

# Smart Client Guide

Version: 3.1  
10 November 2022

Global Processing Services  
6th Floor, Victoria House, Bloomsbury Square , London WC1B 4DA  
**Support Email:** ops24@globalprocessing.com  
**Support Phone:** +442037409682

For the latest technical documentation, see the [Developer Portal](#).

(c) 2021. Global Processing Services Ltd. 6th Floor, Victoria House, Bloomsbury Square , London WC1B 4DA  
Publication number: SCG-3.1-11/10/2022

# 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.

# 1 About this document

This guide describes the GPS Smart Client portal which is part of the GPS Apex platform.

**Target Audience**

This guide is aimed at users such as Payment Card Administrators, Customer Service Specialists, and Card Fraud Risk Managers.

**What's Changed?**

To find out what's changed since the previous release, see the [Document History](#) section.

## Related Documents

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

Document	Description
<i>Web Services Guide</i>	How to use the Web Services API to integrate your applications to GPS.
<i>External Host Interface (EHI) Guide</i>	How to use the GPS External Host Interface (EHI), and specifications on how to process and respond to messages received from EHI.
<i>3D Secure RDX and Biometric or In-App Authentication Guide</i>	How to use the GPS 3D Secure Realtime Data eXchange (RDX) service and how to implement a 3D Secure project with biometric/In-app authentication.
<i>Fees Guide</i>	How to set up and manage card fees for your card products on the GPS system.
<i>Tokenisation Service Guide</i>	About the Mastercard and Visa token services and how GPS supports tokenisation.

## How to Use this Guide

If you are new to Smart Client and want to understand how you can use it to view and manage your customers' transactions and card usage, begin by reading the following topics: [Overview of Smart Client](#), and [Getting Started with Smart Client](#).

## 2 Overview of Smart Client

This topic introduces Smart Client, describes its key features and components, and explains how you can use it to manage your card programmes.

Smart Client is the user interface for managing your account on the GPS Apex platform. Using the Smart Client portal, you can configure and control your payment programmes in real-time. Smart Client provides a feature-rich dashboard that allows you to view and manage the full lifecycle of your customers' transactions and card usage.

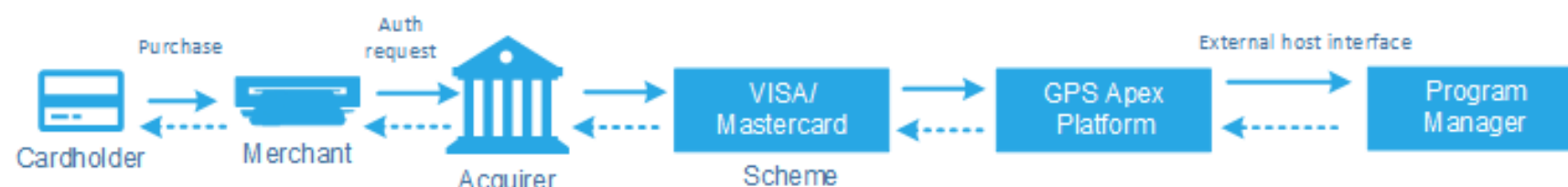
Using Smart Client, you can:

- Display details about card activity, transaction type, and customer interaction
- Drill down into the details of a specific transaction; for example, to view the:
  - Precise Point-of-Sale where a transaction took place
  - Chip settings at the time of transaction
  - Data stored on the chip of an individual card
  - Cardholder verification results
  - Terminal capability
- Allow Customer Service Agents to amend details and take appropriate actions, including:
  - Restoring blocked PINs and sending in-app notifications direct to customers
  - Providing customers with a clear explanation of transaction status
  - Viewing a real-time dashboard on limits and usage
  - Accessing an instant easy-to-understand breakdown of card usage to share with customers
- Manage the entire chargeback lifecycle, including initiating a request and producing chargeback reports
- Use the Case Filing process for dispute management to raise pre-arbitration or arbitration requests to Mastercard
- View information about MDES- and VDEP-enabled cards
- Retrieve cards that have been archived

### 2.1 About the Card Payment Process

To understand what information Smart Client shows and how you can use it to manage your customers' transactions and how a card can be used, you need to know about the card payment process. This topic describes the main concepts, components and processes.

The following diagram shows the key components in the payment flow:



*Figure 1: Parties involved in the payment process*

When a cardholder uses a card to make a purchase, the authorisation request is sent from the merchant terminal to the merchant acquirer, and then to the relevant card scheme. The authorisation request is passed to GPS for authorisation where it is processed according to the card usage rules determined by the Program Manager (card issuer). The payment process is explained in more detail below.

#### Cards

Cards can be either physical or virtual. Physical cards are printed by a manufacturer and sent to the cardholder. Virtual cards are linked to a card image which is displayed to the cardholder. GPS supports the following types of cards:

- Prepaid cards and gift cards – the card is loaded with a prepaid amount available for the cardholder to spend. The card is not permitted to go into a negative balance and you can provide a facility to enable cardholders to load additional funds to the card if required.
- Multi-currency (FX) cards – the card is linked to a multi-currency wallet and enables the cardholder to pay in any desired currency.
- Credit cards – on the GPS platform, there is no distinction between a prepaid and a credit card. If you offer cardholders a credit facility, you will need to have a separate arrangement with them relating to overdraft charges and loading the card with an available funds limit in accordance with the overdraft facility. The GPS card must hold a sufficient balance to enable a card payment.

GPS provides web services (APIs) to create cards.

### Card Usage Groups

Card usage groups are used to control what the cardholder can do with the card, as well as the various card usage fees that are charged to the cardholder.

### Tokens

Tokens enable you to use the GPS platform without needing to store or supply the full 16-digit card primary account number (PAN). Smart Client tokenises card numbers so that sensitive information is not shown. GPS generates two types of tokens:

- 9-digit unique random token, linked to the PAN.
- 16-digit, formed from the 3-digit identifier, plus the 9-digit token, plus the last 4 digits of the PAN.

Both Mastercard and Visa offer a tokenisation service to card issuers. Mastercard offer the Digital Enablement Service (MDES), and Visa the Visa Token Service (VTS) which GPS refers to as the Visa Digital Enablement Program (VDEP). GPS supports both tokenisation services.

### Acquirer

This is the merchant acquirer or bank that offers the merchant a trading account, to enable them to take payments in store or online from cardholders. For example, Worldpay.

### Card Scheme

This is the card network, such as MasterCard or Visa, responsible for managing transactions over the network and for arbitration of any disputes.

### GPS Apex Platform

GPS Apex is a powerful, scalable, multi-currency issuer processing platform that is certified by Mastercard and Visa. GPS Apex supports Chip and PIN (EMV), magstripe, virtual and contactless card processing across prepaid, debit and credit rails. Smart Client is the user interface for the GPS Apex platform.

### External Host Interface (EHI)

The External Host Interface (EHI) offers a way to exchange transactional data between the GPS processing system and the Program Manager's externally hosted systems. All transaction data processed by GPS is transferred to the external host system via EHI in real time.

### Card Transactions

The main transactions that take place on a card are:

- Authorisations. These transactions occur at the stage where a merchant requests approval for a card payment by sending a request to the card issuer to check the card is valid, and the requested authorisation amount is available on the card. Funds are not deducted from the card at this stage.
- Presentments. This is the stage in a transaction where the funds authorised on a card are captured (deducted from the cardholder's account). Also referred to as the *First presentment*.

### Program Manager (Issuer)

A GPS customer who manages a card programme. The Program Manager can create branded cards, load funds and provide other card or banking services to their end customers. Each Program Manager is assigned their own unique issuer code on the system. The card issuer is typically a financial organisation authorised to issue cards. The issuer has a direct relationship with the relevant card scheme.

## 3 Getting Started with Smart Client

This topic provides a high-level overview of the steps to help you get up and running with Smart Client, with pointers to where to find further information.

### Step 1 - Install and launch Smart Client

Smart Client is installed as a desktop application and requires a VPN connection to GPS systems.

- For information about system requirements and installation, see [Installing Smart Client](#).
- For information about launching the application, how to navigate the main screens, and about roles and permissions, see [Launching Smart Client](#).

### Step 2 - Search for a card or transaction

Smart Client provides powerful search functions and filters to help you find specific cards and transactions.

- For information about searching for a specific card, see [Searching for a Card](#).
- For information about searching for transactions, see [Searching for a Transaction](#).

### Step 3 - View card and transaction details

Smart Client provides detailed information about each card and transaction and the ability to drill down deeper. For example, you can view information about a card's status, limits, fees and spending history, or all the transactions made using the card.

- For information about viewing card details, see [Viewing Card Details](#).
- For information about viewing transaction details, see [Viewing Transaction Details](#).

### Step 4 - Manage cards

Depending on your role, you can perform various actions on a specific transaction or token, such as removing an authorisation or adjusting a balance. You can also manage chargebacks and MDES/VDEP-enabled cards.

- For information about managing cards, see [Managing Cards](#).
- For information about viewing, creating and managing chargebacks, see [Managing Chargebacks](#).
- For information about dealing with MDES/VDEP-enabled cards, see [Managing MDES/VDEP cards](#).

## 4 Installing Smart Client

This topic explains how to install the GPS Smart Client application on a computer, and how to access and download the prerequisites you need.

**Note:** Ensure you have a working VPN connection with GPS in place. For more information, contact your GPS Implementation Manager.

### 4.1 System Requirements

To install the GPS Smart Client application, you require a computer running Windows 7 or later.

Before you download and install Smart Client, you need to install the prerequisite software:

- Microsoft .NET Framework 4.5 (x86 and x64)
- Microsoft .NET Framework 4.5 Client Profile (x86 and x64)
- Microsoft Visual Studio 2008 Report Viewer (Or later version)

To install the prerequisite software, follow this link using Internet Explorer or Microsoft Edge: <https://psc7rlo4.globalprocessing.net/smartclient/publish.htm>

To install the User Acceptance Testing (UAT) version of Smart Client, follow this link using Internet Explorer or Microsoft Edge: <https://sc-uat.globalprocessing.net/SmartClient/publish.htm>

**Note:** GPS recommends you use Internet Explorer or Microsoft Edge.



Figure 2: Smart Client application installation screen

1. Click **Download prerequisites** and save the archive to your local drive.
2. Extract the archive and run/open the file *ReportViewer.exe* (Ensure the file is not blocked by antivirus or any other software.)
3. Once the prerequisites are installed, click **Launch** and follow the online instructions to access GPS Smart Client.

## 5 Launching Smart Client

This topic explains how to launch the GPS Smart Client application. Smart Client must be installed, and a working VPN connection with GPS in place. Also explained is how to navigate the main Smart Client screens.

### 5.1 Starting Smart Client

1. To start Smart Client, double click the **Card Processor** desktop icon:



2. When prompted, enter the username and password you received from GPS.

Tip: Leave Auth Code blank.

After entering your login credentials, click **Login** or press the Return key to access Smart Client. The main Smart Client screen appears (this is described in the following section).

### 5.2 About the Smart Client Display



Figure 3: The main Smart Client (Card Processor) screen

The Smart Client portal provides the following main menus and functions:

**Note:** what you can see and do in Smart Client depends on your role and permissions. If you cannot see a menu option, this may be because you do not have the appropriate permissions. For more information, see [About roles and permissions](#).

- **Configure** – Use this to change your password.
- **Card Activity** – View and manage cards and transactions.
- **Help** – View information about the installed Smart Client version and check for the latest updates
- **Exit** – Exit the Smart Client application.

### 5.3 About Roles and Permissions

Different levels of access can be configured on the Smart Client portal, depending on role. For example, some users may only be able to view information about cards and transactions using the portal, while others can view information and make changes.

The figure below shows default roles and permissions, but note that these may differ to the ones configured in your organisation.



Smart Client Default User Roles and Permissions		
Customer Support 1	Customer Support 2	Manager
<b>Configure</b>	<b>Configure</b>	<b>Configure</b>
Change my password	Change my password	Change my password
<b>Card Activity</b>	<b>Card Activity</b>	<b>Card Activity</b>
View Cards	View Cards	View Cards
<b>View Transactions</b>	<b>View Transactions</b>	<b>View Transactions</b>
View Transaction Details	View Transaction Details	View Transaction Details
Change Card Status	Change Card Status	Change Card Status
Activate a Card	Activate a Card	Activate a Card
Tracker History	Tracker History	Tracker History
PIN Services	PIN Services	PIN Services
View Multi-FX cards	View Multi-FX cards	View Multi-FX cards
	Balance Adjustment	Balance Adjustment
	Balance Transfer	Balance Transfer
	Card Unload	Card Unload
	Edit Card Details	Edit Card Details
		Remove Authorisation
		View Chargebacks
		Extend Expiry
		Create Chargeback <sup>1</sup>
<sup>1</sup> Not available for all institutions; subject to Issuer Approval		

Figure 4: Default user roles and permissions

If you cannot see a menu option, this may be because you do not have the appropriate permissions. To make changes to roles or permissions, contact your Smart Client administrator or raise an authorised change request with GPS.

## 5.4 Next Steps

- For information about how to search for a particular card or token, see [Searching for a Card](#).
- For information about how to find a particular transaction and drill down into the details, see [Searching for a Transaction](#).

## 6 Searching for a Card

This topic explains how to find a specific card or token in Smart Client.

Smart Client provides powerful search functions and filters to help you find specific cards and transactions. This is useful if you are trying to locate a card or transaction using only partial information from a cardholder. For example, the customer may not know their card number, but you can search based on their first name, last name and post code.

- To display details about a specific card or token, select **Card Activity** > **View Cards**. The **View Cards** screen appears.
- Use the dropdown search options and filters located along the top of this screen to find cards.

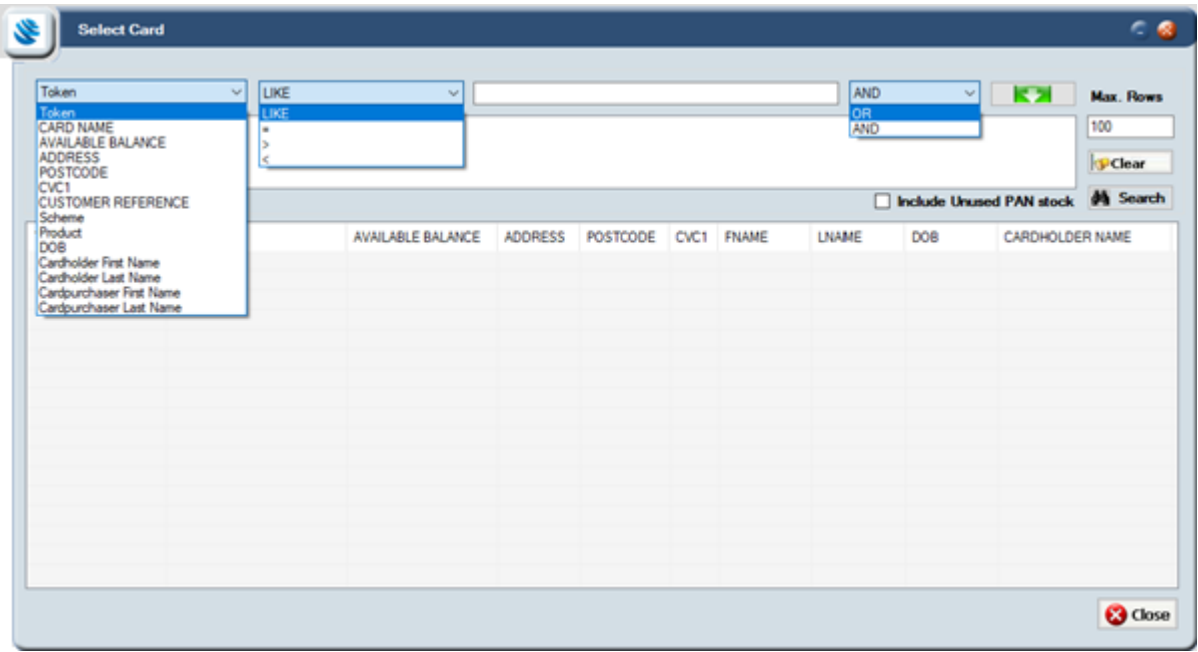


Figure 5: The View Cards screen

### Hints and tips!

- To add multiple parameters (for example, Cardholder First Name, Cardholder Last Name and Postcode) click the green down arrow to add each parameter to your search:



- To clear all selected filters, click **Clear**.
- To configure the maximum number of rows displayed, enter a value in **Max. Rows**. The default is to show 100 rows at a time.

## 6.1 Examples

### Searching for a specific token number

To search for a specific token number:

1. Click **Token** (this is the default)
2. Click **LIKE** and choose = (equals sign) from the dropdown.
3. In the search bar, type the token number you want to search for. You must specify a complete token number; you cannot search for a partial token number.
4. Click **Search**. Smart Client displays the card assigned this token number.

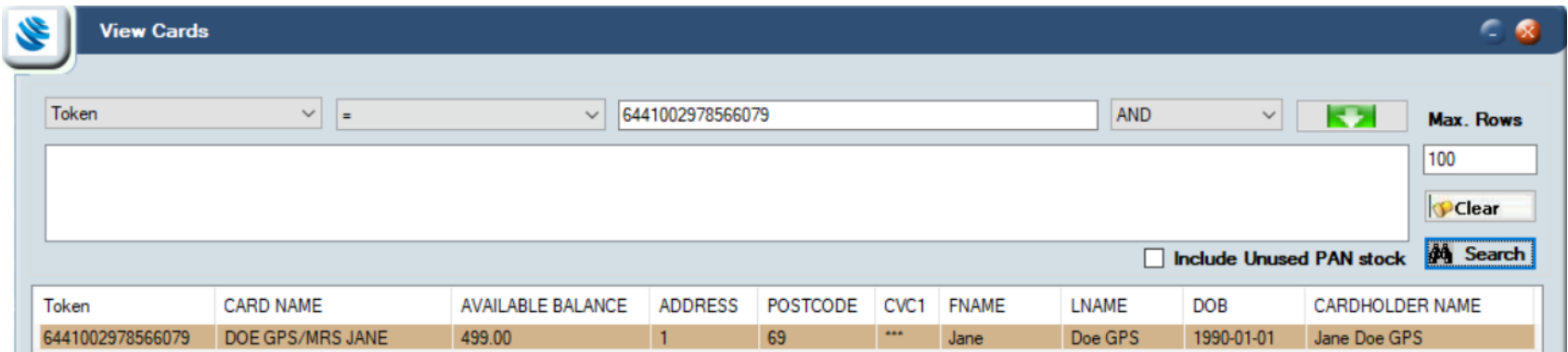


Figure 6: Searching for a token number

Searching based on a card holder’s name and address

To search for cards with a cardholder name similar to 'Jane Doe':

1. Click **Token** and choose **Cardholder First Name** from the dropdown.
2. Click **LIKE** and choose **LIKE** from the dropdown (or to find a specific name, choose = (equals sign) from the dropdown.
3. In the search bar, type the name you want to search for — in this example 'Jane'.
4. Click the green arrow to add this to your search:



5. Repeat this process to add **Cardholder Last Name** to the search.
6. Click **Search**. Smart Client displays a list of all cards matching these parameters.

