After completion of the chargeback process, the acquirer and issuer can file relevant case documents. They can also raise fee collection requests.

Collaboration Option

Mastercard offer a collaboration option, where the chargeback first goes directly to the merchant (the acquirer is not involved at this stage). If the merchant accepts collaboration, they will need to issue the refund as a separate transaction.

By improving communication between the issuer and merchant prior to the formal dispute process taking place, many disputes can be settled without entering the chargeback process.

This service is enabled via Mastercard. Check with your Issuer for details.

3. MasterCom API

Mastercom API offers Mastercard customers the ability to create and manage dispute claims in Mastercom. Mastercom is a system for dispute management. All activities for any given dispute can be tracked within a single claim using Mastercom, including *Retrieval Request and Fulfilment*, *First Chargeback*, *Second Presentment*, *Fraud reporting*, *Case Filing*, and *Fee Collection* requests. All activities for any given dispute throughout its lifecycle can be tracked within a single claim.

The Mastercom API is available to Programme Managers and card issuers to use.

GPS provides an interface to Mastercom via Smart Client, which means you do not need to develop your own Mastercom API integration. See *Chargeback Options*: Option 2: Using the GPS Smart Client.

4. Chargeback Options

There are two options available for managing your chargebacks.

4.1. Option 1: Using the Scheme UI

If you are a card issuer, or you are a GPS Program Manager who has been provided access via your card issuer, you can use the Mastercard and Visa online systems to raise chargebacks and manage the dispute processes.

- Mastercard offer the Mastercom Claims Manager
- Visa offer the Claims Resolution Visa system, which we refer to as the Visa Resolution Online (VROL) platform

Note: These systems require you to be fully PCI DSS compliant, as full PAN is used. Chargeback details will be available in XML messages.

Notes on using Mastercom Claims Manager

- When you are onboarded to Mastercom Claims Manager, to reduce the need to raise a chargeback claim, you can opt in for their collaboration option. This is enabled by Mastercom.
- GPS provide an option to automatically credit the chargeback amount to the cardholder. This configured at GPS product level. For details, contact your GPS account manager.

4.2. Option 2: Using the GPS Smart Client

If you do not have access to the Mastercard or Visa systems or are unable or prefer not to use full PAN, GPS provides a backend integration into these systems to enable receipt of chargeback files, when chargebacks are raised and responded to. You can view chargebacks transactions directly in Smart Client (the GPS application for managing your account).

For Mastercard transactions (currently Europe/UK only), you can raise and respond to chargebacks directly in Smart Client. Support for Visa and additional Mastercard jurisdictions are being added.

How to Implement

You must complete the following prerequisites before the Smart Client Chargeback service can be enabled:

- Please contact your issuer to request they enable GPS to use the Mastercom API data feed for your BIN codes.
- Costs for the service must be agreed with your GPS account manager and added as an addendum to your GPS contract.

5. Managing Chargebacks on Smart Client

Smart Client enables you to view Visa and Mastercard chargebacks.

For Mastercard transactions only you can raise chargebacks requests to Mastercard and manage your charged back transactions. This service uses the Mastercom API and requires that you first sign up for the service and enable the API data feed via your issuer. See How to Implement.

Using Smart Client, you are able to:

- View details of existing chargebacks across your programme or for a specific card. See Viewing Chargebacks
- View details of the transaction linked to a chargeback. See Viewing Transaction Details.
- View details of the Presentment transaction linked to a chargeback. See Viewing Presentment Details.

Note: Functionality described below is provided for Mastercard only.

- Retrieve information about a disputed transaction from the acquirer (prior to raising a chargeback). See Creating a Retrieval Request.
- Raise a chargeback for a single transaction. See Creating a Chargeback.
- Raise multiple chargebacks in one transaction, using a chargeback bulk upload spreadsheet. See Creating Bulk Chargebacks.
- Attach a file to a chargeback. See Uploading Chargeback Documentation.
- Retrieve documentation previously uploaded for a chargeback case. See Downloading Chargeback Documentation.
- Withdraw a chargeback. See Reversing a Chargeback.
- Re-raise a rejected chargeback. See Re-raising a Chargeback.
- Create a Fee Collection request. See Managing Fee Collections.
- Send a SAFE report to Mastercom for a fraudulent transaction. See Creating a Mastercom SAFE Report.

Note: You may require access to be set up on your account to view some of these options. Please contact GPS Support for details.

5.1. Creating a Chargeback

Note: Currently supported for Mastercard cards only.

This option enables you to raise a chargeback to Mastercom for a disputed transaction. You can do this with or without attaching documentation.

Note: The transaction must be in the Presentment state in order to create the chargeback (i.e., the transaction has been previously authorised, and the funds have been debited from the cardholder's account).

1. In the **View Transactions** window, right-click the transaction being disputed by the cardholder and select **Actions > Create Chargeback**.
2. In the **Chargebacks** window, enter the details of the chargeback. Refer to *Table 1* below for details.
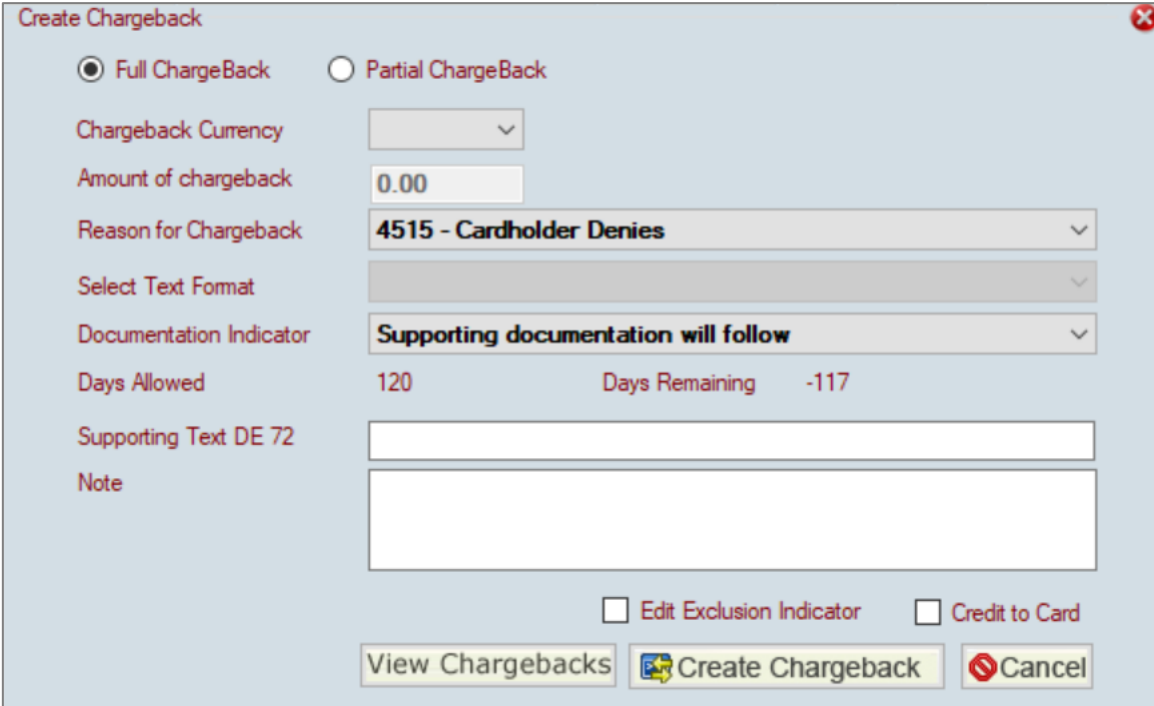

Figure 5: Create a Chargeback

3. To create the chargeback request, click **Create Chargeback**.

   If all the details provided are correct, then a success response is returned from Mastercom.