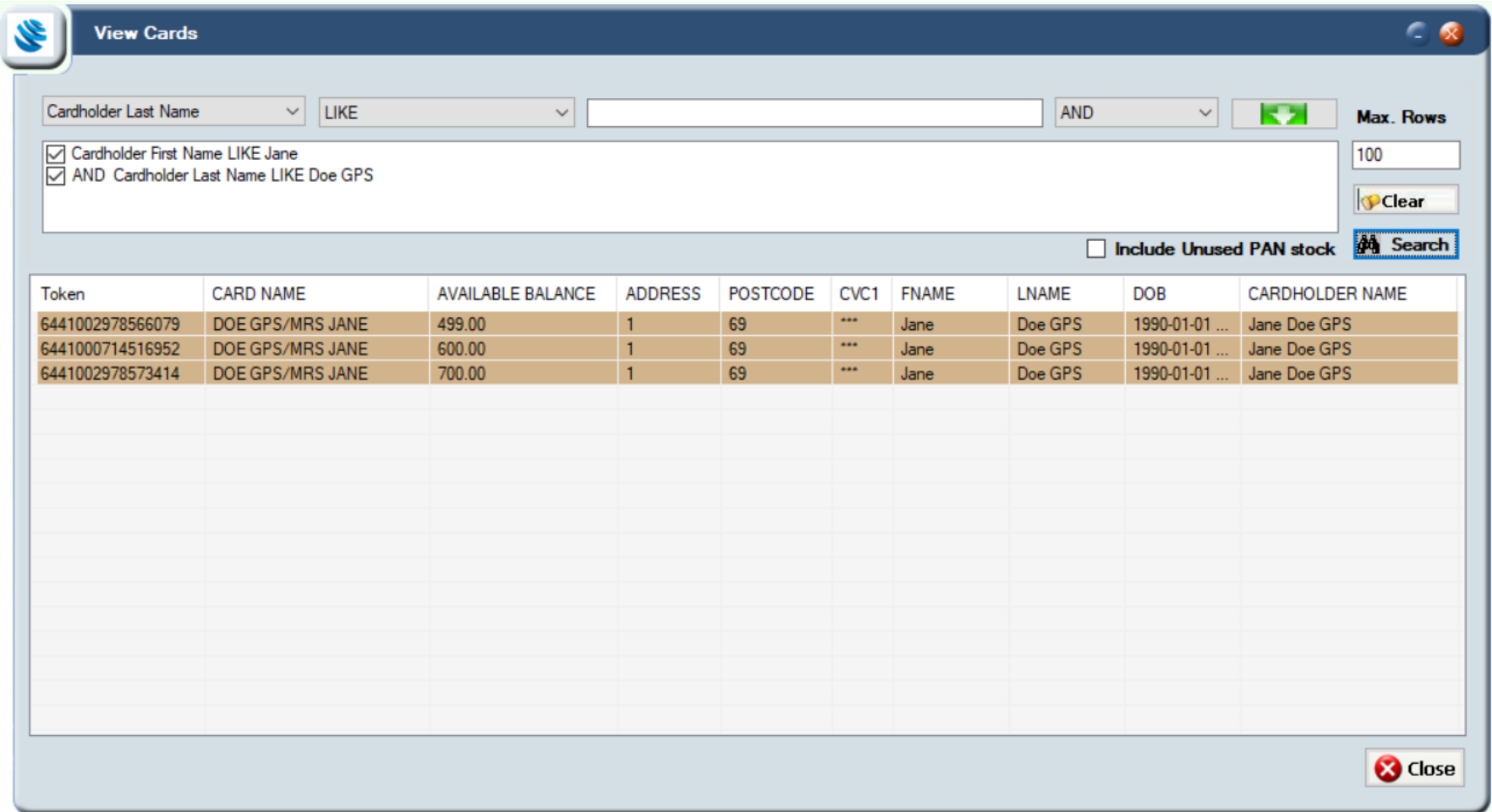
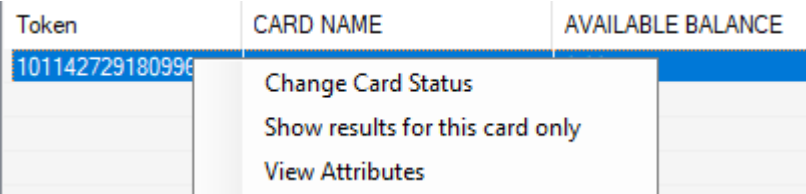


Figure 7: Searching based on a cardholder's name and address

6.2 Next Steps

To see more information about a card, highlight it in the list, and right-click. The following options appear:



- To view and/or change the card status, choose **Change Card Status**. The **Status Change** screen appears. For more information, see [Managing Cards](#).
- To view all transactions associated with this card, choose **Show results for this card only**. The **View Transactions** screen appears. For more information, see [Viewing Transaction Details](#).
- To view more details about the card, such as the card purchaser and holder’s details, choose **View Attributes**. The **Card Master** screen appears. For more information, see [Viewing Card Details](#).

# 7 Searching for a Transaction

This topic explains how to find a specific transaction or list of transactions in Smart Client, and how to search and filter on information.

Smart Client provides powerful and flexible search functions and filters to help you find specific transactions. This is useful when trying to locate a transaction using only partial information from a card holder, such as the approximate date and time that a transaction took place. These options allow you to search:

- For specific types of transactions, such as declined transactions
- For a specific 6-digit BIN
- Based on specific card details, such as token number or card holder’s name, or on transaction details such as location
- Across a range of dates and times

## 7.1 Finding Transactions

- To search for transactions:
1. Select **Card Activity > View Transactions**. The **View Transactions** screen appears.
  2. Use the options displayed along the top of the screen to narrow your search (for example, to display only declined transactions) or select **All** to display all transactions. The different search options are shown below and explained in the table:

☐ Auth Not Cleared☐ Declined☐ Load/UnLoad☐ Chargeback☐ Offline☐ Refund/Fin Rev☐ Auth Advice☐ BIN All Token =

☐ Auth Cleared☐ Reversed☐ Presentment☐ Balance Adjust☐ Expiry☐ Payment☐ Unknown☒ All 7109260169918850

☒ Apply Style

3. After making your selections, click **Search** to display transactions matching your criteria.

The following section explains how to use each of these options to find transactions. See the examples for typical scenarios and for hints and tips to help you make the most of Smart Client’s powerful search functions.

### 7.1.1 Searching for transaction types

You can search for specific types of transactions by selecting the following options:

Transaction type	Description
<b>Auth Not Cleared</b>	An authorisation that has not cleared (GPS has not yet received a presentment that can be matched to the authorisation on the token). If GPS does not receive a presentment that can be linked to the authorisation, GPS reverses the authorisation automatically after the hanging auth filter period has expired (as specified by the client for the product). For standard authorisations this is typically 7 days. It is usually longer (up to 30 days) for merchants using pre-authorisations, including but not limited to Car Hire and Hotels.
<b>Auth Cleared</b>	An authorisation which has cleared (GPS has received a presentment that could be matched to the authorisation).
<b>Declined</b>	A transaction that has been declined. To find the decline reason, scroll right to the notes field of the transaction to see the reason for the decline. For a list of the most common decline reasons, see <a href="#">Appendix A: Common Decline Reasons</a> .
<b>Reversed</b>	An authorisation that was reversed. To find the reversal reason, right click the reversal and choose <b>More details &gt; View transaction details</b> . See the <b>Response Status (DE039)</b> . There are various reasons for a reversal, including: Customer Cancellation, Wrong Format, Manual Reversal, Issuer Time-Out. For a full list of reasons, refer to the <i>Mastercard Customer Interface Specification</i> or <i>Visa Base</i> manual.
<b>Load/Unload</b>	Load and unload Web Service (funds paid in; for example, via a load channel such as a retailer e.g. PayPoint in the UK, Ireland or Romania, or unloaded by the Program Manager).
<b>Presentment</b>	A transaction for authorisations that require settlement. First presentment occurs when the merchant sends a request to take either part or all of the amount previously authorised on the card.
<b>Chargeback</b>	Presentments that have gone through the chargeback process. For more information, see <a href="#">Managing Chargebacks</a> .
<b>Balance Adjust</b>	An adjustment to the balance or the blocked amount. This can be a Credit or a Debit.
<b>Offline</b>	Offline transactions occur when a presentment is received without a matching authorisation. This can happen in situations where an authorisation is not possible (for example, a transaction on a plane where there is no internet connection).

Transaction type	Description
<b>Expiry</b>	Transaction Expiry, response 54 'Expired Card' (Process – Debits Unload).
<b>Refund/ Fin Rev</b>	Presentment returning funds to the Card Holder/ Financial Reversal – Process (Credits for Refund).
<b>Payment</b>	Payment originating from non-card network entity, paying funds into or out of the customer account (for example, Faster Payments, BACS, Direct Debits via Agency Banking).
<b>Auth Advice</b>	A system generated message about the transaction. This message is for information only (typically from Visa or Mastercard) and has no effect on the transaction. For example, it may note a slow response time.
<b>Unknown</b>	Card not found: Unknown Card. In large volumes this can indicate a BIN attack. For information, see <a href="#">FAQs</a>

### 7.1.2 Searching for a BIN

Use the BIN dropdown box to search for transactions with a specific 6-digit BIN. You can search for a single BIN at a time.

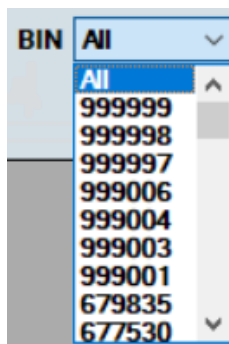


Figure 8: BIN dropdown box

### 7.1.3 Searching using other details

Use the dropdown box labelled **Token** (the default) to search using other card and transaction details.

You can filter your search further using the dropdown box to the right and specifying a search value. You can search on PANs, Public tokens (including 9 digit and 16-digit tokens). When you enter a PAN number and select search, Smart Client automatically converts it to the 16-digit token.

Select from the following list:

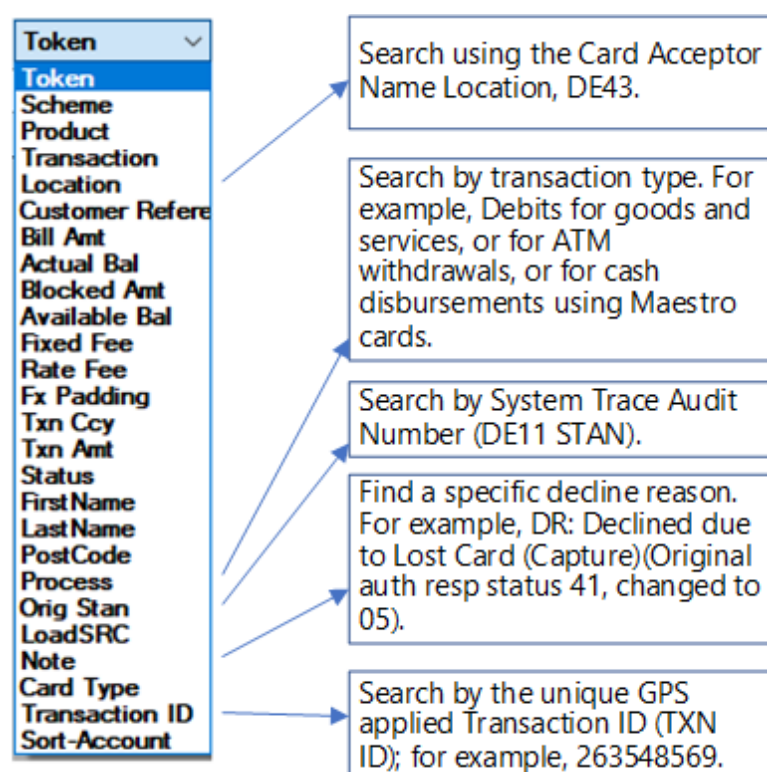


Figure 9: Search options available from the dropdown box beneath Token

### 7.1.4 Searching based on date and time

Use the date and time filters to search for transactions that occurred on a specific date and time. By default, today's date is shown.

You can also narrow your search to a specific time or range (for example, if a customer reports that a transaction happened around lunchtime).

Date

26-05-2021

10:00:00

☒

To

26-05-2021

11:59:59

### 7.1.5 Setting default search options

You can tailor your default search parameters so that your current selections are used in future.

To set your current search parameters as the default:

- Click the arrow to the right of **Search** and choose **Set Ticked as Default**.

## 7.2 Example

### 7.2.1 Show all transactions for a specific day

To see all transactions that occurred on a specific day:

- Select **All**.
- In **Date**, specify the date (by default, today's date is shown). To search across a date range, select **To** and specify the date. The range you can search across depends on the type of search — it may be one day or up to 180.

**Tip:** To narrow your search further to a specific time or range, specify the time; for example:

Date

26-05-2021

10:00:00

☒

To

26-05-2021

11:59:59

## 7.3 Next Steps

For information about interpreting the results displayed in the **View Transactions** screen and the colour-coding used, see [Viewing Transaction Details](#).

After finding the transaction(s) you want to examine, you can explore further details; for example, to discover why a transaction was declined. For more information about how to drill down deeper into transaction details, see [Examining a transaction in detail](#).



# 8 Viewing Transaction Details

This topic describes how to display a list of transactions using the **View Transactions** screen, and how to drill down deeper into the transaction details.

To display the **View Transactions** screen:

- From the main Smart Client menu, select **Card Activity > View Transactions**.

The **View Transactions** screen appears. For information about how to search for transactions, see [Searching for a Transaction](#).

## 8.1 Understanding the Display

The **View Transactions** screen provides a wealth of information about each transaction and the ability to drill down into the details (described later). This section explains what information is displayed and the colour-coding used to highlight the different types of transaction.

The results of your search appear in colour-coded rows. The colours are explained in the key at the bottom of the screen. When an option at the top of the screen is selected, only those types of transactions are displayed; for example, Auth Not Cleared, Declined.

Use the scroll bar at the bottom of the screen to view all the fields.

**Tip:** You can sort the list (for example, by date or transaction type) by clicking on the column headers and using the up and down arrows to sort in ascending or descending order.



Figure 10: The View Transactions screen

The following information is shown for each transaction:

**Note:** the information displayed depends on the type of transaction; for example, more information is shown about authorisations than about presentments.

Column	Description
<b>Token</b>	Unique GPS 9-digit token assigned to this card.
<b>Scheme</b>	Card network responsible for managing the transaction.
<b>Product</b>	Specific card network's product.
<b>Date</b>	Date and time the transaction occurred. The time relates to GPS time; for example, GMT.
<b>Location</b>	Location provided by the merchant.
<b>Transaction</b>	Type of transaction, such as authorisation, balance adjustment, presentment, auth reversal etc.
<b>Status</b>	Transaction status, such as Settled.
<b>T Ccy</b>	Transaction currency.
<b>Tx Amt</b>	Transaction amount (in the transaction currency).
<b>Bill Amt</b>	Bill amount (in the currency of the card).
<b>Act Bal</b>	Actual balance.
<b>Blk Amt</b>	Blocked amount (pending payments).
<b>Avl Bal</b>	Available balance.

Column	Description
F Fee	Fixed fees levied against the transaction.
R Fee	Rate-based fee. Fees levied against the transaction based on a percentage charge.
Fx Pdg	Financial padding (to allow for currency fluctuations)
MCC Pdg	Financial padding applied to transactions in specific MCCs (typically used for hotels and rental cars where cardholders might be charged a little more than authorised for).
Process	Transaction process; for example, recurring fees, balance inquiry.
Orig Stan	6-digit number STAN number used to link the authorisation and the presentment.
Customer ref	An alphanumeric identifier unique to the cardholder which is different to the GPS token.
Notes	Information about the transaction, such as why a decline has happened.

Tip: The **Notes** field is a useful source of information about a transaction, particularly for declines, as it can point you to what has happened. For example, in the case of a decline, an incorrect PIN or the transaction exceeding the maximum permitted limit. Scroll right on the **View Transactions** screen to display it.

## 8.2 Examining a Transaction in Detail

This section explains how to drill down deeper into the details of a specific transaction.

To display more details about a particular transaction:

- Highlight it in the **View Transactions** screen, then right-click. The following options appear:

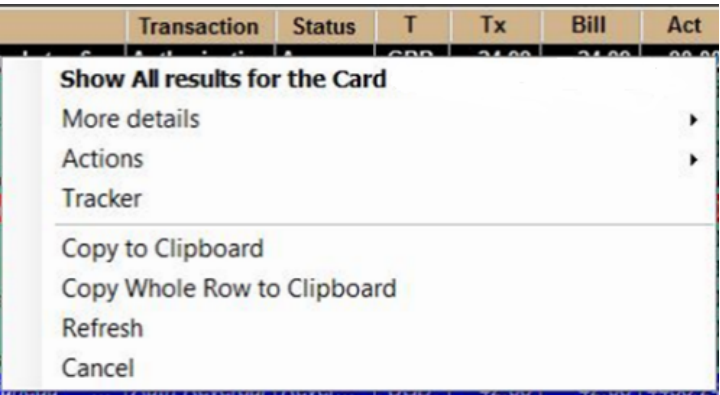


Figure 11: Further options available in the View Transactions screen

These options are explained in the following section.

Tip: Use the **Copy to Clipboard** and **Copy Whole Row to Clipboard** options to copy information about the transaction. This is useful, for example, to copy a token number across screens.

### 8.2.1 Viewing all transactions for the card

To display a list of all the transactions for this particular token:

- Choose **Show All results for the Card**.

Tip: You can also double-click on a transaction to display all the results.

### 8.2.2 Viewing transaction details

To display detailed information about a transaction:



1. Highlight the transaction, right-click and choose **More details**. Further options appear.

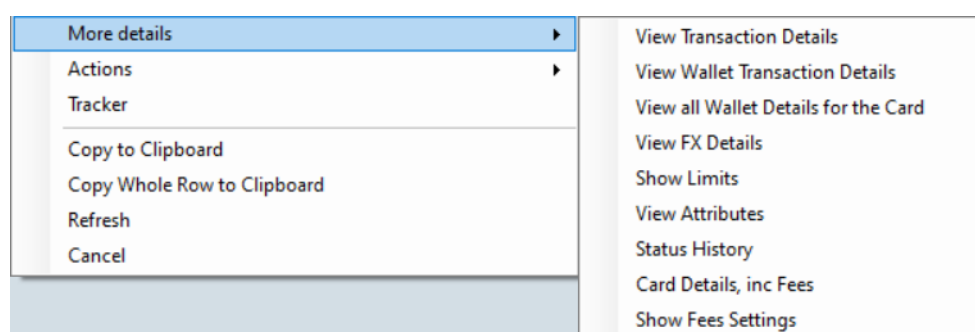


Figure 12: More details options available from the View Transactions screen

2. Select **View Transaction Details**.

The **Transaction Details** screen shows detailed information about the transaction, including the transaction date, status, card acceptor name location, transaction amount and fees.

The example below shows details for an authorisation:

**Note:** The details shown depend on the type of transaction; for example, fields relating to presentments, such as Settlement Amount (DE005), are blank for authorisations.

#### About the Transaction Details screen

The following section explains the main transaction information shown:

**Tip:** DE000–DE999 refers to the Data Element number (for example, DE004 = Transaction Amount). For a full list of Data Elements and their definitions, see the *Mastercard Customer Interface Specification* or *Visa Base* manual.

Click the arrow available next to some fields to display more information; for example, POS data (DE061).

Field	Description
<b>Message Type</b>	The type of transaction, such as an authorisation or presentment.