   If the details provided are not correct, then an error response is returned from Mastercom.

Handling error codes

An error code starting with '1' indicates errors from Mastercom; an error code starting with '5' indicates the error has occurred during GPS processing of chargeback request. You can try fixing the details and resending the chargeback request or contact GPS support.

Table 1: Create Chargeback Options

Option	Description
Full Chargeback	Check this option if you want to dispute the full amount of the transaction. For example, for goods not received or a fraudulent transaction.
Partial Chargeback	Check this option to dispute a part amount of the transaction. For example, cardholder disputes the billing amount.
Chargeback Currency	Select the chargeback currency. Depending on the card region, options include the local card billing currency (e.g. GBP) or the international scheme currency used by the card scheme (e.g. USD). The **Amount of chargeback** field is updated based on the selected currency.
Amount of Chargeback	Enter the chargeback amount. Up to two decimal places are allowed. If the **Full Chargeback** option is checked, this field is disabled, and the full amount taken during the Presentment transaction stage is displayed.
Reason for Chargeback	Select one of the reasons for the chargeback from the drop-down list. For a full list of chargeback reasons, see Chargeback Reason Codes. **Note**: If the reason is fraud related, you must create a SAFE Report *before* issuing the chargeback. [1]
Select text format	The available text format options depend on the **Reason for chargeback** previously selected. Some chargeback reasons do not provide a default text format. If you are unsure as to which format to select, check with your Account Manager. Depending on the selection, this reason is also populated in the **Supporting Text DE 72** field.
Documentation Indicator	Select how documentation to support this chargeback will be supplied: • Supporting documentation is not required • Supporting documentation will follow Refer to the Mastercard Guide for details of the types of Chargeback Reason Codes that require supporting documentation.

Option	Description
Days Allowed	Read-only field indicating the number of days allowed to process the chargeback. This varies between region and chargeback reason code. Typical values are 90 days, 120 days and 540 days.
Days Remaining	Read-only field indicating the number of days remaining to process the chargeback. If this number is negative, it indicates the period in which to submit the chargeback has been exceeded. If you submit the chargeback, Mastercom will reject it.
Supporting Text DE 72	Add a description, to be displayed in the *DE 72* field of the chargeback message sent to Mastercom. This field can also be populated with a standard message as selected in the **Select text format** field.
Note	Free text field to enable you to add an internal note about the chargeback request. This note is not passed on to Mastercom.
Edit Exclusion Indicator	Check this option to indicate to Mastercom they should ignore the *Days Allowed/Days Remaining* indicator. This enables you to still raise a chargeback, even if the Mastercard default eligibility period has expired. [2] **Note**: This functionality is not yet released. Check with your Account Manager for details.
Credit to Card	If you check this option, the chargeback amount will be credited back to the card. [3]

Notes

1) If the reason for raising the chargeback is fraud related, Mastercard require you to first raise a SAFE report to report the fraud before raising the chargeback. See Creating a Mastercom SAFE Report.

2) In some specific circumstances, it may be possible to extend the chargeback validity period for a specific transaction, even if it has expired. For details, check with your issuer.

3) Some Program Managers and issuers prefer to refund the cardholder immediately on raising a chargeback, since the chargeback process can take several weeks or months to complete. Note that raising a chargeback does not necessarily mean that the acquirer or Mastercard will approve the chargeback. You may prefer to wait for confirmation before crediting the cardholder.

5.2. Viewing Chargebacks

Note: Supported for both Mastercard and Visa cards.

1. From the Smart Client menu, select **Card Activity > Chargebacks**.
2. In the **Chargebacks** window, you can view raised chargeback details for a specific card or for all cards:
   a. To query chargebacks for a specific card, in the **Token** field enter the public token number of the card you want to query.
   b. To list chargebacks within a specified date range and status, select the **Status** and date range and click **List**.
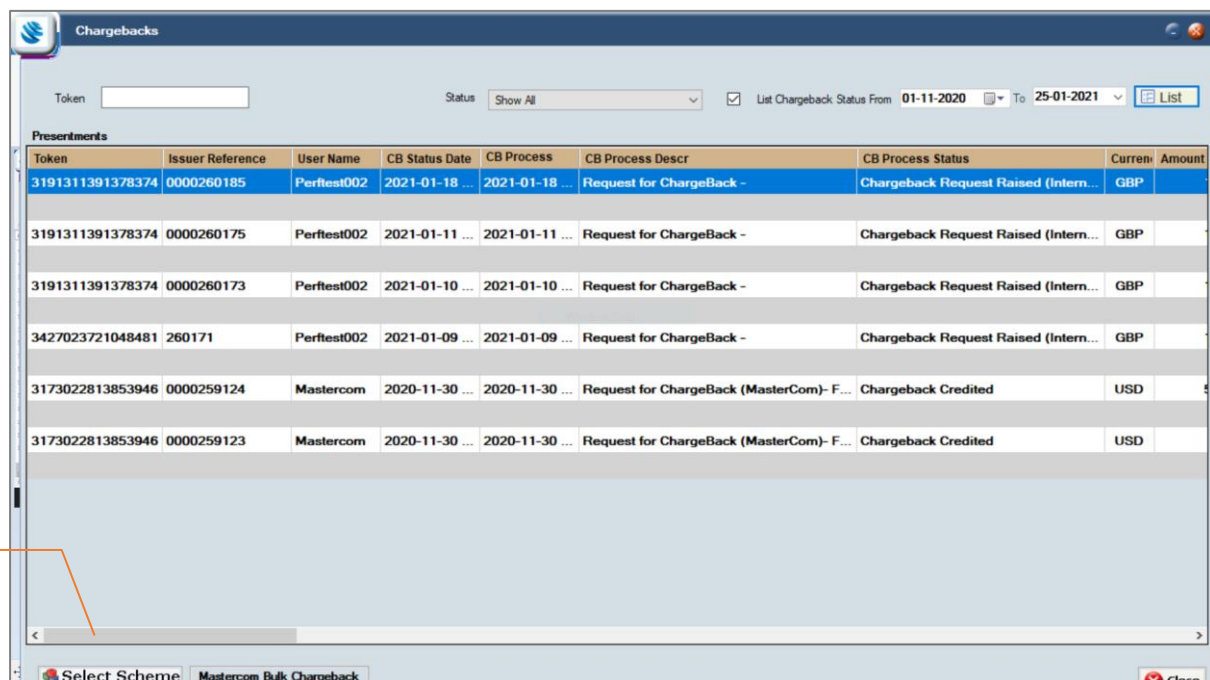