Field	Description
<b>Token</b>	The unique token number associated with the transaction.
<b>Date Expiry</b>	The expiry date provided at the time of the transaction (useful to check in case the cardholder has entered an incorrect expiry date).
<b>POS entry mode (DE022)</b>	How the transaction was created; for example, contactless at a machine, ecommerce, online, ATM. ICC indicates the card was physically inserted into a machine and the PIN entered.
<b>Response status (DE039)</b>	The status sent back to the merchant; for example, 05 - do not honour. Click the arrow next to this field to see more information.
<b>STAN (DE011)</b>	System Trace Audit Number. This links the authorisation and presentment (note this number is not unique).
<b>Processing code</b>	Indicates the type of transaction; for example, a debit.
<b>POS data (DE061)</b>	Useful information about the machine on which the transaction took place. Click the arrow next to this field to see more information; for example, if the card is in card capture status.
<b>Card Acceptor Identification Code (DE042)</b>	Code relating to the specific Point of Sale (POS) terminal.
<b>Card Acceptor Name Location (DE043)</b>	Merchant's details.
<b>Till Time</b>	Time provided by the merchant (can be incorrect but matches what is on the receipt).
<b>Transaction ID</b>	Useful identifier for tracing a specific transaction and narrowing a search.
<b>Transaction Amount (DE004)</b>	Transaction amount and currency.
<b>Settlement Amount (DE005)</b>	Settlement amount and currency.
<b>Billing Amount (DE006)</b>	Amount applied to the account in the currency of the card.
<b>Merchant Category Code (MCC)</b>	Code that describes a merchant's primary business activities.
<b>Retrieval Reference Number (DE037)</b>	A unique reference to the transaction assigned by the acquirer. All messages related to the same transaction (reversals, presentments, chargebacks) should have the same RRN; however, this may not be enforced.
<b>Request Time</b>	The time when GPS receives this authorisation, in the local timezone of the GPS servers.
<b>Response Time</b>	The time when GPS sends the response (the difference between the request and response times is shown below in milliseconds), in the local timezone of the GPS servers. Note that the response time in milliseconds is the time for the <i>entire</i> transaction to complete across all parties.
<b>ICC Data (DE055 - 0100)</b>	Data from the card's chip. Click the arrow next to this field to see more information; for example, you can check whether the online and offline PINs were verified when making a transaction.
<b>Additional data (DE048)</b>	Information about 3D Secure (payer authentication) for online transactions. Click the arrow next to this field to see more information. For more information, see <a href="#">Viewing 3D Secure details</a> .
<b>Fee Detail Note</b>	Shows any fees applied to this transaction.

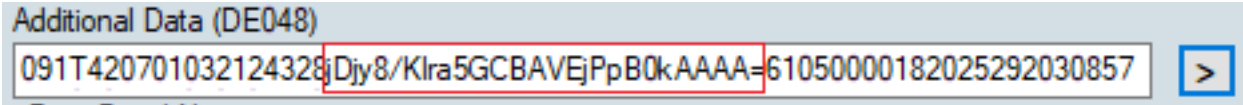
### 8.2.3 Viewing 3D Secure details


3D Secure is a set of online protocols created by the different card networks to improve the level of security in card-not-present (CNP) transactions. Branded with different names, including 3D Secure, Mastercard ID Check, Verified by Visa, and 3DS, 3D Secure provides additional protection when making ecommerce transactions. By default, authentication is biometric ('in client app' authentication), with fallback authentication set to 'OTPSMS', where a one-time passcode (OTP) is sent to the cardholder via SMS. For more information, see the *3D Secure Guide RDX and Biometric or In-App Authentication Guide*.

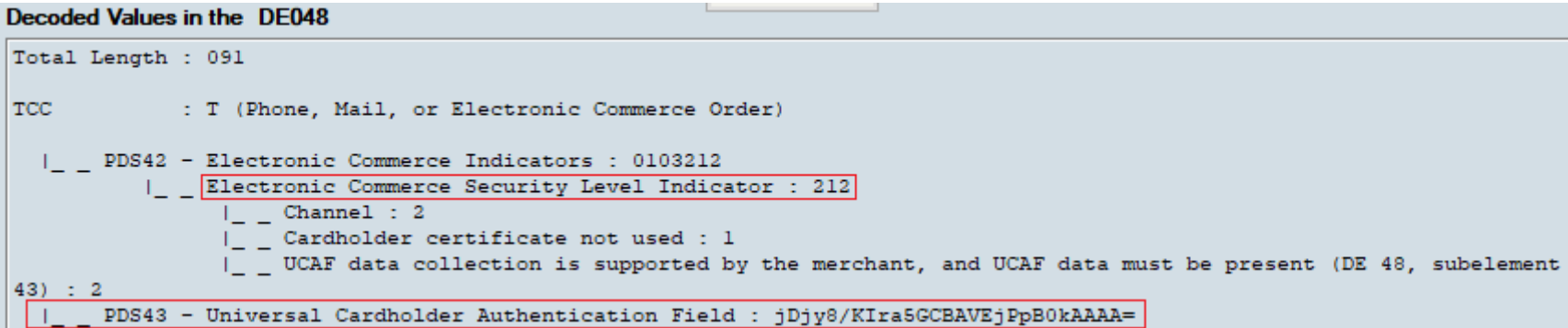
#### Viewing Mastercard 3D Secure transactions

To see information about a Mastercard 3D Secure transaction:

1. In the **View Transactions** screen, right click the transaction and select **View Transaction Details**.
2. In the **Transaction Details** screen, inspect the **Additional Data (DE048)** field (bottom right).



3. Click the arrow  to expand the information displayed. For example:



Note the following:

- **PDS42** contains Electronic Commerce Indicators (ECI) results.
- For non-3D Secure transactions such as eCommerce merchants who are not enrolled or have disabled the checks, these display as 'UCAF data collection is not supported by the Merchant'.
- **PDS43** contains the Accountholder Authentication Value (AAV). The results are provided by the 3D Secure Provider to the Merchant/Acquirer and are submitted within the Authorisation request.


Tip: EHI Data also provides 3D Secure Authentication results containing AAV data; for example:  
><cavv>jDjy8/KIra5GCBAVEjPpB0kAAAA=</cavv>< For more information, see the *External Host Interface (EHI) Guide*.

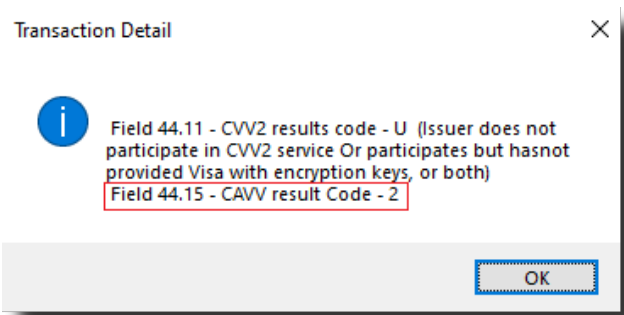
Viewing Visa 3D Secure transactions

To see information about a Visa 3D Secure transaction:

1. In the **View Transactions** screen, right click the transaction and select **View Transaction Details**.
2. In the **Transaction Details** screen, inspect the **Additional Response Data (DE044)** field (bottom left).



3. Click the arrow  to expand the information displayed. For example:



Note: **Field 44.15** – GPS Received Cardholder Authentication Verification Value (CAVV)

Tip: EHI Data also provides 3D Secure Authentication results containing AAV data; for example: ><cavv>AAABBBQ5KVc-glogDBDkpEFQKZyo==</cavv>< For more information, see the *External Host Interface (EHI) Guide*.

## 9 Viewing Card Details

This topic explains how to view more information about cards and how to drill down into the details. You can access card details either through the **View Cards** screen or the **Transaction Details** screen. To view card details:

1. Select **Card Activity > View Transactions** . Search for a transaction (for information, see [Searching for a Transaction](#)):
2. Highlight the transaction, right-click and choose **More details > View Transaction Details**.
3. Click the **Show Card Details** button (bottom of screen). The **Card General Details** screen shows information about the card associated with this transaction.
4. Click the **Show Card Attributes** button (bottom of screen). The **Card Master** screen appears showing details about the card-holder and card purchaser for this token.

**Tip:** You can also display the **Card Master** screen by right clicking on a transaction and choosing **More Details > View Attributes**.

–OR–

1. Select **Card Activity > View Cards**. Search for a card (for information, see: [Searching for a Card](#)).
2. From the **View Cards** screen, highlight the card in the list, right-click and choose **View Attributes**. The **Card Master** screen appears.

The screenshot shows the 'Card Master' window. At the top, the title bar says 'Card Master'. Below it, there's a 'Cards' tab. The main area is divided into several sections. On the left, there's a 'Token' field with the value '6441002978566079'. Next to it is the 'FileName' field with the value 'GPSINSTITUTIONTEST\_GPSVISA\_6\_45726'. To the right of that are 'Issued Up' (22-07-2021) and 'Actual Balance' (499.00). Below these are two columns: 'Card Purchaser' and 'Card Holder'. Each column has fields for First Name, Last Name, Address1, Address2, PostCode, and Country. The 'Card Purchaser' fields are filled with 'Jane', 'Doe GPS', '1', 'London Road', 'SS6 9EE', and 'United Kingdom'. The 'Card Holder' fields are also filled with the same information. To the right of these columns are fields for 'File Generated On' (2021-07-22 21:47:41.480), 'Status' (00 - All Good), and 'Centre Name'. Below these are several dropdown menus: 'Card Acceptor List', 'Card Disallow List', 'Group Web', 'Card FX Group', 'Calendar Group', 'Card Linkage', 'Group Usage' (set to 'GPS PHYSICAL USAGE TEST'), 'Group MCC', 'Group Limit' (set to 'GPS LIMITS GBP TEST'), 'Group Auth', 'Limited Network', and 'Rec Fee'. At the bottom, there are fields for 'Adv Permission' (00000000 00000000 00000000 00000000 00000100), 'Scheme' (GPS SCHEME TEST), 'Product' (GPS PRODUCT TEST VISA GBP L), 'Currency' (GBP), 'Customer Ref', 'Passcode' (636746), 'Activation Date' (2021-07-22 14:05:49.180), 'GPS Expiry' (2022-06-30 00:00:00.000), 'IsLiveDate' (2021-04-14 18:01:29.067), 'Primary' (6441002978566079), and '3D Secure VDE's Valid' (N/A). A '( Byte 5 -> Byte 1 )' button is also present. A 'Close' button is in the bottom right corner.

Figure 13: The Card Master screen

The following section explains the main card information shown:

- **Card Purchaser** — name and address of card purchaser. This may differ to the cardholder if the card was purchased by a company but is used by an employee.

**Note:** If an alternative address has been submitted via Web Services – for example, by including ‘dlv’ (Delivery Address) values such as the TAG <dlvaddr1> for Ws\_CreateCard Web Service – this information appears here. For more details, see the *Web Services Guide*.

- **Card Holder** — name and address of the person in possession of the card. The cardholder address reflects the Address Verification Service (AVS) checks that are performed.

**Note:** Records can be amended using Web Services (Ws\_Update\_Cardholder\_Details). For more details, see the *Web Services Guide*.

Note the following fields in the top right of the screen which are useful:



- **Actual Balance** — current card balance
- **File Generated On** — date the token was created
- **Status** — card status code and description; for example, 00 - All Good. For more information, see [Appendix B: Card Status Codes](#).

The following fields in the bottom left of the screen are also useful:

- **Activation Date** — date the card was activated (if blank, the card isn't activated yet)
- **GPS Expiry** — card expiry date held on the GPS platform

The fields in the right-hand pane relate to the rules governing card acceptance. These are known as Usage Rules which you can set to control card acceptance. For example, you can prevent a card from being used on gambling sites by disallowing specific Merchant Category Codes (MCC). For information about the usage rules and card acceptance methods, see [Appendix C: Usage Groups](#).

## 9.1 Viewing the Card Limits Graph

You can get an 'at a glance' view of the daily and cumulative limits in place for a card or an account, as per the product configuration, using the **Limit Graph**. This graph also shows the frequency of the card's use, cumulative cash withdrawal, load, payments in, payments out, and POS (Point of Sale) spend amounts for the specified period of time. For more information about the limits set on a card, see [Viewing card limits](#).

**Tip:** The **Limit Graph** is useful to understand when spend limits are being reached or how much is still available to use.

To view the **Limit Graph** screen:

1. From the **View Transactions** screen, highlight a transaction in the list, right-click and choose **More details**.
  2. Choose **Show Limits**. The **Limit Graph** appears.
- The following example shows the data by day, every 31 days and 365 days. The cumulative time periods are configurable.

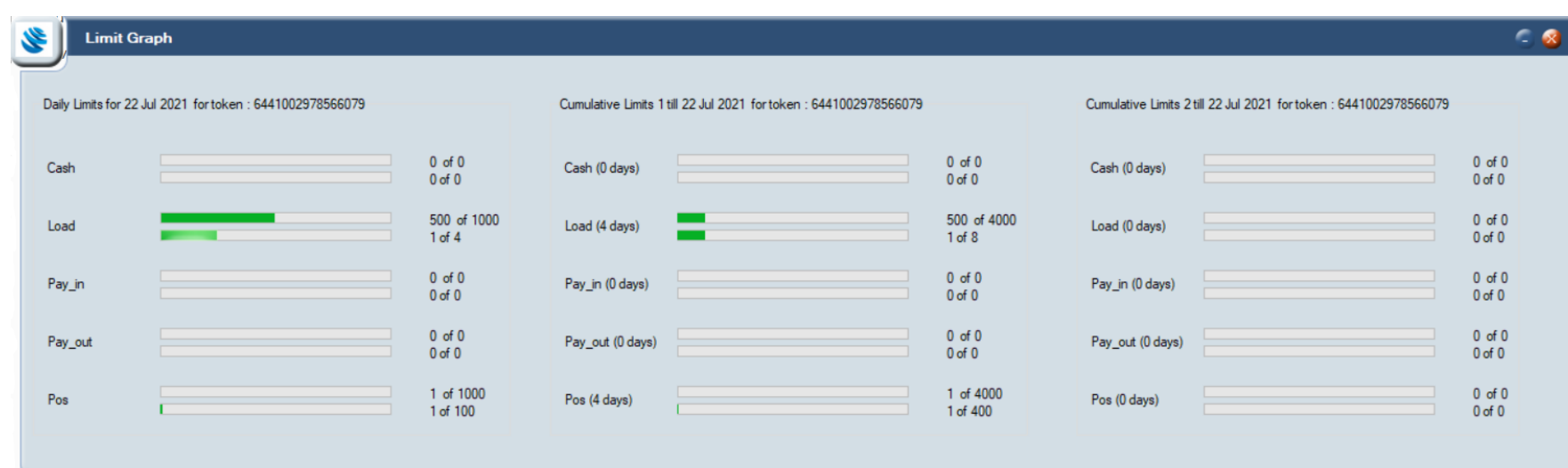


Figure 14: The Card Limits Graph

The limits are based on the **Group Limit** settings in the **Card Master** screen. Click the arrow next to **Group Limit** to see the limits configured.

For example:

The screenshot displays the 'Group Limit Settings' window. It features a 'Group Limit' dropdown menu, a 'Max Balance' input field set to 25000.00, and a warning message: 'The following limits are denominated in the billing currency of the card to which they apply. To omit a limit enter 0.' Below this is a table with 13 columns: SI, Process, Max Per Tran, Min Per Tran, Daily Limit, Daily Frequency, Accum Limit1, Accum Frequency1, Accum Period1, Accum Limit2, Accum Frequency2, and Accum Period2. The table lists limits for CASH, LOAD, PAY\_IN, PAY\_OUT, and POS.

SI	Process	Max Per Tran	Min Per Tran	Daily Limit	Daily Frequency	Accum Limit1	Accum Frequency1	Accum Period1	Accum Limit2	Accum Frequency2	Accum Period2
1	CASH	250.00	10	250.00	25.00	1000.00	100	30	12000.00	1200	365
2	LOAD	0.00	0	0.00	0.00	0.00	0	0	0.00	0	0
3	PAY_IN	3750.00	0	3750.00	50.00	25000.00	300	30	60000.00	3600	365
4	PAY_OUT	3750.00	1	3750.00	50.00	25000.00	300	30	60000.00	3600	365
5	POS	5000.00	0	5000.00	50.00	5000.00	300	30	60000.00	3600	365

Figure 15: The Group Limit Settings screen showing an example of typical limits

## 9.2 Viewing Card Status History

Using the **Card Status History** screen, you can see a history of the activities carried out on the card, such as balance adjustments and loads.

To view a card’s status history:

1. From the **View Transactions** screen, highlight a transaction in the list, right-click and choose **More details**.
2. Choose **Status History**. The **Card Status History** screen appears.

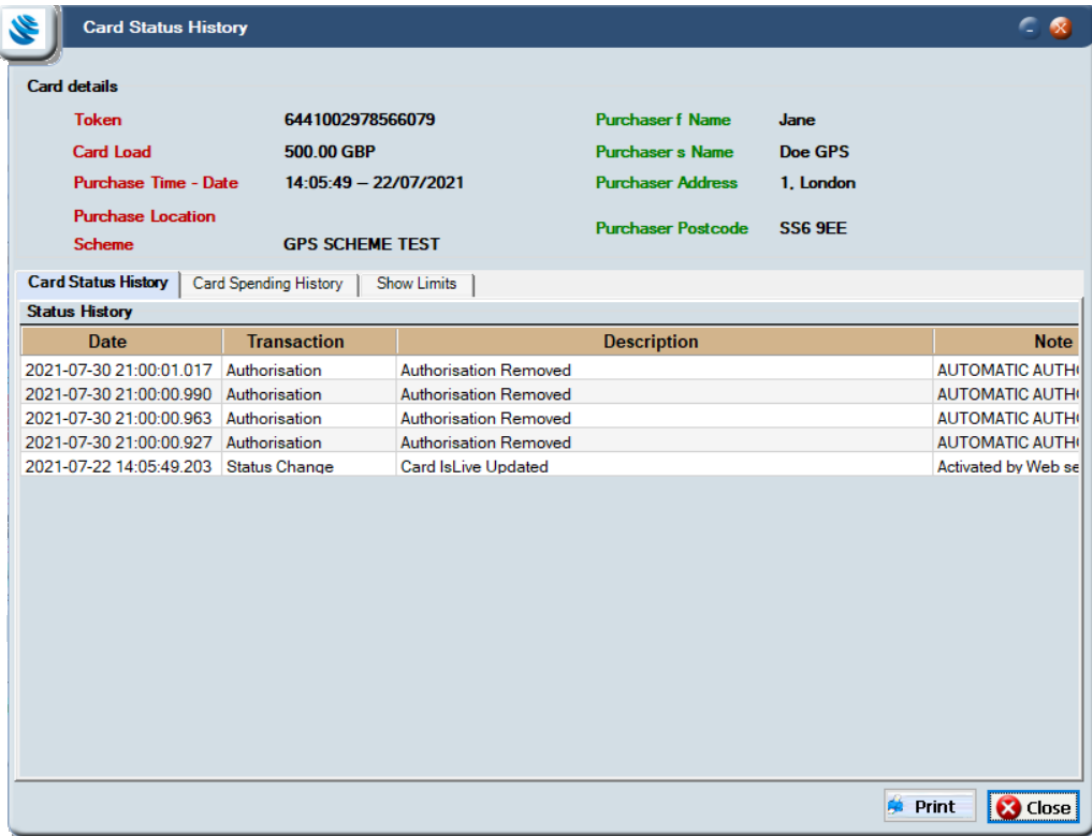


Figure 16: The Card Status History screen

There are three tabs: **Card Status History**, **Card Spending History** and **Show Limits**.  
By default, the **Card Status History** tab appears, showing a history of card activity.

Tip: The **Notes** field displays useful information about activity - you can adjust the column widths to see it. You can also sort the list (for example in date order) by clicking on the column headers and using the up and down arrows to sort in ascending or descending order.

The other tabs are described below.

### 9.2.1 Viewing spending history

To view the spending history of a card:

- From the **Card Status History** screen, click the **Card Spending History** tab. A history of spending activity appears.

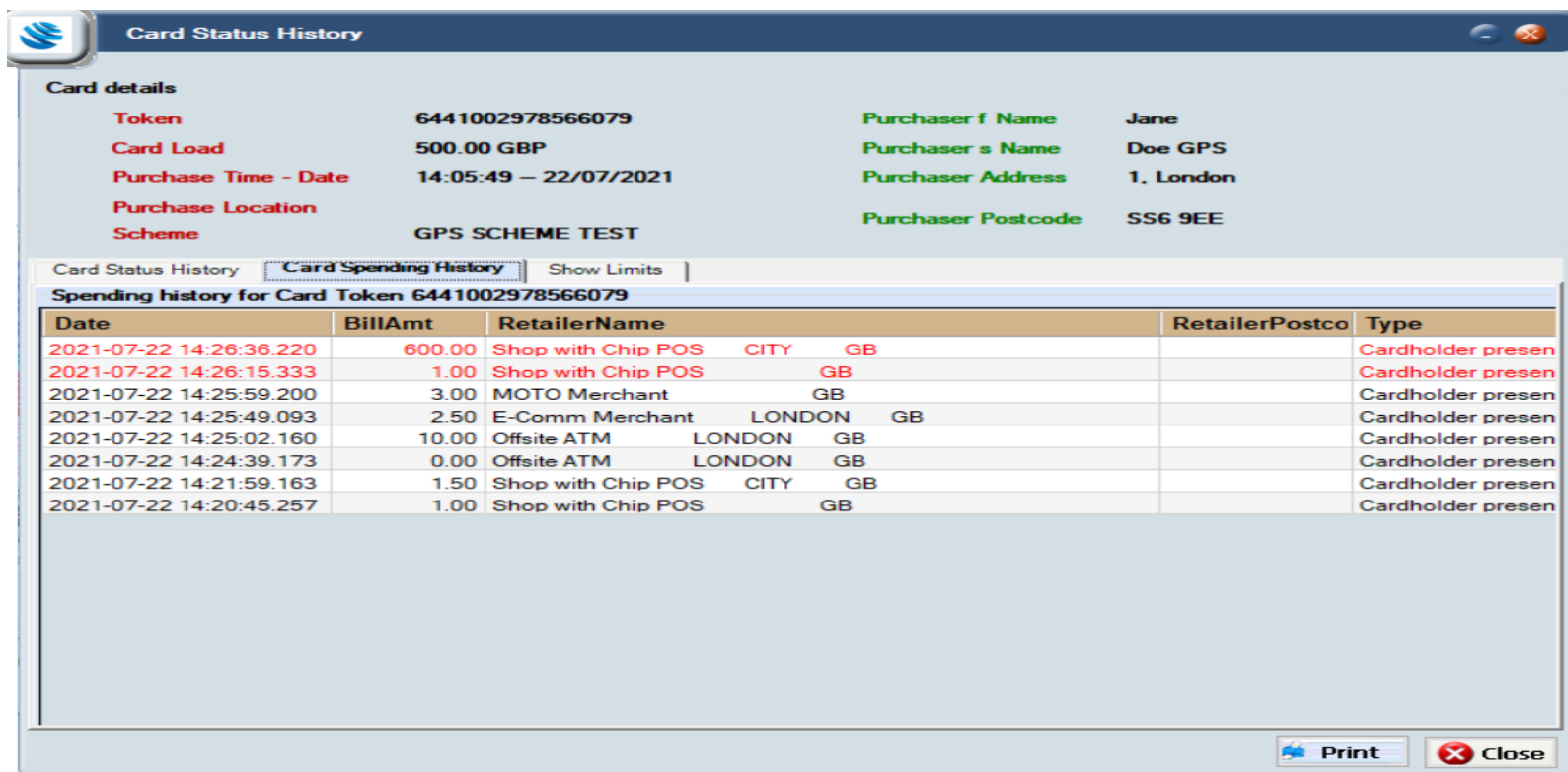


Figure 17: The Card Spending History tab on the Card Status History screen

## 9.2.2 Viewing card limits

You can view the limits that are applied to a card, such as limits on cash withdrawals, the number of times a cardholder can use an ATM or load their card.

To view card limits:

- From the **Card Status History** screen, click the **Show Limits** tab. Daily and accumulated limits for the card are shown together with the transactions and amounts contributing to these limits.

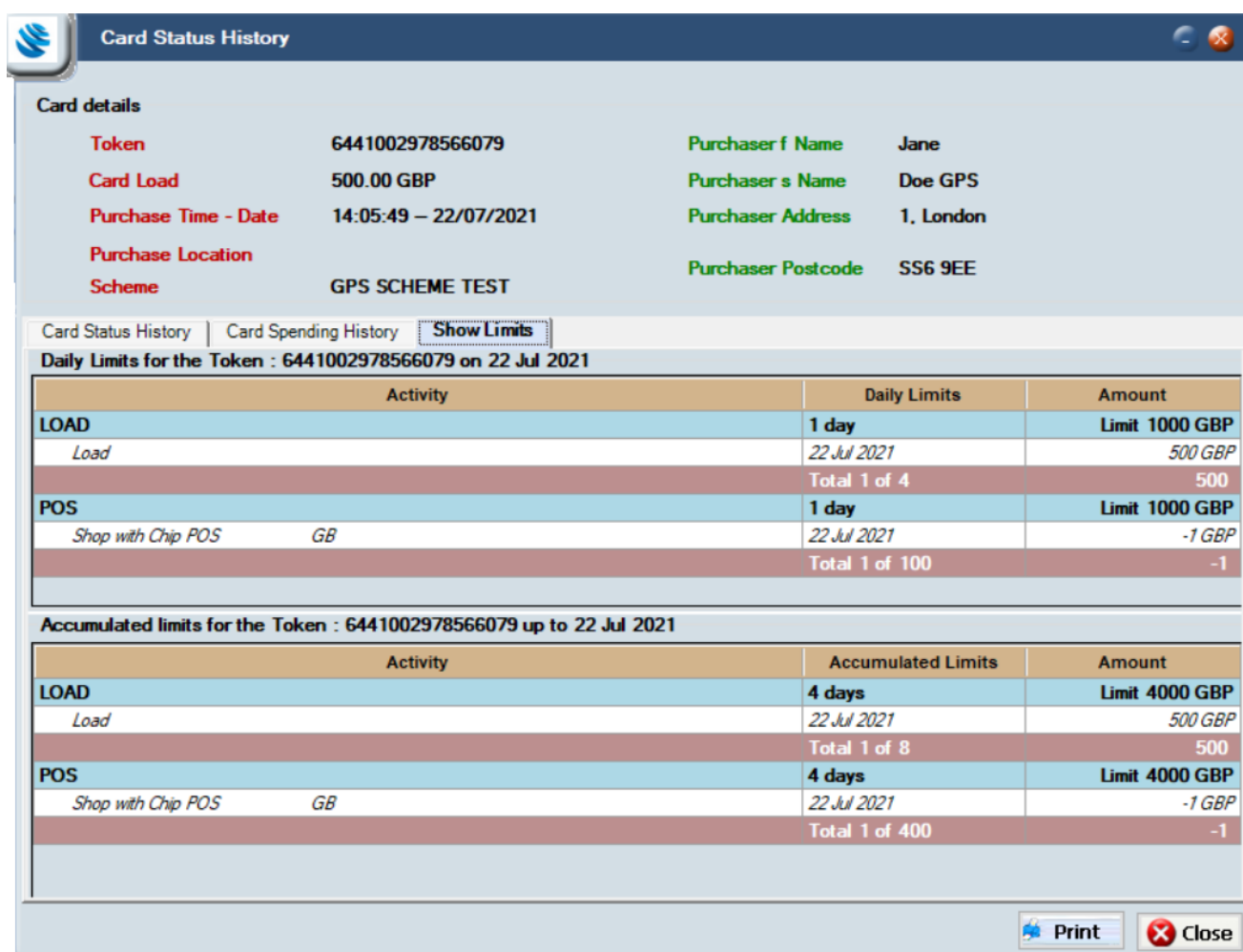


Figure 18: The Show Limits tab on the Card Status History screen

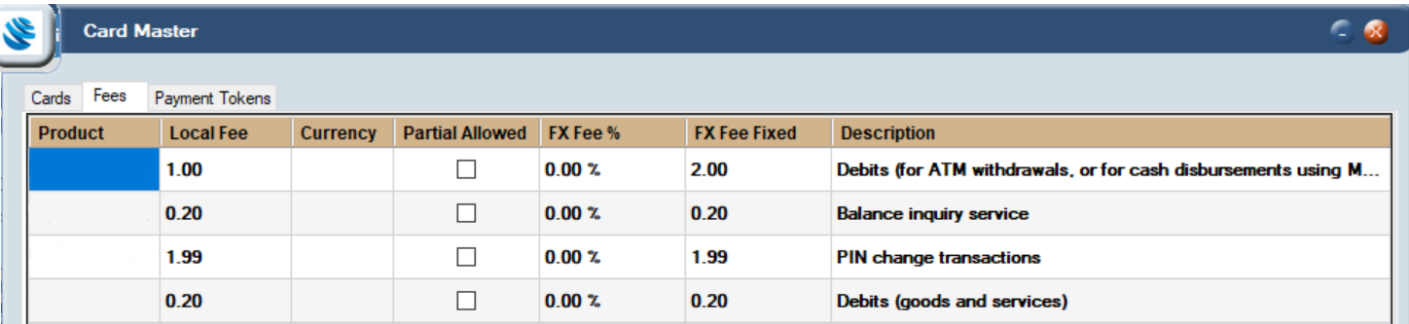
### 9.3 Viewing Card Fees and Fee Settings

You can see the fees associated with a card, which were configured during product set up. For example, you can see the domestic and non-domestic fees that apply when the card is used at home and abroad. For more information on fee setup, see the *GPS Fees Guide*.

**Note:** Fees can only be altered using a Change Request. You cannot update fees using Smart Client. Contact your GPS Account Manager for more information.

To view card fees and settings:

- 1. From the **View Transactions** screen, highlight a transaction in the list, right-click and choose **More details**.
- 2. Choose **Card Details inc Fees**. The **Card Master** screen appears with two additional tabs (for more information about the details shown in the **Card Master** screen, see: [Viewing Card Details](#)).
- 3. Click the **Fees** tab.



Product	Local Fee	Currency	Partial Allowed	FX Fee %	FX Fee Fixed	Description
	1.00		<input type="checkbox"/>	0.00 %	2.00	Debits (for ATM withdrawals, or for cash disbursements using M...
	0.20		<input type="checkbox"/>	0.00 %	0.20	Balance inquiry service
	1.99		<input type="checkbox"/>	0.00 %	1.99	PIN change transactions
	0.20		<input type="checkbox"/>	0.00 %	0.20	Debits (goods and services)

Figure 19: The Fees tab on the Card Master screen

Local (domestic) fees, fixed fees and fees based on a percentage are shown.

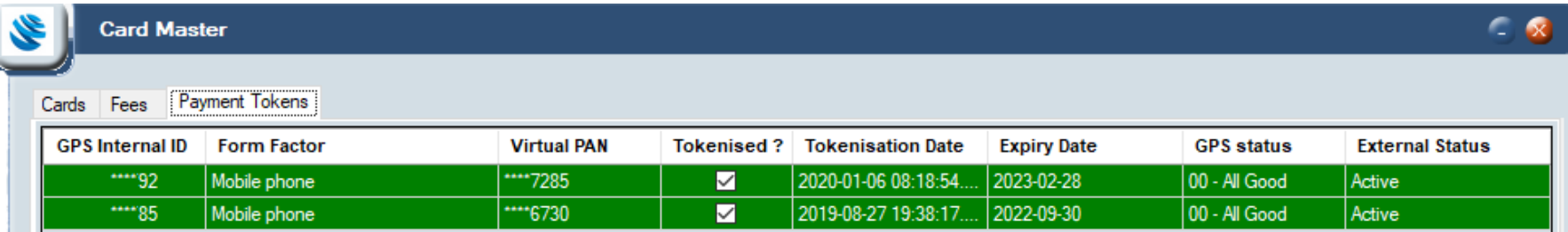
**Partial Allowed** indicates whether a partial fee is permitted or not. For example, if the fee is £1 but the customer has only 50 pence in their account, only a partial fee of 0.50 can be claimed.

### 9.4 Viewing Payment Tokens

You can see information about payment tokens, such as when a token was set up with MDES/VDEP, and the form factor which is the type of device used for the wallet (for example, a mobile phone). For more information, see [Managing MDES and VDEP cards](#).

To view payment tokens:

- 1. From the **View Transactions** screen, highlight a transaction in the list, right-click and choose **More details**.
- 2. Choose **Card Details inc Fees**. The **Card Master** screen appears with two additional tabs.
- 3. Click the **Payment Tokens** tab. The results appear in colour-coded rows. The colours are explained in the key at the bottom of the screen.



GPS Internal ID	Form Factor	Virtual PAN	Tokenised ?	Tokenisation Date	Expiry Date	GPS status	External Status
****92	Mobile phone	****7285	<input checked="" type="checkbox"/>	2020-01-06 08:18:54....	2023-02-28	00 - All Good	Active
****85	Mobile phone	****6730	<input checked="" type="checkbox"/>	2019-08-27 19:38:17....	2022-09-30	00 - All Good	Active

Figure 20: The Payment Tokens tab on the Card Master screen

- 4. Double click the green line to open the Payment Token. For more information, see [Managing MDES/VDEP cards](#).


### 9.5 Viewing Fees Configuration

You can see information about the fees that apply to a card, including recurring fees and authorisation fees, using the **Fees Configuration** screen.

To view fees configuration:



1. From the **View Transactions** screen, highlight a transaction in the list, right-click and choose **More details**.
2. Choose **Show Fees Settings**. The **Fees Configuration** screen appears.


**Fees Configuration**

**Fees Configuration for the card :**

**Auth Fee (Group)**
**Auth Fee (Group) History**
Close

Group	Proc Code	Description	Dom Fee	Partial Allowed	Dom Fee Rate (in %)	Non Dom Fee	Non Dom Rate (in %)	Dom Min Fee	Non Dom MinFee	Decline Fee	Fx Fixed	Fx Rate	Thresho Type
	01	Debits (for ATM withdrawals, or f...	1.00	<input checked="" type="checkbox"/>	0.00	2.00	2.75	0.00	0.00	0.00			
	00	Debits (goods and services)	0.20	<input type="checkbox"/>	0.00	0.20	2.75	0.00	0.00	0.00			
	30	Balance inquiry service	0.20	<input type="checkbox"/>	0.00	0.00	2.75	0.00	0.00	0.00			
	92	PIN change transactions	0.20	<input type="checkbox"/>	0.00	0.00	2.75	0.00	0.00	0.00			

**Recurring Fee (Group)**
**Reccuring Fee (Group) History**

Fee Group	Fee Group Code	Recurring Fee	Fee Start Date	Fee End Date	Is live	Fee Amt	Fee Currency	Partial Allowed	Frequency	Freq Period
		Monthly Fee ....	11/03/2014	11/03/2014	<input checked="" type="checkbox"/>	5.95	826	<input checked="" type="checkbox"/>		

**Webservice Fee (Group)**
**Webservice Fee (Group) History**

Group	Proc Code	Description	Dom Fee	Partial Allowed	Dom Fee Rate (in %)	Non Dom Fee	Non Dom Rate (in %)	Dom Min Fee	Non Dom MinFee

**Webservice Fee (Product)**
**Webservice Fee (Product) History**

Product	Description	Dom Fee	Partial Allowed	Dom Fee Rate (in %)	Non Dom Fee	Non Dom Rate (in %)	Dom Min Fee	Non Dom MinFee
	Fees : 14 Fees : Unknown	0.00	<input type="checkbox"/>	0.00 %	0.00	0.00 %	0.00	0.00
	Fees : 02 Fees : GPS Kiosk	1.00	<input type="checkbox"/>	0.00 %	0.00	0.00 %	0.00	0.00
	Fees : 03 Fees : GPS Web Site	1.00	<input type="checkbox"/>	0.00 %	0.00	0.00 %	0.00	0.00
	Fees : 04 Fees : Card Processor	1.00	<input type="checkbox"/>	0.00 %	0.00	0.00 %	0.00	0.00

- **Auth Fee (Group)** — Displays fees configured on the card which are applied during the authorisation stage based on the processing code.
- **Recurring Fee (Group)** — Displays any rule-based fees which apply to the card such as a dormancy fee due to card inactivity.
- **Web service Fee (Group and Product)** — Displays any fees triggered by Web Services.

**Tip:** Use the scroll bars to see more information on the right hand side, such as the **Note** field.

## 9.6 Next Steps

For information about managing cards and transactions, such as adjusting a balance or activating a card, see [Managing Cards](#). For more information on fee setup, see the *GPS Fees Guide*.

# 10 Managing Cards

This topic explains how to perform various actions on specific transactions or tokens, such as removing an authorisation, adjusting a balance or changing the status of a card.

You use the **Actions** menu to manage transactions or tokens. To display the **Actions** menu:

1. Highlight a transaction in the **View Transactions** screen, then right click.
2. Select **Actions** to display a menu.

The options shown depend on the type of transaction, so the actions available on authorisations will differ from those for pre-sentments. For example:

## Actions when clicking on Authorisations

Authorisation	Accepted	EUR	96.53	-96.53	0.00	0.00	0.00	0.00	0.00	0.00
Presentment	Settled	EUR	22.58	-22.58	0.00	0.00	0.00	0.00	0.00	0.00
Presentment	Settled	EUR	148.55	-148.55	0.00	0.00	0.00	0.00	0.00	0.00
Presentment	Settled	EUR	73.66	-73.66	0.00	0.00	0.00	0.00	0.00	0.00
Presentment	Settled	EUR	32.55	-32.55	0.00	0.00	0.00	0.00	0.00	0.00
Authorisation	Cleared	EUR	148.55	-148.55	0.00	0.00	0.00	0.00	0.00	0.00
Authorisation	Cleared	EUR	22.58	-22.58	0.00	0.00	0.00	0.00	0.00	0.00
Presentment	Settled	EUR	76.05	-76.05	0.00	0.00	0.00	0.00	0.00	0.00
Authorisation	Cleared	EUR	145.77	-145.77	0.00	0.00	0.00	0.00	0.00	0.00
Authorisation	Cleared	EUR	51.81	-51.81	0.00	0.00	0.00	0.00	0.00	0.00

More details

Actions

Tracker

Copy to Clipboard

Copy Whole Row to Clipboard

Refresh

Cancel

Balance Adjustment

Card UnLoad

Change Card Status

Activate Card

Extend Expiry

Edit Card Details

PIN and CVC2 services

Add transaction to MasterCard SAFE Report

Resend to EHI

Ctrl+B

Ctrl+S

Ctrl+E

Figure 21: Options available on an authorisation

**Note:** If you cannot see a menu option, this may be because you do not have the appropriate permissions. For more information, see [About Roles and Permissions](#).

## 10.1 Removing an Authorisation

You can remove an authorisation on a selected transaction. Removing an authorisation releases the blocked amount related to the authorisation (the auth amount), making it available for the cardholder to spend again.

**Note:** Removing an authorisation does not prevent the associated presentment from posting on the account. Because of this, use caution as the presentment can bring the account into a negative balance if insufficient funds remain to cover it. If a pre-sentment is received for this authorisation, then another authorisation is created to match the presentment. This authorisation is marked as 'offline' as there is no matching un-cleared authorisation.

To remove an authorisation:

1. From the **Actions** menu, select **Remove Authorisation**.
2. Add a note for the audit trail so colleagues can see why an authorisation was removed.
3. Click **Remove Now**.



Figure 22: Remove Authorisation screen

# 10.2 Adjusting a Balance

You can add or remove funds from a cardholder’s balance manually

Tip: You can also use the Web Services APIs to do this (Ws\_BalanceAdjustment). For more information, see the *Web Services Guide*.

To adjust a balance:

- 1. From the **Actions** menu, select **Balance Adjustment**. The **Balance Adjustment** screen appears.