Figure 6: Chargeback Window on Smart Client

3. To view details of the chargeback, use the scrollbar at the bottom-left corner of the window to scroll through the chargeback transaction table.
4. To perform further actions related to the chargeback, right-click the transaction row. The options displayed depend on the type of card and chargeback status. See the examples below:
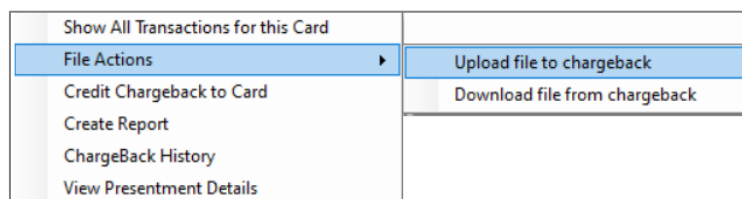

Figure 7: Chargeback File Actions Menu

Tip: To display details for the specific the card issuer scheme used by your programme, click the **Select Scheme** button (Bottom-left of window), click **Clear All** and then check the
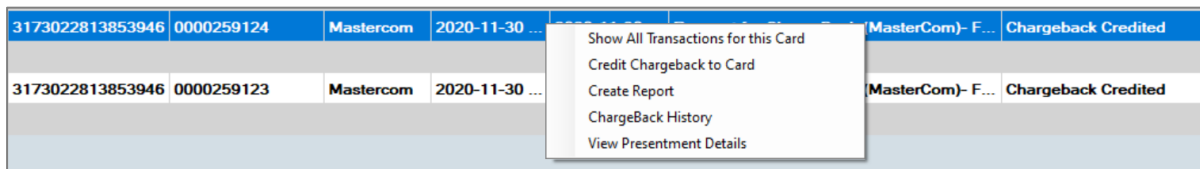
relevant Card Processing Scheme. This option is only relevant if your programme supports multiple card schemes.

5.3. Chargeback Transaction Options

This section provides details of options you can use to view and manage the transaction and card that is linked to a chargeback.

5.3.1. Showing all Transactions for a Card

1. To view all transactions linked to the card, in the **Chargebacks** window, right-click the required transaction and select **Show All Transactions for this Card**.

Figure 8: Transaction Right-Click Menu

2. The **View Transactions** window appears, with the card's public token preselected and displaying a list of transactions linked to the card.

5.3.2. Crediting a Chargeback to a Card

This option enables you to manually credit the charged back amount to the cardholder's account. It is typically used once you have confirmation from the card scheme that the chargeback was successful.

1. To credit the chargeback amount back to the card, in the **Chargebacks** window, right-click the required transaction and select **Credit Chargeback to Card**.
2. A popup message is displayed, asking you to confirm. Click **Yes**.
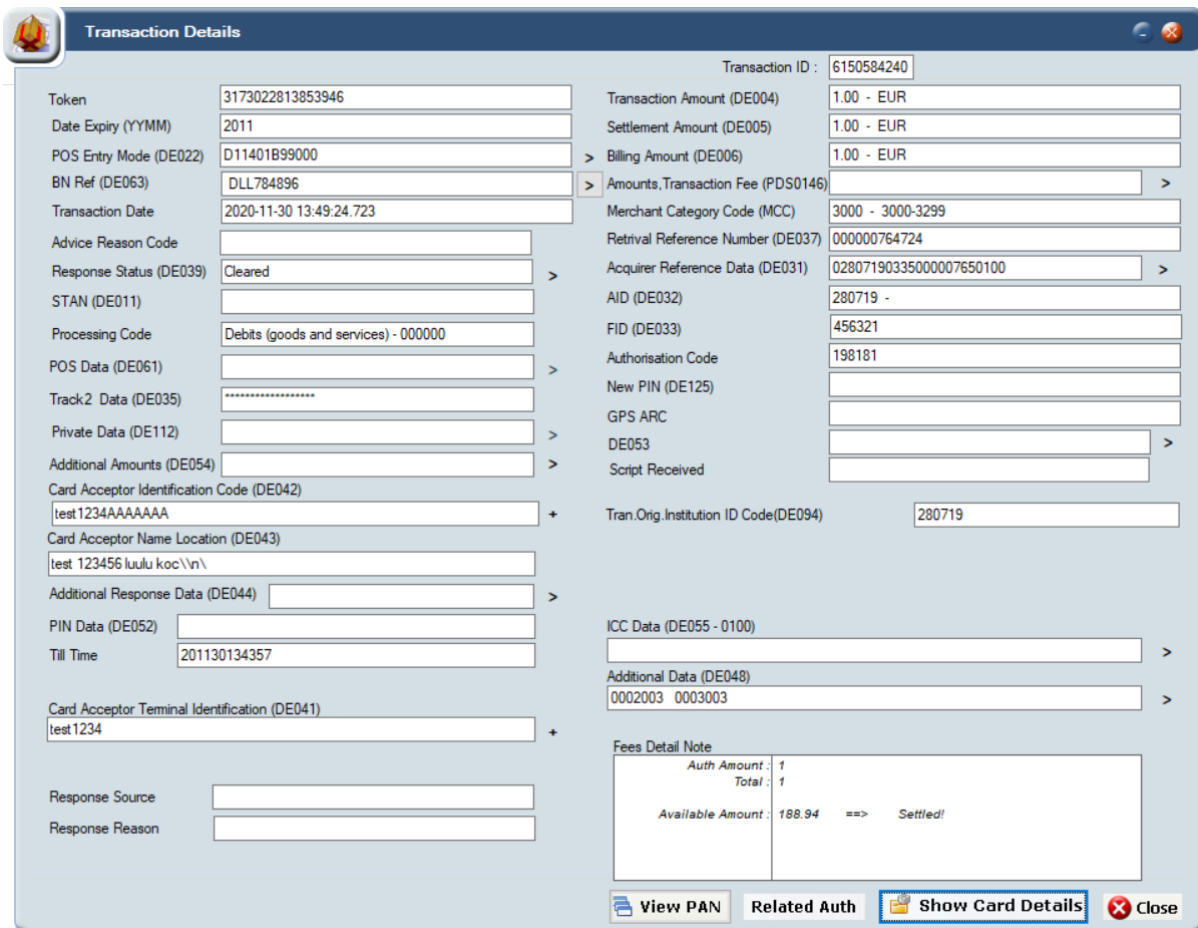   The chargeback amount is credited back to the cardholder's account.

Note: When creating a chargeback, you can also tick the **credit to card** option to automatically credit the card. See Creating a Chargeback.

5.3.3. Viewing Linked Transaction Details

This option enables you to view details of the transaction being charged back.

1. To view further details about the transaction on which you have raised the chargeback, in the **Chargebacks** window, right-click the required transaction and select **Create Report**.

   The **Transaction Details** window is displayed.

Figure 9: Transaction Details Window
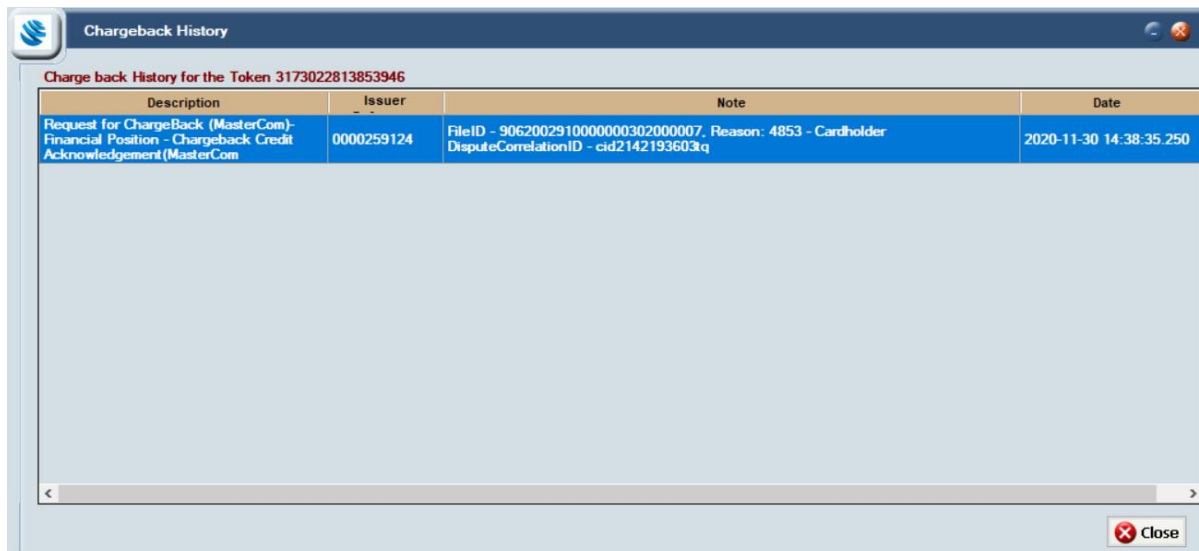
2. Use the buttons at the bottom right of the window to view further details.

Note: Option displayed on this window may vary, depending on your version of Smart Client and the fields enabled for your account.

5.3.4. Viewing Chargeback History

1. To view the Chargeback history of a chargeback transaction, in the **Chargebacks** window, right-click the required transaction and select **Chargeback History**.

   The **Chargeback History** window is displayed.

Figure 10: Chargeback History Window

5.3.5. Viewing Presentment Details

You can use this option to view details of the presentment linked to the chargeback.

1. To view details of the presentment transaction linked to the chargeback, in the **Chargebacks** window, right-click the required transaction and select **View Presentment Details**.

Note: If there is a second presentment, to view details right-click the chargeback and select **View Sec Presentment Details**.

The **View Transactions - Presentments** window is displayed, showing details of the linked presentment transaction.

5.3.6. Creating a Retrieval Request

A retrieval request occurs after a cardholder communicates with their issuer to question or dispute a transaction. You can use Smart Client to create a retrieval request from the acquirer for documentation related to a disputed transaction. The acquirer fulfils a retrieval request by sending documentation through Mastercom.

After receiving the retrieval request documentation from the acquirer, you can proceed with the chargeback if required.

Note: Retrieval requests are optional. You can proceed to create a chargeback even if you have not created a retrieval request.

To raise a retrieval request:

1. In the **Transactions** window, right-click the required transaction and select **Create Retrieval Request**.

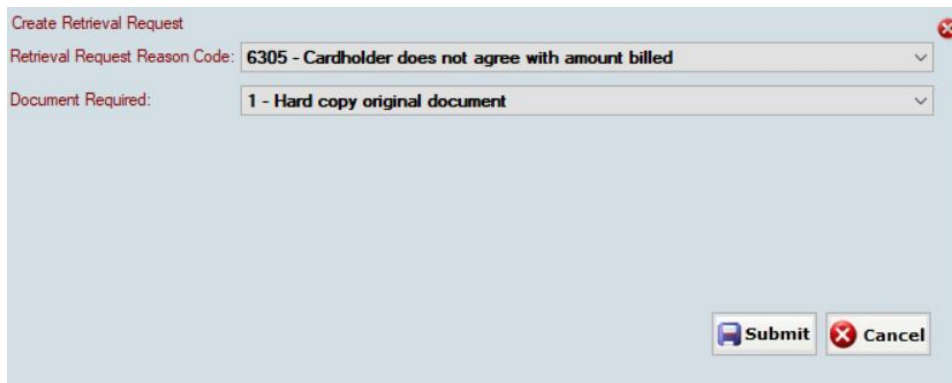The **Create Retrieval Request** window is displayed.

Figure 11: Retrieval Request Window

2. In the **Retrieval Request Reason Code** field, select an appropriate reason for the retrieval request. For details, see *Table 2* below.

3. In the **Document Required** field, select the format required. Options are:
    a. Hard copy of the original document
    b. Copy or image of the original document
    c. Substitute draft

4. Click **Submit**.

    A confirmation message is displayed, indicating if the retrieval request was successfully registered with Mastercom. In this case a *Request ID* and *Claim ID* are returned, which you can use to track the status of the request.

    If the retrieval request failed, a message box is displayed, providing details of the error. For example, a request has already been submitted. Please resolve the error and try again or contact GPS support.

5. To close the message box, click **OK**.

Table 2: Retrieval Request Reason Codes

Codes	Description
6305	Cardholder does not agree with amount billed.
6321	Cardholder does not recognize transaction.
6322	Request Transaction Certificate for a chip transaction.
6323	Cardholder needs information for personal records.
6341	Fraud investigation.
6342	Potential chargeback or compliance documentation is required.
6343	IIAS Audit (for healthcare transactions only).
6390	Identifies a syntax error return.

Tracking the Status of the Request

Once the request has been successfully registered, you can track the status of the request as follows:

- You can view the new retrieval request raised in the **Chargeback** window.
- Once the acquirer responds to the retrieval requests, to download the documentation, right-click the retrieval request in the **Chargeback** window and select **File Actions > Get Documentation**. For details, see Download Chargeback Documentation.

5.3.7. Uploading Chargeback Documentation

You can use this option to upload documentation to support a chargeback. The documents will be sent to Mastercom and made available to the acquirer.

> **Note**: If you subsequently upload another file, this will overwrite any previous file uploaded to Mastercom.

1. To upload supporting documentation for the chargeback, in the **Chargebacks** window, right-click the required transaction and select **File Actions > Upload file to chargeback**.

   The following window is displayed:
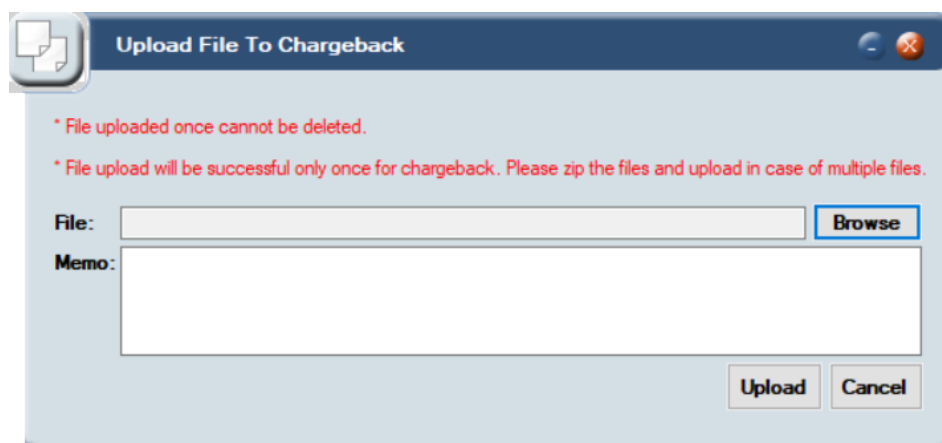
Figure 12: Upload File to Chargeback Window

   If you have multiple files to upload, please add these to a zipped file and upload a single zip file. Examples of files you can include are items such as scanned. documents, images and transaction receipts. Make sure that all documents scanned are clear and legible, and not truncated, or these may be rejected by Mastercard.