Figure 23: Balance Adjustment screen

- 2. From the **Credit/Debit** dropdown box, select **Debit** or **Credit**.
- 3. In **Adjustment Type**, select the reason for the balance adjustment.

Figure 24: Balance Adjustment screen showing adjustment types

- 4. In **Adjustment Amount**, enter the amount the cardholder needs to be credited or debited.

Note: Ensure this amount is correct as it will cause issues with the balance if input incorrectly.

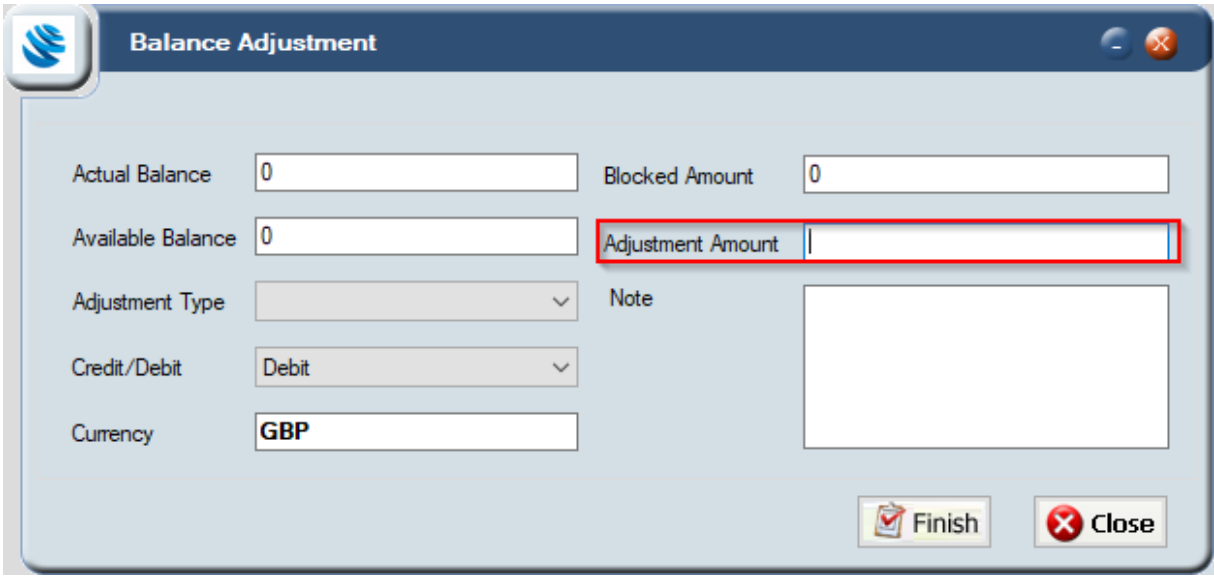


Figure 25: Balance Adjustment screen showing adjustment amount

- 5. In the **Note** field, add the reason for the adjustment. This is required for audit purposes.
- 6. Click **Finish**.

### 10.3 Performing a Balance Transfer

You can transfer part of a balance or the whole balance from one card to another. For example, you may need to transfer a balance if a card is reported stolen. You can also apply any associated fees using the **Card Load Fee** options.

To perform a balance transfer:

- 1. From the **Actions** menu, select **Balance Transfer**. The **Balance Transfer** screen appears showing the actual and available balance on the card, and any blocked amount.

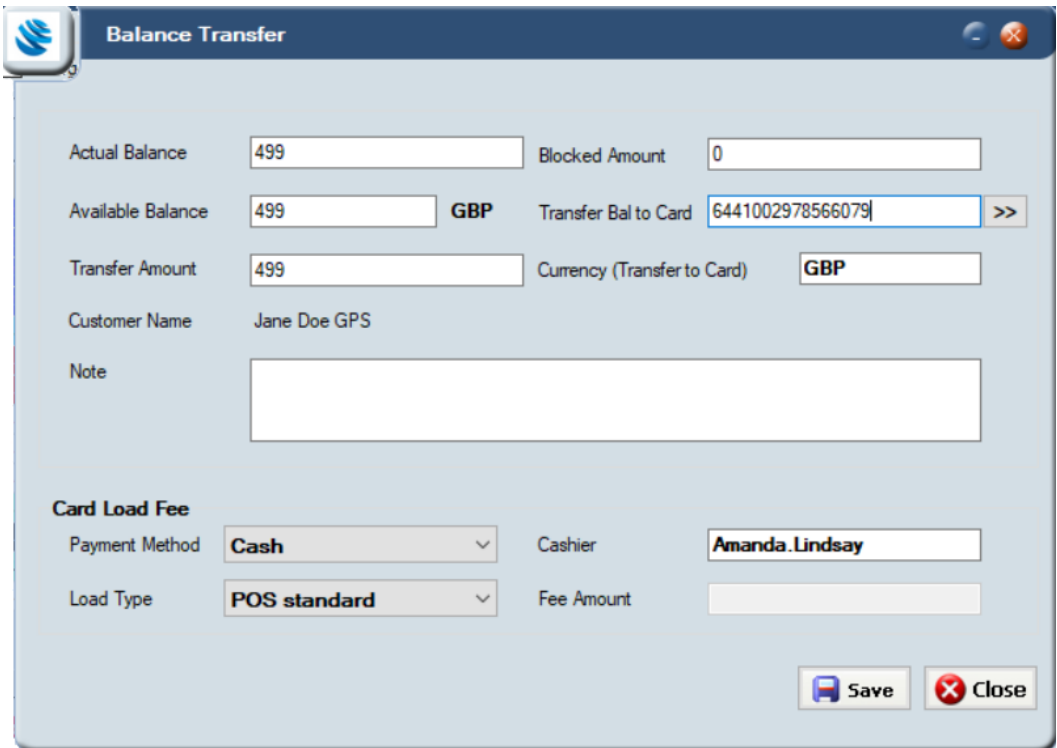


Figure 26: Balance Transfer screen

- 2. Enter the amount you want to transfer in **Transfer Amount**.
- 3. In **Transfer Bal to Card**, click the arrow and specify the token you want to transfer the balance to.
- 4. If the type of transfer falls under a fee group applied to that token, the **Card Load Fee** shows the fee applied to the balance transfer.
- 5. Click **Save**.

### 10.4 Performing a Card Unload

You can unload a specified amount from an account using **Card Unload**. For example, you may need to do this if you are closing an account.

To perform a card unload:

1. From the **Actions** menu, select **Card Unload**. The **Card Unload** screen appears.

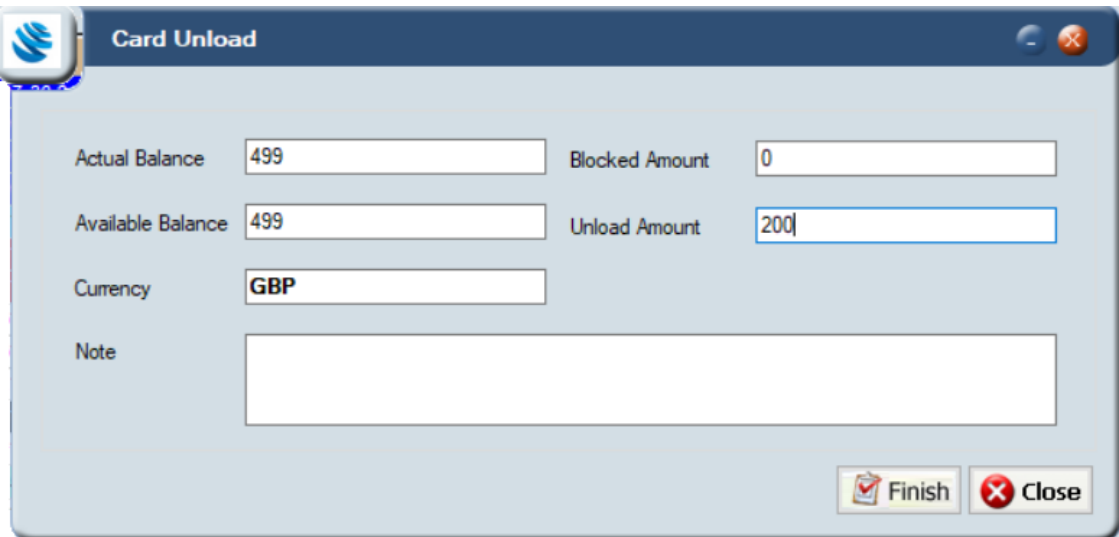


Figure 27: Card Unload screen

1. In **Unload Amount**, specify the amount you want to unload from the card. You cannot unload more than the available balance.
2. Add a note for audit purposes (optional but recommended).
3. Click **Finish**.

## 10.5 Changing the Status of a Card

You can change the status of a card using **Change Card Status**. For example, you may need to do this if a card is reported as lost or stolen. Each card status has a different effect on how the card can be used. For a full list of card statuses, see [Appendix B: Card Status Codes](#).

**Tip:** You can also use the Web Service APIs to do this (Ws\_StatusChange). For more information, see the *Web Services Guide*.

To change the status of a card:

1. From the **Actions** menu, select **Change Card Status**. The **Status Change** screen appears.
2. From the **Change Card Status To** dropdown box, select a card status.

**Note:** If you attempt to apply an incorrect or unsupported card status, the **Action** field displays the reason and the status that Smart Client will apply.

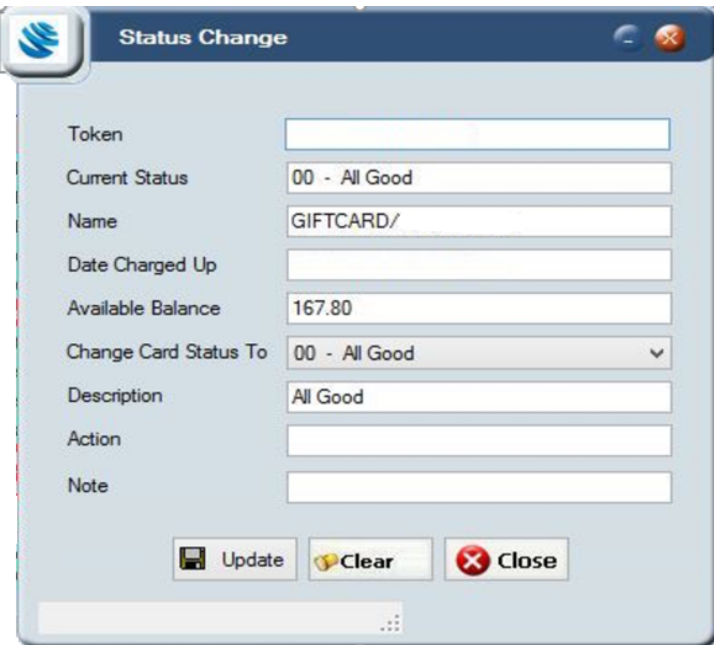


Figure 28: Status Change screen

3. Add a note for audit purposes (optional but recommended).
4. Click **Update** to apply the status change.



## Notes

- Most statuses are reversible (except for 83 – Card Destroyed, and 43 – stolen)
- All statuses other than 00 will prevent the card from being used over the Mastercard or VISA network
- Do not use 01 – Refer to Card Issuer or 54 – Expired Card; these are for GPS use only
- Changing the status to 99 (card voided) or 98 (refund to customer) automatically generates a card balance adjustment down to 0.00. A negative balance must be manually adjusted to 0.00.
- Where MDES or VDEP is in place and a cardholder is using, for example Apple Pay, G Pay, Fitbit Pay, Sony Pay, Mont Blanc Pay or similar, the DPAN Token (Device PAN token) can have a different status to the FPAN (Funding Primary Account Number — the PAN on the physical card).

## 10.6 Activating a Card

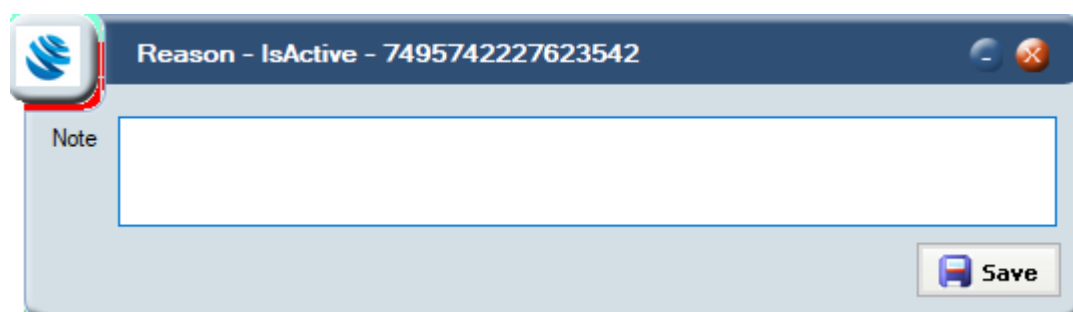
You can activate a card using the **Activate Card** option.

Once a card has been activated it cannot be deactivated using this option.

**Note:** When converting a virtual card to physical, you can use this option to activate the physical card.

To activate a card:

1. From the **Actions** menu, select **Activate Card**.



*Figure 29: Activate Card screen*

2. In **Note**, provide a reason for the activation.
3. Click **Save**.

## 10.7 Extending the Expiry Date

You can extend the period that a card is valid for using the **Extend Expiry** option. For example, you may want to do this to extend the expiry date on a gift card.

**Note:** This updates the expiry date held on the GPS platform. Use caution because this may cause a mismatch between this date and the expiry date embossed on the card.

To extend the expiry date:

- 1. From the **Actions** menu, select **Extend Expiry**.

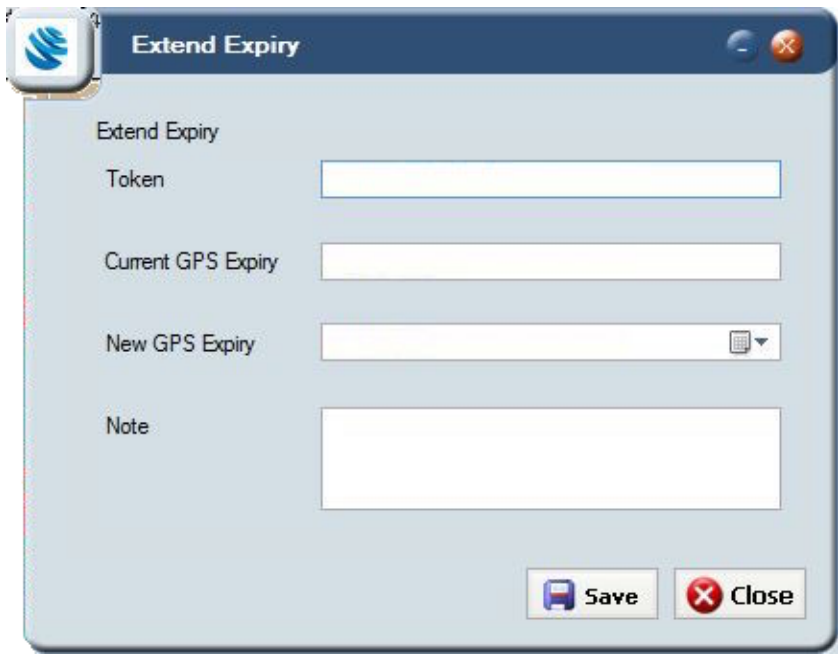


Figure 30: Extend Expiry screen

- 2. In **New GPS Expiry**, click the arrow and specify the new expiry date.
- 3. In **Note**, provide a reason for the extension.
- 4. Click **Save**.

## 10.8 Editing Card Details

You can edit the cardholder details and change the rules governing card acceptance methods using the **Edit Card Details** option. For example, you can prevent a card from being used on gambling sites by disallowing a specific Merchant Category Code (MCC).

To edit card details:

- 1. From the **Actions** menu, select **Edit Card Details**. The **Card Master** screen appears. For more information about the information on this screen, see [Viewing Card Details](#).

**Tip:** Click the arrow adjacent to some fields to display more information; for example, **Group Limit**.

Card Master

Cards

Fees

Payment Tokens

Token6441002978566079>>>

FileNameGPSINSTITUTIONTEST\_GPSVISA\_6\_45726

led Up22-07-2021

Actual Balance499.00

Card Purchaser

First NameJane

LastNameDoe GPS

Address11

Address2London Road

PostCodeSS6 9EE

CountryUnited Kingdom

Card Holder

First NameJane

LastNameDoe GPS

Address11

Address2London Road

PostCodeSS6 9EE

Mobile No:

EmailID

File Generated On2021-07-22 21:47:41.480

Status00 - All Good

Centre Name

Card Acceptor List

Card Disallow List

Group Web

Card FX Group

Calendar Group

Card Linkage

Group UsageGPS PHYSICAL USAGE TEST

Group MCC

Group LimitGPS LIMITS GBP TEST

Group Auth

Limited Network

Rec Fee

Adv Permission00000000 00000000 00000000 00000000 00000100

SchemeGPS SCHEME TEST

ProductGPS PRODUCT TEST VISA GBP L

CurrencyGBP

Customer Ref

Passcode \*636746

Activation Date2021-07-22 14:05:49.180

GPS Expiry2022-06-30 00:00:00.000

IsLiveDate2021-04-14 18:01:29.067

Primary6441002978566079

3D Secure VDE's ValidN/A

( Byte 5 -> Byte 1)

SaveDeleteClearClose

Figure 31: Editable Card Master screen

2. After making your changes, click **Save**.

Tip: For information about configuring fees and payment tokens using the **Fees** and **Payment Tokens** tabs, see [Viewing card fees and fee settings](#) and [Viewing payment tokens](#).

# 10.9 Unblocking a PIN

You can unblock a PIN and send the PIN via an SMS message to a cardholder using the **PIN and CVC2 Services** option. The PIN stored on the card’s chip is called the offline PIN. The PIN stored on the GPS system is the online PIN. To unblock a PIN:

1. From the **Actions** menu, select **PIN and CVC2 Services**. The **PIN and CVC2 Services** screen appears.

PIN and CVC2 services

Token

Card Status : All Good

Online PIN tries remaining : 3

Offline PIN tries remaining : 3

CVC2 tries remaining : unlimited

SMS Pin To Card Holder

Reset all & Send PIN Unblock

Close

Figure 32: PIN and CVC2 services screen

The following information is shown:

- **Card Status** — the card's status. For a full list of card statuses, see [Appendix B: Card Status Codes](#).
- **Online PIN tries remaining** — the number of online PIN attempts left. The limit is 3 consecutive incorrect attempts. Online PIN checks are counted when the PIN is checked against the PIN stored in the GPS system, not the PIN of the chip.



- **Offline PIN tries remaining** — the number of offline PIN attempts left. The limit is 3 consecutive incorrect attempts. Offline PIN checks are made between the POS terminal and the chip (chips store the PIN, eliminating the need to do an online PIN verification).
- **CVC2 tries remaining** — the number of Card Validation Code (CVC) attempts left.

**Note:** If the offline PIN is blocked, the card will decline at the POS terminal. In this circumstance, the decline may not show in Smart Client (this can happen because the chip informs the POS terminal that the PIN limit has been exceeded). The GPS system is updated only when the card is used at an online EMV-capable terminal.

### 10.9.1 Sending a PIN Unblock

You can send the PIN via SMS to a cardholder using **SMS Pin To Card Holder**. This automatically generates a script that gets queued. As soon as the card is used at an online EMV terminal, the script is sent to the card where it unblocks the PIN counter on the chip. During this procedure, the card will decline the first transaction.

**Tip:** If multiple transactions decline due to an incorrect PIN, repeat the procedure to send another PIN unblock script and ask the cardholder to use another POS (preferably an ATM). To check whether a card was used at an EMV-capable terminal, refer to the **POS Data (DE061)** field. See [Examining a Transaction in Detail](#).