> **Note**: You can only upload documentation once (single upload only). Therefore, please ensure you have all the documents you need before using this option.

2. To select a file to upload, click **Browse**.
3. You can use the **Memo** field to provide further details of the file being uploaded.
4. To upload your supporting case documentation to Mastercom, click **Upload**.
   The uploaded file is sent to Mastercom.

> **Notes**:
> Once the file is uploaded, it cannot be deleted. However, you can replace this file with another one using the upload option.
>
> The uploaded file is end-to-end encrypted; GPS does not have access to the details in the file.

5.3.8. Downloading Chargeback Documentation

You can use this option to view any case documentation which you previously submitted to Mastercom.

1. To download documentation linked to the chargeback, in the **Chargebacks** window, right-click the required transaction and select **File Actions > Download file from chargeback**.

   The following window is displayed:
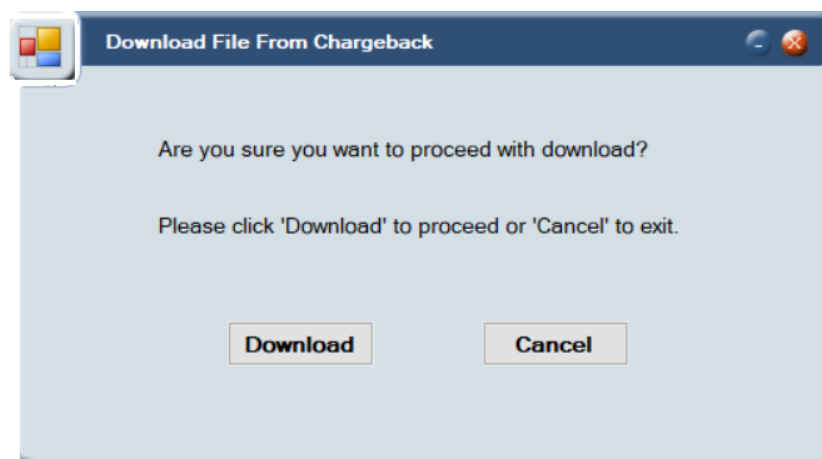
Figure 13: Download File from Chargeback Window

2. To continue with the download, click **Download**.
   The file is downloaded to your computer.

> **Note**: the downloaded file is end-to-end encrypted; GPS does not have access to the details in the file.

5.3.9. Reversing a Chargeback

You can use this option reverse a chargeback that has been previously successfully raised and approved by Mastercard. This can be used if you do not want to proceed with the chargeback.

1. To reverse a chargeback, in the **Chargebacks** window, right-click the required transaction and select **Reverse Chargeback**.
2. A popup message is displayed, asking you to confirm. Click **Yes**.

   A confirmation message is displayed, indicating if the chargeback was successfully reversed or if the chargeback reversal failed.

3. To close the message box, click **OK**.
   A chargeback reversal message is sent to Mastercom.

5.3.10.Re-raising a Chargeback

You can use this option re-raise a chargeback request that has been rejected. You should try and fix the issue before re-raising the chargeback. There is no limit to the number of re-raise chargeback requests.

1. To re-raise a chargeback, in the **Chargebacks** window, right-click the rejected chargeback transaction and select **Re-Raise Chargeback**.

   The following window is displayed:

Figure 14: Re-Raise Chargeback Window

2. Provide all the details as per the instructions in the Creating a Chargeback section and click **Save**.
   The re-raised chargeback requestion is sent to Mastercom. A confirmation message is displayed, indicating if the re-raised chargeback was successful or if the request failed.

5.3.11. Managing Fee Collections

Mastercom supports the ability of issuers to send and receive fee collections related to disputes. For more information about fee collection messages and the fee collection cycle, refer to the Mastercard Global Clearing Management System Reference Manual. (**Note**: you need a Mastercom account to access this link).

To create a fee collection:

1. In the **Transactions** window, right-click the required transaction and select **Create Mastercom fee collection message**.

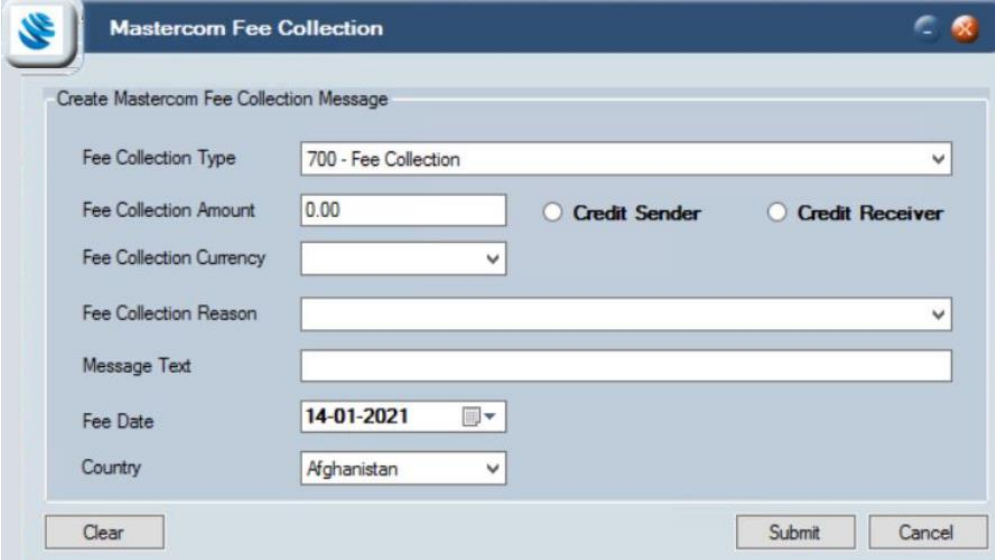   The **Mastercom Fee Collection** window is displayed.

Figure 15: Mastercom Fee Collection Window

2. Provide all the details as per the instructions in *Table 3* below and click **Submit**.

    A confirmation message is displayed, indicating if the Fee collection request was successfully registered with Mastercom. In this case a *Fee ID* and *Claim ID* are returned, which you can use to track the status of the request.

    If the fee collection request failed, a message box is displayed, providing details of the error. For example, a request has already been submitted. Please resolve the error and try again or contact GPS support.

3. To close the message box, click **OK**.
4. The created fee collection message is displayed in the **Chargeback** Window:

| 1133804018876801 | 0000007526 | Perftest002 | 2021-01-14 ... | 2021-01-14 ... | Request for Mastercom fee collection | Fee Collection Request Raised |

    You can view details of any chargeback fees raised in the **Fee Collection** window. See [Viewing Fee Collections](#).