### 10.9.2 Resetting all and sending a PIN unblock

The offline PIN and online PIN can become out of sync in the event a cardholder changes their PIN at an offline terminal then uses their card at an online terminal that doesn't recognise the change.

- To unblock the online PIN and reset all online and offline PIN and CVC2 tries back to zero (if these are not set to unlimited), click **Reset all and send PIN unblock**.

## 10.10 Resending a Transaction to EHI

**Note:** This feature is available on request. For information, contact your GPS Account Manager.

You can resend a transaction (an EHI Message) to your External Host Interface (EHI) using the **Resend to EHI** option. This immediately resends the selected transaction (for example, an Authorisation or Presentment) to the EHI. For example, if an EHI timeout occurred for a minute due to downtime, you may need to resend a transaction that happened during that time to EHI.

To resend a transaction to EHI:

1. From the **Actions** menu, select **Resend to EHI**.
2. Click **OK** to proceed. The transaction's EHI message is resent to your host.

For more information, see the *EHI Guide*.

## 10.11 Viewing Card History

You can view a history of all the actions applied to a card using the **Tracker** option. This shows actions including:

- Date of activation
- Group changes
- Card status changes
- Other actions taken against the card, with details about the user who performed the action.

To view card history:

- From the **Actions** menu, select the **Tracker** option. The **Tracker History** screen appears:

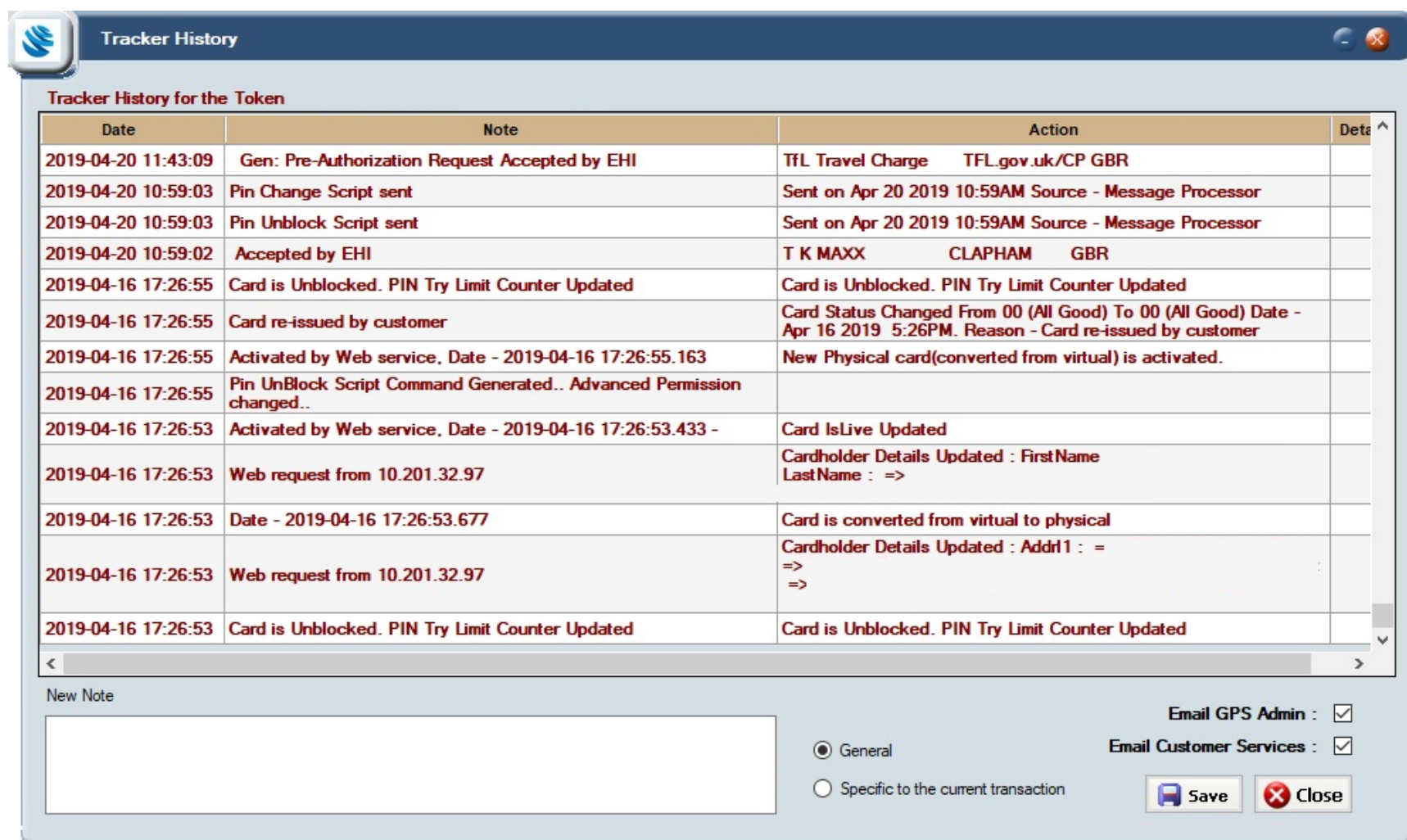


Figure 33: Tracker History screen showing a history of all the actions applied to a token

Tip: Use the scroll bar to see all the information.

### 10.11.1 Adding a note to a transaction

You can add a note to a transaction which will be visible in the **Tracker History** screen in Smart Client.

**Note:** The note is informational only and is not sent via the External Host Interface or shared with your own systems.

To add a note to the transaction:

1. Input the message into **New Note**.
2. To apply the note to this particular transaction, select **Specific to the current transaction**.
3. Click **Save**. The note is appended.

# 11 Managing Chargebacks

Smart Client enables you to view Visa and Mastercard chargebacks.

For Mastercard transactions only, you can raise chargeback 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. You must complete the following prerequisites before the Smart Client Chargeback service can be enabled:

- 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.

Using Smart Client, you can:

- 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 Linked 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. Contact GPS Support for details.

## 11.1 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 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 screen, right-click the transaction being disputed by the cardholder and select **Actions > Create Chargeback**.
2. In the **Chargebacks** screen, enter the details of the chargeback. Refer to the table below for details.

Create Chargeback

☒ Full ChargeBack

☐ Partial ChargeBack

Chargeback Currency

Amount of chargeback

0.00

Reason for Chargeback

4515 - Cardholder Denies

Select Text Format

Documentation Indicator

Supporting documentation will follow

Days Allowed

120

Days Remaining

-117

Supporting Text DE 72

Note

☐ Edit Exclusion Indicator

☐ Credit to Card

View Chargebacks

Create Chargeback

Cancel

Figure 34: Create Chargeback screen

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 the chargeback request. You can try fixing the details and resending the chargeback request or contact GPS support.

Chargeback 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 the latest chargeback reasons, see the <i>Mastercard Chargeback Guide</i> . <b>Note:</b> If the reason is fraud related, you must create a SAFE Report before issuing the chargeback. <sup>(1)</sup>
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: <ul style="list-style-type: none"><li>Supporting documentation is not required</li><li>Supporting documentation will follow</li></ul> Refer to the <i>Mastercard Guide</i> for details of the types of Chargeback Reason Codes that require supporting documentation.
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	Add a description, to be displayed in the DE 72 field of the chargeback message sent to Mastercom. This field

Chargeback Option	Description
DE 72	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. <sup>(2)</sup> <b>Note:</b> This functionality is not yet released. Check with your GPS Account Manager for details.
Credit to Card	If you check this option, the chargeback amount will be credited back to the card. <sup>(3)</sup>

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.

11.2 Viewing Chargebacks

**Note:** Supported for both Mastercard and Visa cards.

1.

From the Smart Client menu, select **Card Activity > Chargebacks**.
2.

In the **Chargebacks** screen, you can view raised chargeback details for a specific card or for all cards:

1.

To query chargebacks for a specific card, in the **Token** field enter the public token number of the card you want to query.

2.

To list chargebacks within a specified date range and status, select the Status and date range and click **List**.

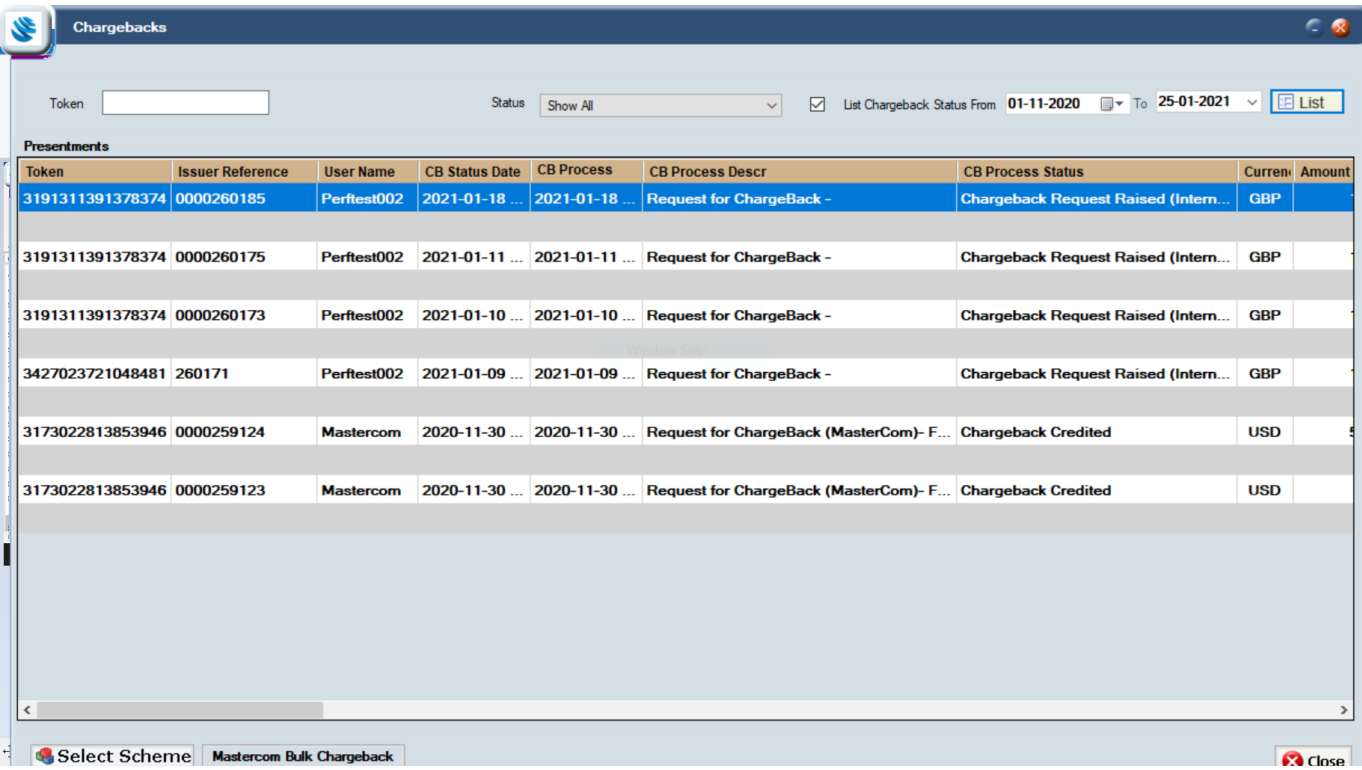


Figure 35: Chargebacks screen

3.

To view details of the chargeback, use the scrollbar at the bottom-left corner of the screen 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:



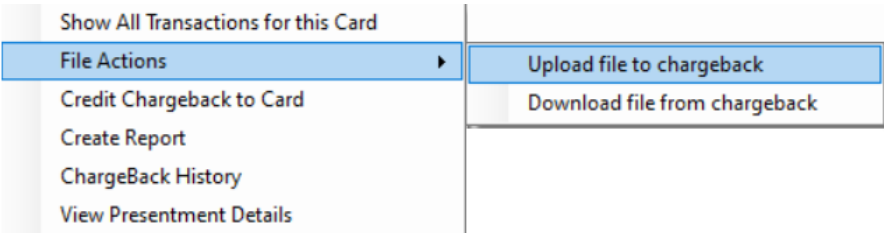


Figure 36: Further actions available on a chargeback

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

## 11.3 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.

### 11.3.1 Showing all Transactions for a Card

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

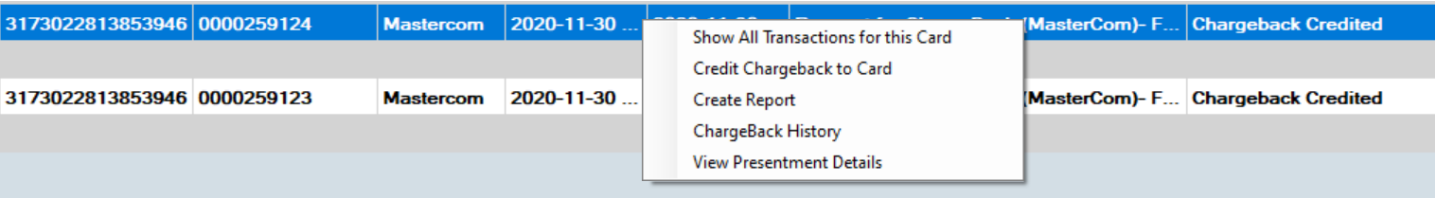


Figure 37: Show All Transactions for this Card option

- The **View Transactions** screen appears, with the card’s public token preselected and displaying a list of transactions linked to the card.

### 11.3.2 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.

- To credit the chargeback amount back to the card, in the **Chargebacks** screen, right-click the required transaction and select **Credit Chargeback to Card**.
- 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](#).

### 11.3.3 Viewing Linked Transaction Details

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

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

The **Transaction Details** screen is displayed.

Transaction Details

Transaction ID : 6150584240

Token

3173022813853946

Date Expiry (YYMM)

2011

POS Entry Mode (DE022)

D11401B99000

BN Ref (DE063)

DLL784896

Transaction Date

2020-11-30 13:49:24.723

Advice Reason Code

Response Status (DE039)

Cleared

STAN (DE011)

Processing Code

Debits (goods and services) - 000000

POS Data (DE061)

Track2 Data (DE035)

\*\*\*\*\*

Private Data (DE112)

Additional Amounts (DE054)

Card Acceptor Identification Code (DE042)

test1234AAAAAA

Card Acceptor Name Location (DE043)

test 123456 luulu koc\\n\

Additional Response Data (DE044)

PIN Data (DE052)

Till Time

201130134357

Card Acceptor Terminal Identification (DE041)

test1234

Response Source

Response Reason

Transaction Amount (DE004)

1.00 - EUR

Settlement Amount (DE005)

1.00 - EUR

Billing Amount (DE006)

1.00 - EUR

Amounts, Transaction Fee (PDS0146)

Merchant Category Code (MCC)

3000 - 3000-3299

Retrival Reference Number (DE037)

000000764724

Acquirer Reference Data (DE031)

02807190335000007650100

AID (DE032)

280719 -

FID (DE033)

456321

Authorisation Code

198181

New PIN (DE125)

GPS ARC

DE053

Script Received

Tran.Orig.Institution ID Code(DE094)

280719

ICC Data (DE055 - 0100)

Additional Data (DE048)

0002003 0003003

Fees Detail Note

Auth Amount : 1

Total : 1

Available Amount : 188.94 ==> Settled!

View PAN

Related Auth

Show Card Details

Close

Figure 38: Transaction Details screen

2. Use the buttons at the bottom right of the screen to view further details.

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

11.3.4 Viewing Chargeback History

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

The **Chargeback History** screen is displayed.

Chargeback History

Charge back History for the Token 3173022813853946

Description	Issuer	Note	Date
Request for ChargeBack (MasterCom)- Financial Position - Chargeback Credit Acknowledgement(MasterCom)	0000259124	FileID - 9062002910000000302000007, Reason: 4853 - Cardholder DisputeCorrelationID - cid2142193603q	2020-11-30 14:38:35.250

Close

Figure 39: Chargeback History screen

11.3.5 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** screen, 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** screen is displayed, showing details of the linked presentment transaction.

11.3.6 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** screen, right-click the required transaction and select **Create Retrieval Request**.

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

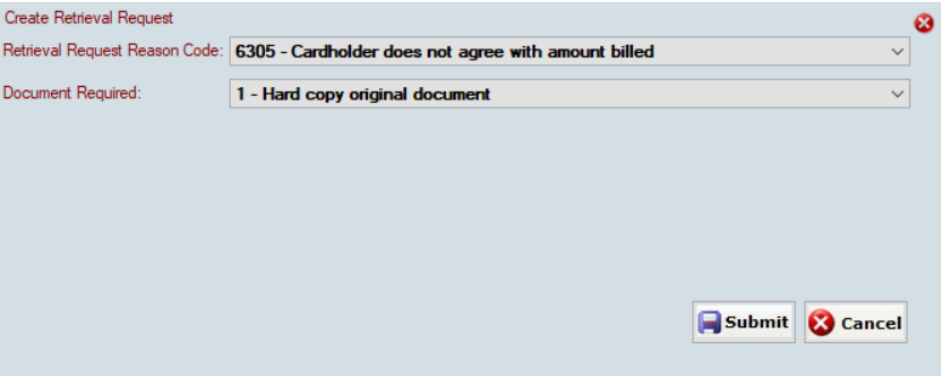


Figure 40: Create Retrieval Request screen

- 2. In **Retrieval Request Reason Code**, select an appropriate reason for the retrieval request. For details, see the table below.
- 3. In **Document Required**, select the format required. Options are:
  - 1. Hard copy of the original document
  - 2. Copy or image of the original document
  - 3. 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**.

Retrieval Request Reason 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 screen.
- Once the acquirer responds to the retrieval requests, to download the documentation, right-click the retrieval request in the **Chargeback** screen and select **File Actions > Get Documentation**. For details, see [Downloading Chargeback Documentation](#).

11.3.7 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** screen, right-click the required transaction and select **File Actions > Upload file to chargeback**.

The following screen is displayed:

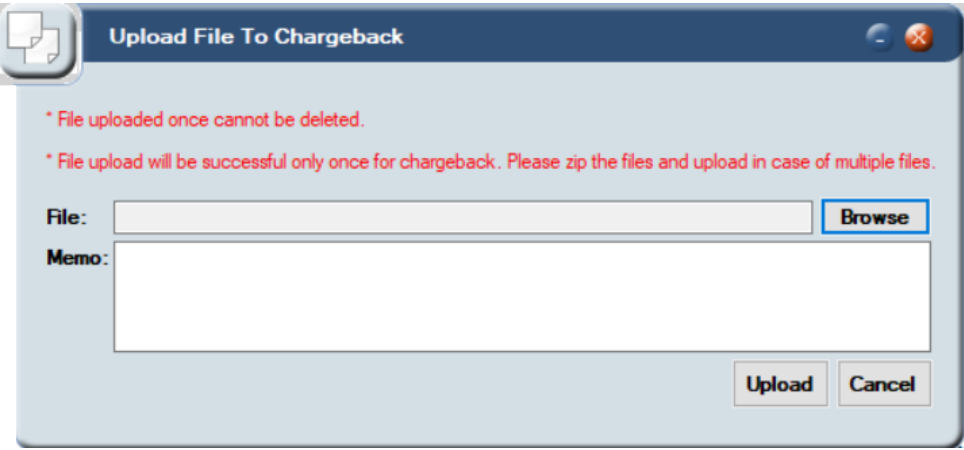


Figure 41: Upload File to Chargeback screen

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, ensure you have all the documents you need before using this option.

2. To select a file to upload, click **Browse**.
3. In **Memo**, 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.

**Note:**

- 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.

11.3.8 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** screen, right-click the required transaction and select **File Actions > Download file from chargeback**.