Table 3: Fee Collection Options

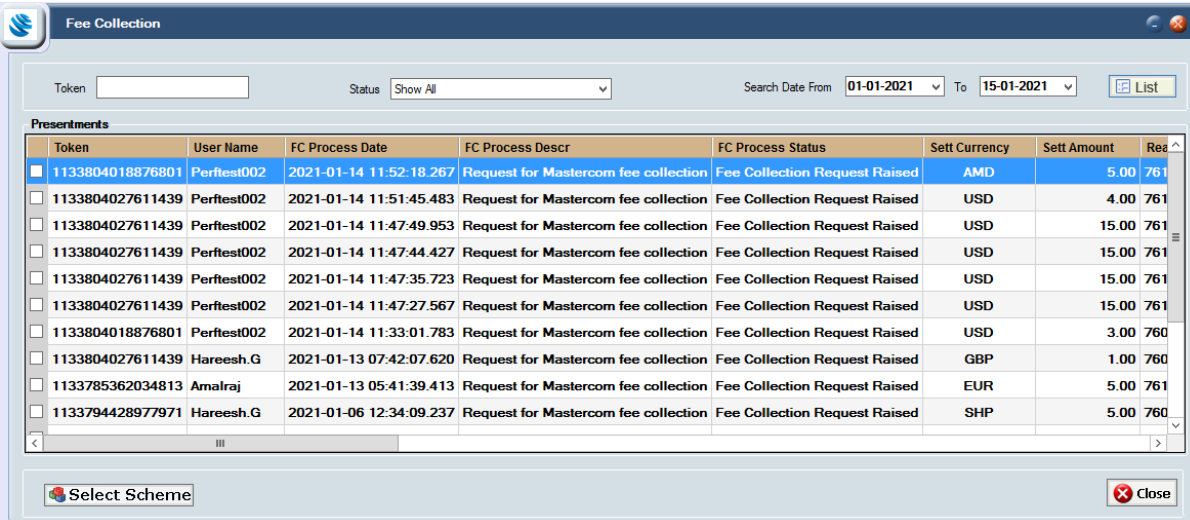| Option	Description
Fee Collection Type	Select the type of fee collection. Options include: • 700 - Fee Collection • 780 - Fee Collection Return • 781 - Fee Collection Return Resubmission • 782 - Fee Collection Arbitration Return
Fee Collection Amount	Enter the fee collection amount. Up to two decimal places are allowed. Tick one of the following options to indicate who to credit the fee to: • **Credit sender** – fee will be credited to your account

Option	Description
	• **Credit receiver** – fee will be credited to the receiver.
Fee Collection Currency	Select the currency of the fee.
Fee Collection Reason	Select the reason for the fee collection (DE 25 Message Reason Code values that apply to the fee collection). For a list, see Fee Collection Reason Codes.
Message Text	Free text field to enable you to add a short message about the fee.
Fee Date	Select the date on which the fee collection is requested.
Country	Select the country where the fee collection applies.

5.3.12.Viewing Fee Collections

This option enables you to view details of all Mastercom fee collection requests.

1. From the Smart Client menu, select **Card Activity > Fee Collection**

   The **Fee Collection** window is displayed.

Figure 16: Fee Collection Window

2. To filter the list of fee collection transactions, enter the transaction **Token** number, select the **Status** and/or select the **Date** range.
3. Click **List**.

5.3.13. Creating a Mastercom SAFE Report

Mastercard require all card issuers to report fraudulent transactions, and you should always do this *before* raising a chargeback in instances where the reason code is related to a fraudulent transaction.

You can report fraudulent transactions to Mastercard by creating a new fraud event in Mastercom, using their SAFE reporting facility (now referred to as the *Mastercard Fraud and Loss Database*).

To create a SAFE report:

1. In the **Transactions** window, right-click the required transaction and select **Create Mastercom SAFE report**.

   The **Create Mastercom SAFE report** window is displayed.
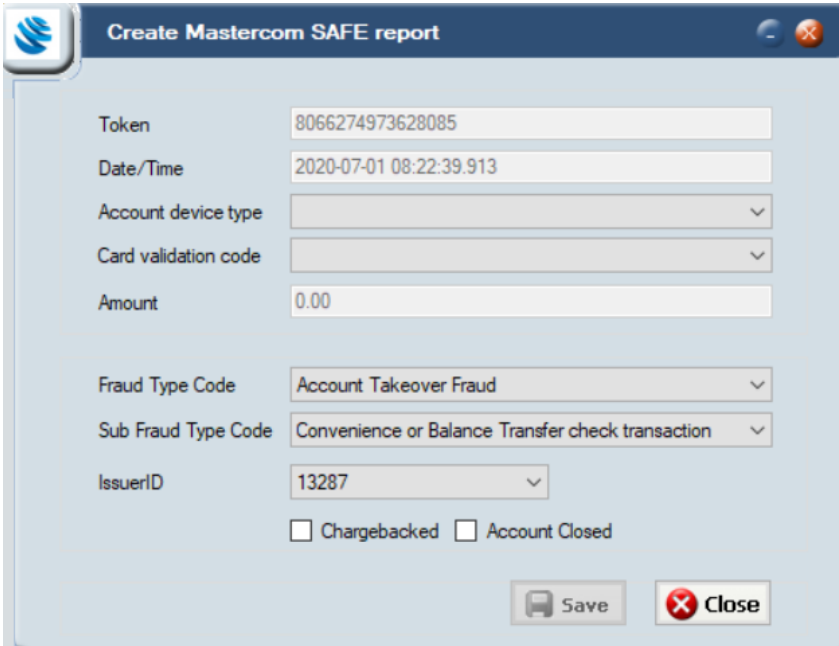
Figure 17: Create Mastercom SAFE Report Window

2. Provide all the details as per the instructions in *Table 4* below and click **Save**.
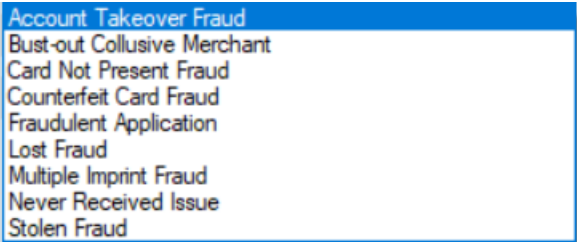
   A confirmation message is displayed, indicating if the SAFE Report request was successfully registered with Mastercom. In this case a *Claim ID* and *Fraud ID* are returned, which you can use to track the status of the request.

   If the SAFE Report request failed, a message box is displayed, providing details of the error. For example, an invalid claim ID. Please resolve the error and try again or contact GPS support.

3. To close the message box, click **OK**.

   The created SAFE message is displayed in the **SAFE Report Details** Window. See Viewing SAFE Report Details.

Table 4: SAFE Report Options

Option	Description
Token	Displays the unique token linked to the card PAN on which the transaction was made.
Date/Time	Displays the date-time stamp of the transaction.
Account device type	Select an option.
Card validation code	Select an option.
Amount	Displays the transaction amount.
Fraud Type Code	Select a fraud type option. Account Takeover Fraud Bust-out Collusive Merchant Card Not Present Fraud Counterfeit Card Fraud Fraudulent Application Lost Fraud Multiple Imprint Fraud Never Received Issue Stolen Fraud
Sub Fraud Type Code	Select a sub-fraud type code. Options include: • Convenience or Balance Transfer check transaction • PIN not used in transaction • PIN used in transaction • Unknown
Issuer ID	Displays the card issuer ID.
Charged Back	Tick this option if the transaction is Charged Back.
Account Closed	Tick this option if the account has been closed.

5.3.14. Viewing SAFE Report Details

This option enables you to view details of all SAFE reports submitted to Mastercom.

1. From the Smart Client menu, select, **Card Activity > Safe Report Details**

   The **Safe Report Details** window is displayed.
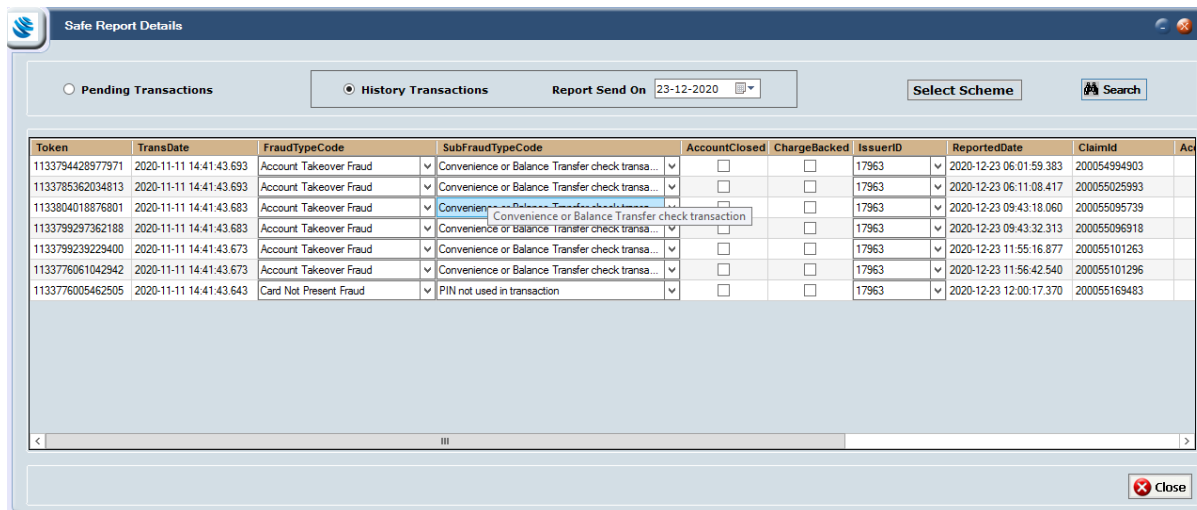
Figure 18: Safe Report Details Window

1. To view only pending transactions, tick the **Pending Transactions** option.

   Alternatively, to filter the list of historical transactions, tick the **History Transactions** option and select the **Date** range.

2. Click **Search**.

5.3.15. Creating Bulk Chargebacks

You can use the Bulk Chargeback CSV template to record details of your chargebacks. Please request a copy of this file from GPS Support. Send the completed file to GPS Support, who will raise the bulk chargeback on your behalf.

Figure 19: Example of a Bulk Chargeback File

For details of the fields in this file, see *Table 5* below.

Table 5: Create Chargeback Options

Option	Description
Token	The unique 9-digit token number for the card being charged back.
ChargebackAmount	The charged back amount. Up to two decimal places are allowed. If the **Full Chargeback** option is checked, this field is

Option	Description
	disabled, and the full amount taken during the [Presentment](#) transaction stage is displayed.
ChargebackCurrency	The three-digit ISO code for the chargeback currency.
ReasonCodeDescription	Reason code for the chargeback. For a full list of chargeback reasons, see [Chargeback Reason Codes](#).
Username	Name of the user who created the chargeback.
Transactionid	The unique token for the transaction being charged back.
IsPartialChargeback	Whether this is a partial chargeback. Enter Y to indicate a partial chargeback amount. For a full chargeback enter N.
IsCreditToCardTransaction	Whether to credit the chargeback amount to the cardholder's account. Y = Yes; N = No.
DocumentIndicator	Whether documentation to support this chargeback will be supplied: Y = yes; N = No. Refer to the Mastercard Guide for details of the types of Chargeback Reason Codes that require supporting documentation.
DE 72	Description, to be displayed in the *DE 72* field of the chargeback message sent to Mastercom. This field can also be populated with a standard message as in the **Select text format** field.

6. How to Reduce the Risks of Chargebacks

Chargebacks are incredibly common. Each year, approximately half of consumers (globally) will initiate a chargeback through their issuing bank. [1]

Chargebacks are expensive and time-consuming to handle, and are a concern for both card issuers, Program Managers and merchants. To help you reduce the incidents of chargebacks, GPS provides a number of options:

- **Merchant Category Code (MCC) Blacklists** – you can add any merchants with high levels of chargebacks or fraudulent transactions to this list, which will prevent your cards being used by these merchants.
- **Card velocity limits and usage limit groups** – you can define limits to the amount, time of day or frequency at which a card is used, as a means to reduce the risks of fraud and chargebacks.
- **3D Secure** – Three Domain Secure (3D Secure) is a card scheme initiative, supported by both Mastercard and Visa, that provides an additional layer of cardholder protection. During an online purchase transaction, the cardholder needs to authenticate by entering a password to their identity. This not only reduces the risks of fraud, but in most instances transfers liability for the transaction to the cardholder. You can use the GPS web services API to implement 3D Secure.

Note: 3D secure checks are only applied to transactions where both the merchant and cardholder are enrolled in this scheme.

- **Out of Band (OOB) authentication** – GPS currently supports OOB authentication types in 3DS V2 (known as Biometrics)
- **Enhanced card security** – GPS enables you to implement two factor authentication and other means to ensure only the legitimate cardholder can use your card.

6.1. More Information

For further details of chargebacks, please contact your account manager.

---

(1) See https://www.chargebackgurus.com/blog/merchant-chargebacks-101-what-they-are-why-they-matter

7. Appendices

7.1. Chargeback Reason Codes

7.1.1. Mastercard Chargeback Reason Codes

The table below is provided for reference only and details are subject to change. For the latest reason codes, always refer to the *Mastercard Chargeback Guide*.

Table 6: Mastercard Chargeback Reason Codes

Code	Description
4515	Cardholder denies.
4522	Authorisation declined.
4801	Requested transaction data not received.
4802	Requested item illegible or missing.
4807	Warning bulletin.
4808	Requested/required authorization not obtained.
4809	Transaction Not Reconciled (European-acquired transactions only)
4812	Account number was not on file.
4831	Transaction amount differs.
4834	Duplicate processing.
4837	Fraudulent transaction; no cardholder authorization.
4840	Fraudulent processing of transaction.
4841	Cancelled recurring transaction.
4842	Late presentment.
4846	Correct transaction currency code was not provided.
4849	Questionable card acceptor activity.
4850	Instalment Transaction Dispute.
4853	Cardholder Dispute Defective/Not as Described.
4854	Cardholder dispute not elsewhere classified (U.S. only).

Code	Description
4855	Non-receipt of merchandise.
4859	Services not rendered.
4860	Credit not processed.
4863	Cardholder does not recognize— Potential fraud.
4870	Chip Liability Shift. Valid for all intraregional transactions (except for excluded regions)
4871	Chip/PIN Liability Shift. (Reserved for intra-Europe and intra-Canada)
4890	Identifies a syntax error return.
4900	General; invalid Second Presentment/1240.
4901	Required documentation not received to support prior Second Presentment/1240.
4902	Documentation received was illegible.
4903	Scanning error– unrelated documents or partial scan.
4905	Invalid Acquirer Reference Data in Second Presentment/1240; no documentation required or provided.
4906	Missing documentation is being supplied.
4907	Other than required/requested documentation provided.
4908	Invalid Acquirer Reference Data in Second Presentment/1240; documentation was received.
4999	Domestic Chargeback Dispute Reserved for intra-European and inter-European use.

7.1.2. Visa Chargeback Reason Codes

The table below is provided for reference only and details are subject to change. For the latest reason codes, always refer to the *Visa Chargeback Guide*.

Table 7: Visa Chargeback Reason Codes

Code	Description
10. Fraud	
10.1	EMV Liability Shift, Counterfeit Fraud.
10.2	EMV Liability Shift, Non-Counterfeit Fraud.
10.3	Other Fraud, Card-Present Environment.
10.4	Other Fraud, Card-Absent Environment.
10.5	Visa Fraud Monitoring Program.
11. Authorisation	
11.1	Card Recovery Bulletin.
11.2	Declined Authorization.
11.3	No Authorization.
12. Processing Errors	
12.1	Late Presentment
12.2	Incorrect Transaction Code
12.3	Incorrect Currency
12.4	Incorrect Transaction Account Number
12.5	Incorrect Transaction Amount
12.6	Duplicate Processing or Paid by Other Means
12.7	Invalid Data
13. Consumer Disputes	
13.1	Services Not Provided or Merchandise Not Received
13.2	Cancelled Recurring Transaction
13.3	Not as Described or Defective Merchandise/Services

Code	Description
13.4	Counterfeit Merchandise
13.5	Misrepresentation of the purchased good and/or service
13.6	Credit Not Processed
13.7	Cancelled Merchandise/Services
13.8	Original Credit Transaction Not Accepted
13.9	Non-Receipt of Cash or Load Transaction Value at ATM

7.2. Mastercard Chargeback Fees

Chargeback fees are reported under the <MasterCardFee> section of the transaction XML file. The Transaction XML is generated daily, around 10 am. This file contains all of the loads, unloads, balance adjustments, cardholder fees and authorisations from the previous 24 hours (midnight to midnight).

For details, refer to the GPS *XML Transactional Data Schema* document.

7.3. Mastercard Fee Collection Reason Codes

The following codes are provided for reference only. For details, please refer to the *Mastercard Chargeback Guide*.

Table 8: Mastercard Fee Collection Reason Codes

Code	Description
7614	Settlement of fulfilment fees other than Mastercom
7622	Handling fee for authorization related chargebacks
7623	Handling fee for authorization related chargebacks
7624	Handling fee for authorization related chargebacks
7627	Failure to provide a merchant advice code in a fee collection
7600	Lost/ stolen telex / phone fee
7601	Recovered card award fee
7602	Emergency cash disbursement
7603	Compliance ruling settlement

Code	Description
7604	Emergency card replacement
7605	Warning bulletin handling fee
7606	Good faith acceptance settlement
7607	Collection letter handling fee
7608	Telex authorization fee
7610	Investigation fee
7611	Retrieval fee reversal
7612	Retrieval handling fee
7616	Warning bulletin handling fee
7617	Adjustment for promotional transactions
7618	Reversal of previously reimbursed State Fuel Tax
7619	Emergency card replacement centre cash advance
7621	ATM Balance Enquiry fee
7625	PIN Management service at ATM
7628	Reclaim surcharge
7629	Non-financial ATM service fee
7700	Intra-currency agreement settlement
7701	Mastercard member settlement of fulfilment fees
7750 to 7799	Bilateral agreement settlement
7800	MCBC Clearing fee
7802	interchange compliance adjustment
7804	ATM transaction settlement
7822	Settlement Adjustment

8. Glossary

This section explains terms used in this document.

Acquirer	The merchant acquirer or bank that offers the merchant a trading account, to enable the merchant to take payments in store or online from cardholders.
Arbitration	Process of managing disputes raised between merchants and cardholders, where the dispute cannot be resolved. The arbitration process is managed by the card scheme, who will make the final decision.
Authorisation	Stage where a merchant requests approval for a card payment by sending a request to the card issuer to check that the card is valid, and that the requested authorisation amount is available on the card. At this stage the funds are not deducted from the card.
Cardholder	Consumer or account holder who is provided with a card to enable them to make purchases.
Card Scheme	Card network, such as MasterCard or Visa, responsible for managing transactions over the network and for arbitration of any disputes.
Chargeback	Where a cardholder disputes a transaction on their account and is unable to resolve directly with the merchant, they can raise a chargeback with their card issuer. The chargeback must be for a legitimate reason, such as goods and services not received, faulty goods, or a fraudulent transaction.
Clearing	Stage in a transaction where the funds authorised on a card are captured (deducted from the cardholder's account). See also Presentment.
EHI	The GPS External Host Interface (EHI) is a system which provides Program Managers with real-time transactional data and control over their transaction authorisations.
Issuer	The card issuer, typically a financial organisation authorised to issue cards. The issuer has a direct relationship with the relevant card scheme.
Merchant	The shop or store providing a product or service that the cardholder is purchasing. A merchant must have a merchant account, provided by their acquirer, in order to trade. Physical stores use a terminal or card reader to request authorisation for transactions. Online sites provide an online shopping basket and use a payment service provider to process their payments.
Merchant Category Code (MCC)	A unique identifier of the merchant, to identity the type of account provided to them by their acquirer.
Out-of-band (OOB) authentication	A type of two-factor authentication that requires a secondary verification method through a separate communication channel along with the typical ID and password.

PCI DSS compliant	The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organisations that handle credit cards from the major card schemes. All merchants who handle customer card data must be compliant with this standard. See: https://www.pcisecuritystandards.org/pci_security/
Presentment	Stage in a transaction where the funds authorised on a card are captured (deducted from the cardholder's account). See also Clearing. Also referred to as the *First presentment*.
Second Presentment	When a merchant resubmits the transaction with evidence to counter the chargeback.
Program Manager	A GPS customer who manages a card program. The program manager can create branded cards, load funds and provide other card or banking services to their end customers.
Representment	Process of responding to a chargeback raised by an issuer, where the acquirer or merchant do not agree with the chargeback and wish to dispute it via the card scheme.
3D Secure	3 Domain Secure is a cardholder authentication scheme provided by the card schemes, which is used to verify the identity of a cardholder during an online transaction. The cardholder typically enters a password or authenticated by submitting a passcode from their mobile device.

Document History

Version	Date	Description	Revised by
1.0	11 February 2021	First version	WS
1.1	07 April 2021	Added new "About this Guide" and "Document History" sections. Section 5.3.3. Should read *Transaction Details* window.	WS
1.1.1	23 June 2021 13 July 2021	Replaced Fraud Type Code figure in *Table 4: SAFE Report Options*. Section 5.3.1 3, SAFE is now referred to as the *Mastercard Fraud and Loss Database*. Step 3 should refer to the SAFE message.	WS