The following screen is displayed:

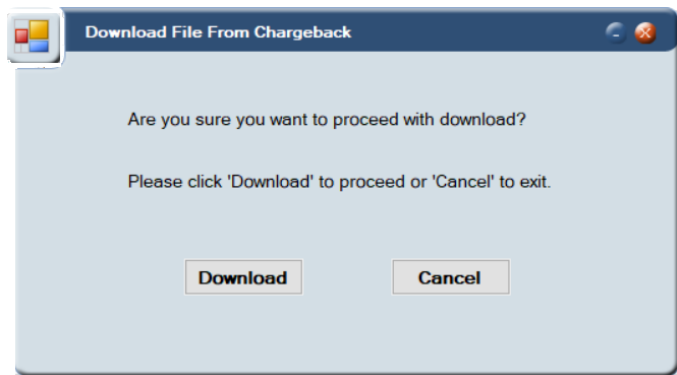


Figure 42: Download File From Chargeback screen

- 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.

11.3.9 Reversing a Chargeback

You can use this option reverse a chargeback that has previously been 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** screen, 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.

11.3.10 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** screen, right-click the rejected chargeback transaction and select **Re-Raise Chargeback**.

The following screen is displayed:

Figure 43: Reraise Chargeback screen

- 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.

11.3.11 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** screen, right-click the required transaction and select **Create Mastercom fee collection message**.

The Mastercom Fee Collection screen is displayed.

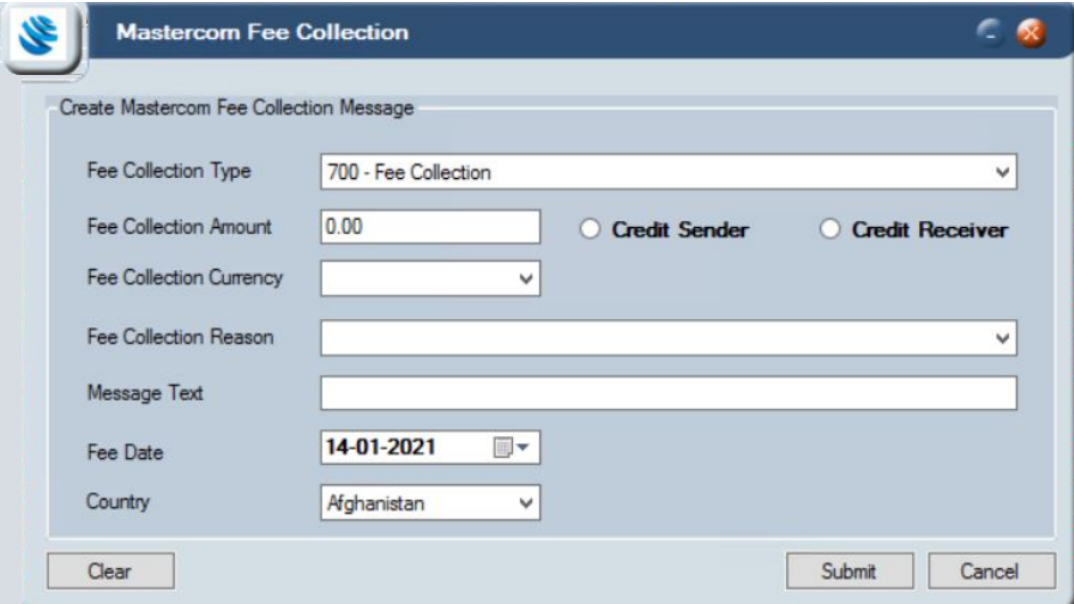
The screenshot shows the 'Mastercom Fee Collection' window. It has a title bar with the application icon and name. Below the title bar is a tab labeled 'Create Mastercom Fee Collection Message'. The form contains several fields: 'Fee Collection Type' is a dropdown menu with '700 - Fee Collection' selected; 'Fee Collection Amount' is a text box with '0.00'; 'Fee Collection Currency' is a dropdown menu; 'Fee Collection Reason' is a dropdown menu; 'Message Text' is a large text area; 'Fee Date' is a date picker showing '14-01-2021'; and 'Country' is a dropdown menu with 'Afghanistan' selected. There are three buttons at the bottom: 'Clear', 'Submit', and 'Cancel'. The 'Credit Sender' radio button is selected.

Figure 44: Mastercom Fee Collection screen

2. Provide all the details as per the instructions in the table 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 Screen**:

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

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

Fee Collection Information	Description
Fee Collection Type	Select the type of fee collection. Options include: <ul style="list-style-type: none"><li>700 - Fee Collection</li><li>780 - Fee Collection Return</li><li>781 - Fee Collection Return Resubmission</li><li>782 - Fee Collection Arbitration Return</li></ul>
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: <ul style="list-style-type: none"><li>Credit sender – fee will be credited to your account</li><li>Credit receiver – fee will be credited to the receiver.</li></ul>
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).
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.

11.3.12 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** screen is displayed.

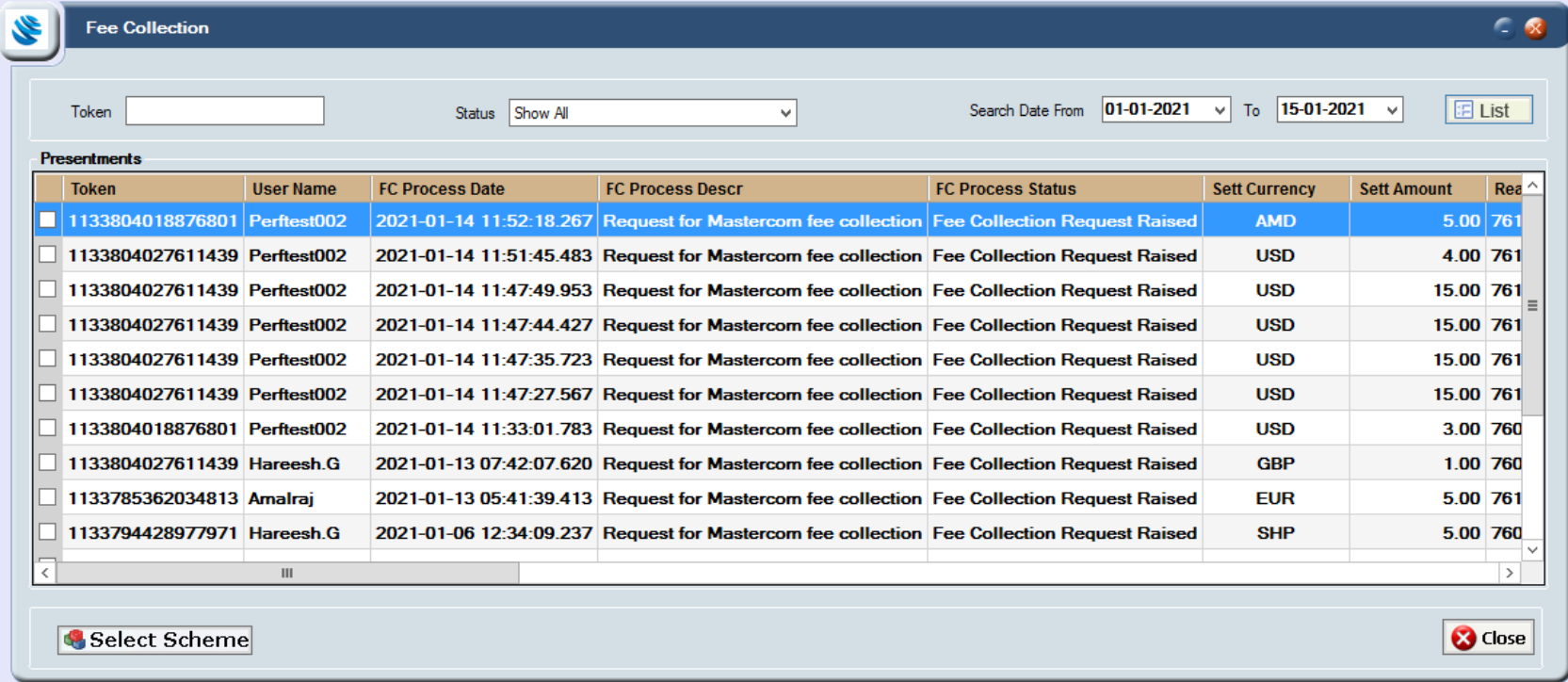


Figure 45: Fee Collection screen

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**.

11.3.13 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.

To create a SAFE report:

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

The Create Mastercom SAFE report screen is displayed.

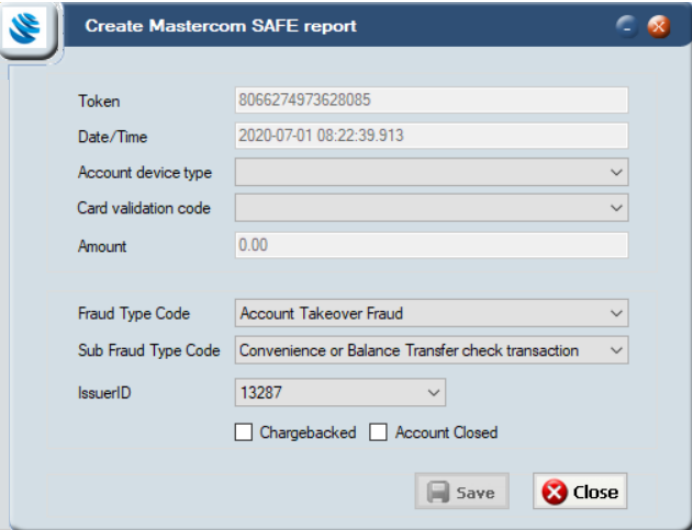


Figure 46: Create Mastercom SAFE report screen

2. Provide all the details as per the instructions in the table 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 fee collection message is displayed in the **SAFE Report Details** Screen. See [Viewing SAFE Report Details](#).

SAFE Report 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. <div><div>Account Takeover Fraud</div><div>Bust-out Collusive Merchant</div><div>Card Not Present Fraud</div><div>Counterfeit Card Fraud</div><div>Fraudulent Application</div><div>Lost Fraud</div><div>Multiple Imprint Fraud</div><div>Never Received Issue</div><div>Stolen Fraud</div></div>
Sub Fraud Type Code	Select a sub-fraud type code. Options include: <ul style="list-style-type: none"><li>• Convenience or Balance Transfer check transaction</li><li>• PIN not used in transaction</li><li>• PIN used in transaction</li><li>• Unknown</li></ul>
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.

11.3.14 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** screen is displayed.

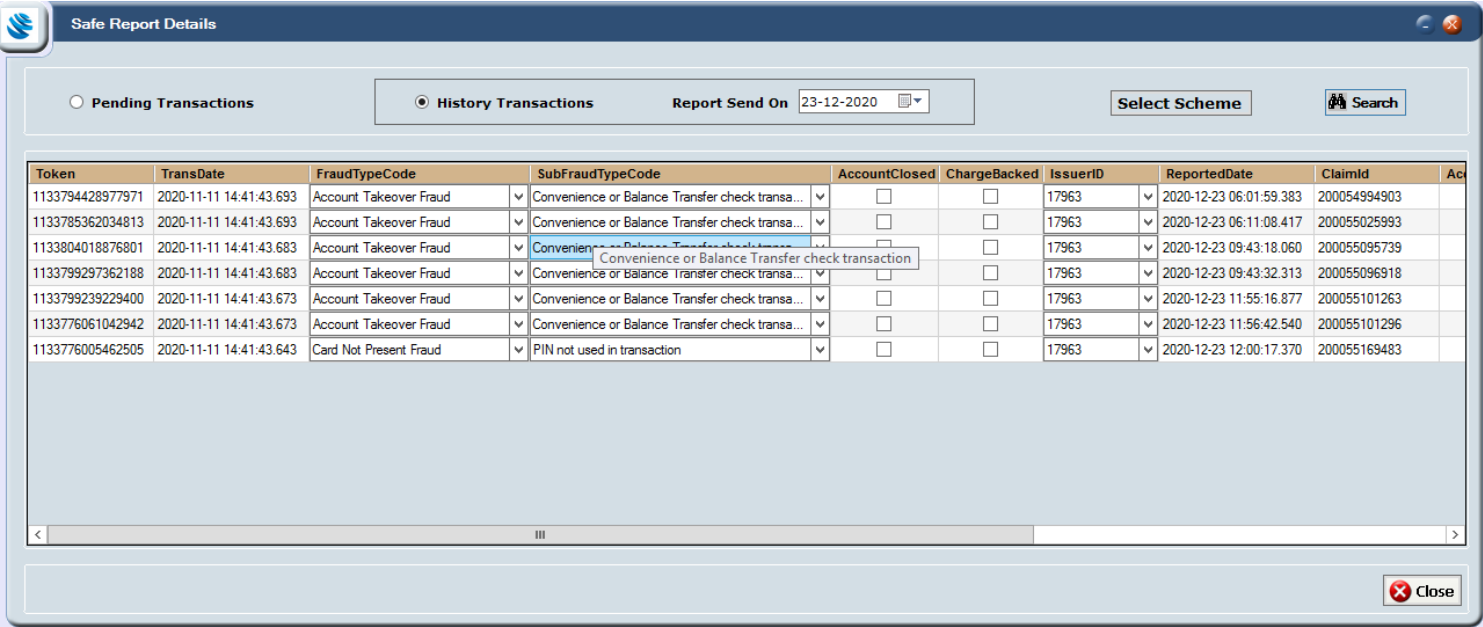


Figure 47: Safe Report Details screen

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

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

2. Click **Search**.

11.3.15 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.

Token	ChargebackAmount	ChargebackCurrency	ReasonCode	ReasonCodeDescription	UserName	TransactionId	IsPartialChargeback	IsCreditToCardTransaction	DocumentIndicator	De72
123456789	100.00	GBP	4515	Cardholder Denies	user	12345678	N	N	N	Cardholder Denies
123456790	170.01	EUR	4853	Goods Not received	user	12345679	N	N	N	Goods Not received
123456791	60.02	EUR	4515	Cardholder Denies	user	12345680	N	N	N	Cardholder Denies
123456792	15.03	GBP	4515	Cardholder Denies	user	12345681	N	N	N	Cardholder Denies
123456793	10.04	EUR	4515	Goods Not received	user	12345682	N	N	N	Goods Not received

For details of the fields in this file, see the table below.

SAFE Report 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 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 the latest chargeback reasons, see the <i>Mastercard Chargeback Guide</i> .
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.



## 12 Case Filing

As of 17 July 2020, Mastercard changed the Chargeback process to a rules-based system which is designed to make dispute resolution fairer and more responsive for all parties.

As a result of these changes, arbitration is no longer part of the Chargeback process. Instead, if a chargeback is rejected and the customer wants to dispute the case further, they can raise this as a case filing to Mastercard.

The fees associated with the case filing process are also different to that for chargebacks. For more information about the fee structure, contact Mastercard.

### 12.1 What is Case Filing?

Mastercard case filing is a feature through which an issuer or an acquirer can raise a concern with Mastercard.

To dispute a transaction after completion of the chargeback cycle, you can create either a pre-arbitration or arbitration case. Pre-arbitration case filing differs from arbitration case filing only in terms of the fees charged by Mastercard. For information about fees, contact Mastercard.

In terms of reporting, case filings and chargebacks are two different transaction types. No transaction is created at card level for the new arbitration/pre-arbitration case filings, thus no data is sent to EHI.

**Note:** GPS do not currently support compliance case filings (pre-compliance and compliance). GPS supports only pre-arbitration and arbitration case filings.

### 12.2 Creating a Case

If you want to dispute a transaction after completion of the chargeback cycle, you can create either a pre-arbitration or arbitration case.

To raise a case with Mastercard, you can either use Smart Client or you can file arbitration cases directly with Mastercard using the Mastercom UI.

**Note:** To access case filing functionality, you require the appropriate user permissions which you must request from GPS. Contact your Account Manager for more information.

The following section explains how to use Smart Client to raise a case with Mastercard, and view cases.

#### 12.2.1 Creating a Case in Smart Client

From the **View Transactions** screen:

1. Right click on the second presentment transaction.
2. Select **Actions > Create Case Filing**.

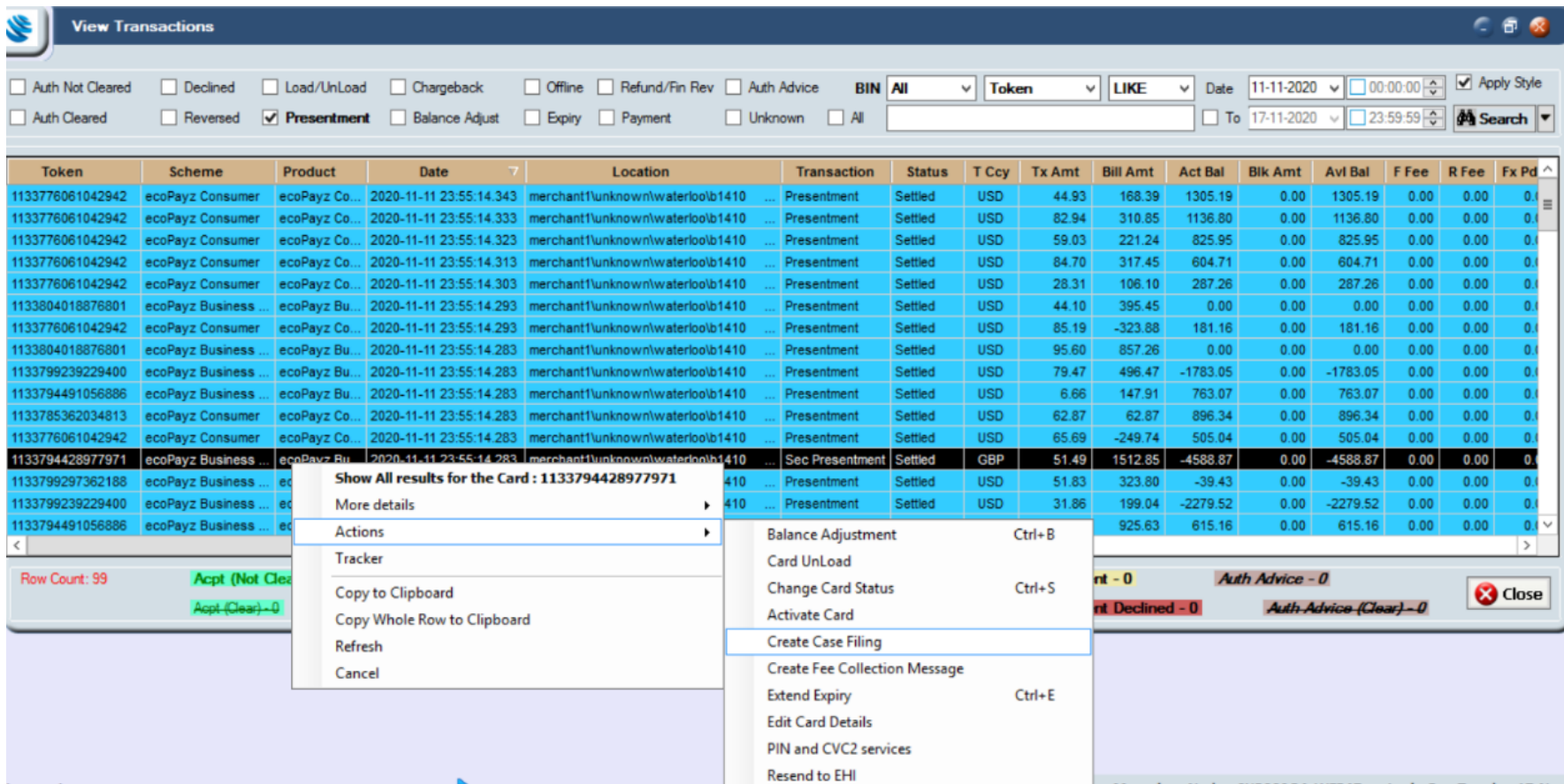


Figure 48: Create Case Filing menu option

The **Create Case Filing** screen appears showing the second presentment details:

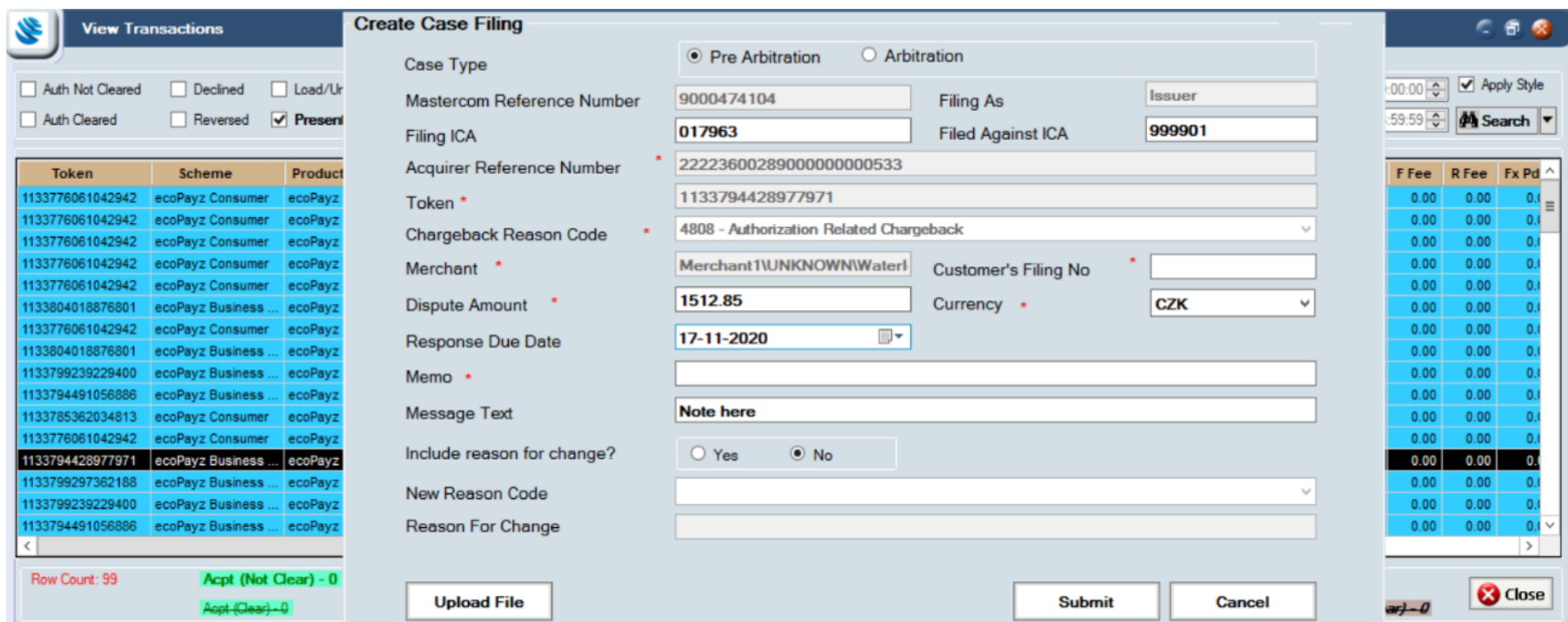


Figure 49: Create Case Filing Screen

- Choose whether to raise a **Pre Arbitration** or an **Arbitration** case.
- To upload a file, select **Upload File**. The following screen appears where you can select the file you want to upload.

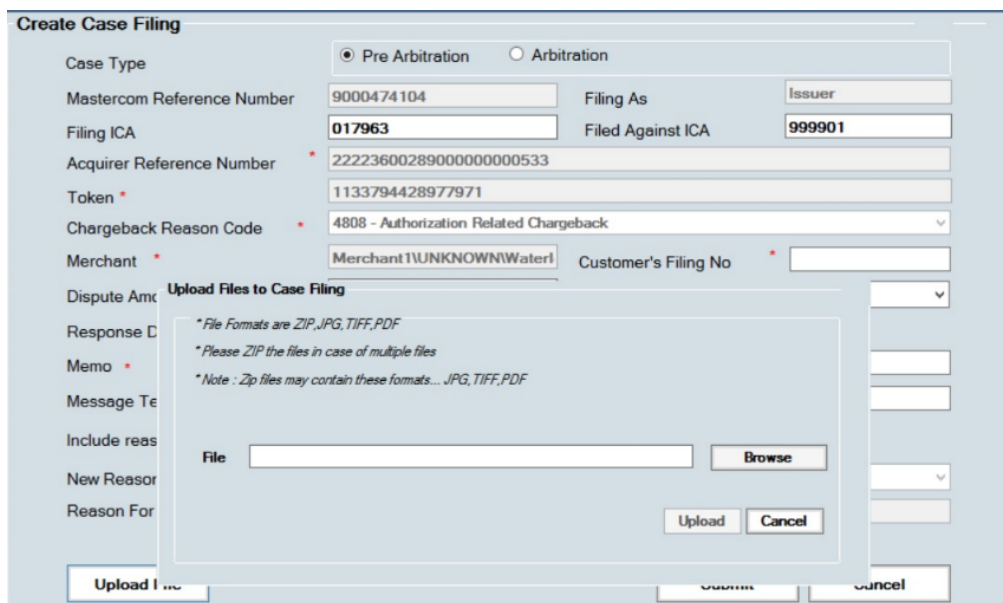


Figure 50: Upload Files to Case Filing Screen

5. Click **Submit** to create the case.

12.2.2 Viewing Cases

To view cases using Smart Client, select **Card activity > Case Filing**. The **Case Filing** screen appears.

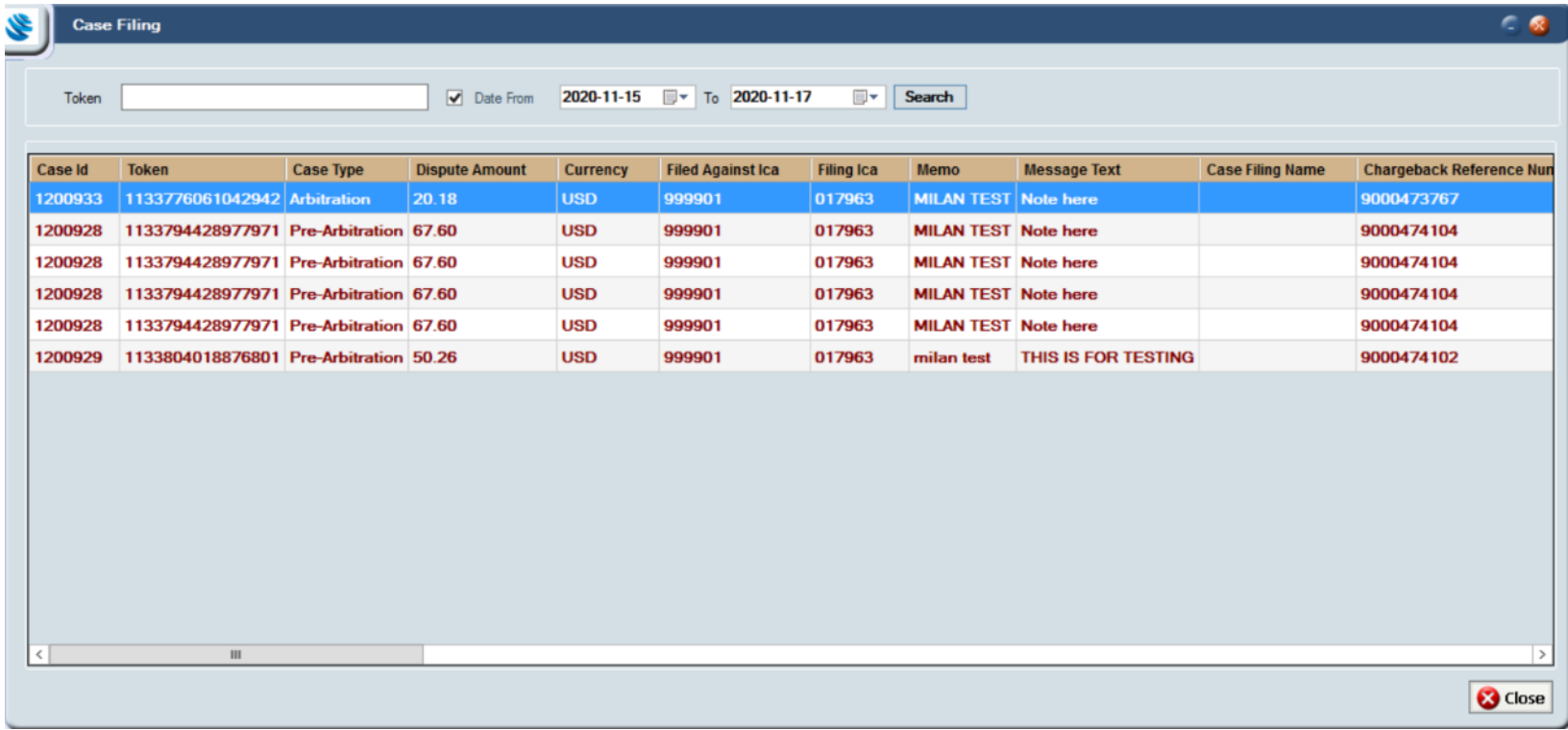


Figure 51: Case Filing Screen

12.2.3 Updating a Case

To update a case:

- Select **Card activity > Case Filing**.
- Right click a file and choose **Update Case Filing**. The following screen appears:

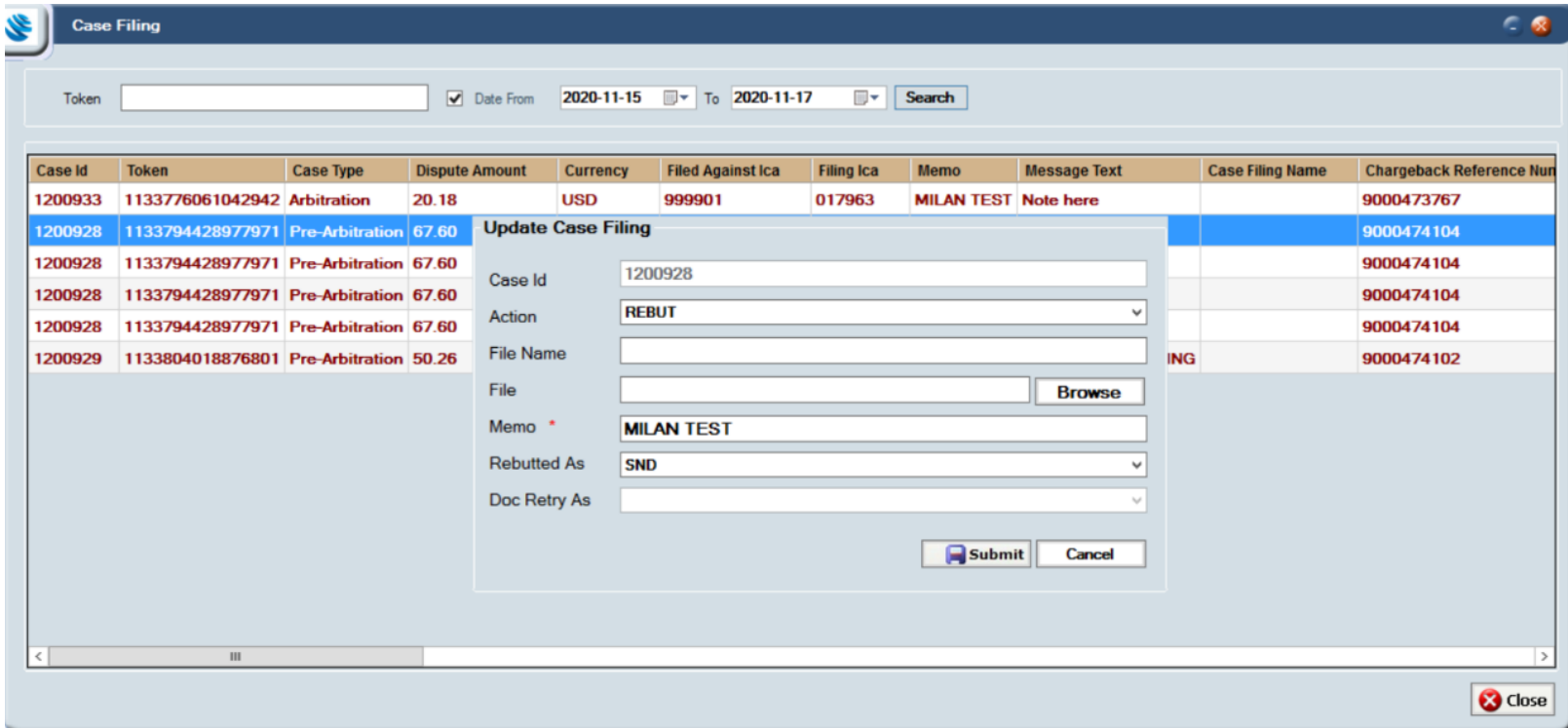


Figure 52: Update Case Filing Screen

- Choose whether to **Escalate**, **Withdraw**, **Rebut**, or **Doc\_Retry**.
- Select **Submit**.

### 12.2.4 Viewing the Status of a Case

To retrieve the status of a case:

- Select **Card activity > Case Filing**.
- Right click a file and choose **Retrieve Case File Status**.

A screen appears showing the status of the case:

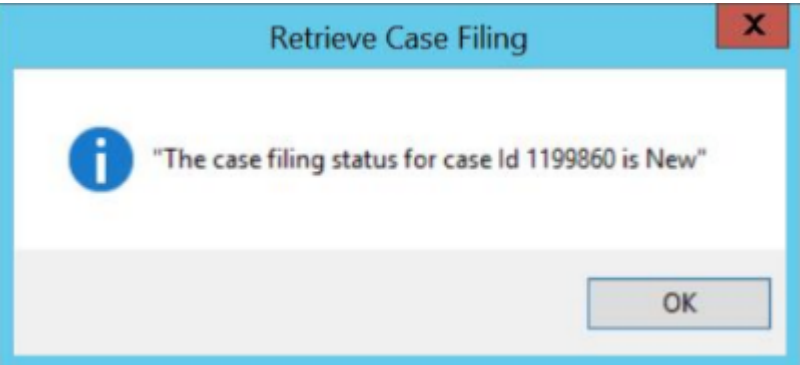


Figure 53: Retrieve Case Filing Screen

### 12.2.5 Downloading a Case Document

You can use the download functionality to check what documents you uploaded as part of the case.

To download a document associated with a case:

1. Select **Card activity > Case Filing**.
2. Right click a file and choose **Download Case Filing file**.
3. When prompted, confirm that you want to proceed with the download.

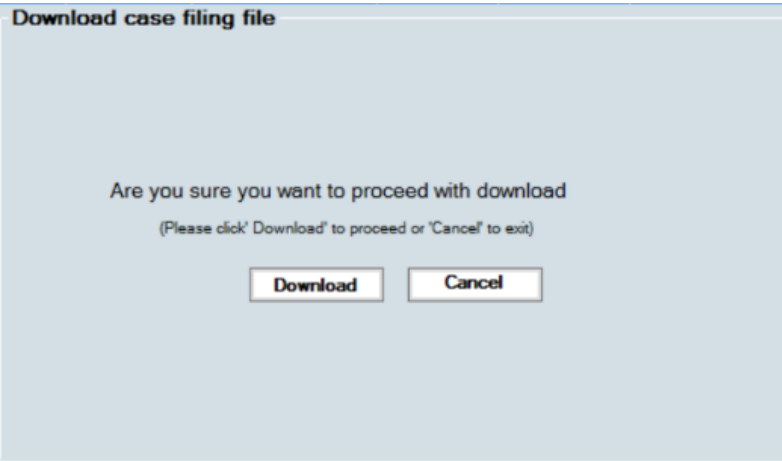


Figure 54: Download Case Filing File Screen

## 12.3 Crediting a Successful Case

This section explains how to credit a successful case to the cardholder.

Unlike chargebacks, upon a successful case filing there is no simple method to credit funds directly into the cardholder’s account. This is because there is no transaction record created at card level for arbitration/pre-arbitration case filings, and therefore no way to link arbitration information to the original transaction.

Instead, after identifying that a case filing is successful, you must credit the funds via a balance adjustment or load.

## 12.4 Viewing Case Filing Fees

This section explains how to see information relating to the fees associated with the case filing.

All fees related to arbitration/pre-arbitration case filing records from Mastercard are included in the MastercardFee section of the Transaction XML reports. For more information, see the [Transaction XML Reporting Guide](#).

# 12.5 Example Case Filing Scenarios

The following scenarios show which party incurs a pre-arbitration fee in a pre-arbitration case involving claims with first chargebacks cleared on or after 17 July 2020.

Billing Event Number	Billing Event Number	Service ID
2MS2601	Pre-arbitration—Receiver	MS
2MS2602	Pre-arbitration—Sender	MS

**Scenario 1**

Acting as the sender, an issuer sends a pre-arbitration case to an acquirer. Acting as the receiver, the acquirer decides that the transaction is its responsibility. The acquirer accepts the case and financial responsibility for it. The disputed amount returns to the issuer. Mastercard assesses billing event 2MS2601; Mastercard does not assess billing event 2MS2602.

**Scenario 2**

Acting as the sender, an issuer sends a pre-arbitration case to an acquirer. Acting as the receiver, the acquirer decides that the transaction is not its responsibility. The acquirer rejects the case and does not assume financial responsibility for it. Mastercard assesses billing event 2MS2602; Mastercard does not assess billing event 2MS2601.

After the acquirer rejects the pre-arbitration case, the issuer, if permitted by the rules, may escalate the case to an arbitration case.

**Scenario 3**

Acting as the sender, an issuer sends a pre-arbitration case to an acquirer. Acting as the receiver, the acquirer does not respond in the required time frame as chargeback rules specify. Mastercard automatically rejects the case. The acquirer does not assume financial responsibility for the case. Mastercard assesses billing event 2MS2602; Mastercard does not assess billing event 2MS2601.

After the acquirer does not respond in the required time frame, the issuer, if permitted by chargeback rules, may escalate the case to an arbitration case.

**Scenario 4**

Acting as the sender, an issuer sends a pre-arbitration case to an acquirer. However, before the acquirer, acting as the receiver, takes action on the case or before Mastercard automatically rejects the case, the issuer withdraws the case. The acquirer does not assume financial responsibility for the case. Mastercard assesses billing event 2MS2602; Mastercard does not assess billing event 2MS2601.



# 13 Managing MDES/VDEP cards

This topic explains how to use Smart Client to view information about MDES- and VDEP-enabled cards, and describes the different MDES and VDEP transaction processes and processing codes.

MasterCard’s Digital Enablement Service (MDES) and Visa’s Digital Enablement Programme (VDEP) deliver EMV-level security for contactless and in-app payments, allowing cardholders to pay using digital wallets. The GPS platform supports numerous digital wallets including Google Pay, Apple Pay, Samsung Pay, Garmin Pay, Fit Bit Pay, Mont Blanc Pay and Sony Pay.

MDES and VDEP work by replacing card numbers with unique payment tokens which differ to GPS Tokens. Tokens are placed into digital environments (a mobile wallet). During a transaction, the process maps tokens to underlying card numbers (FPAN) cryptographically, and acts as a centralised hub connecting the Issuer with Digital Wallet Providers such as Apple, Google, and Samsung. This enables connected devices to make purchases in-store, in-app or online.

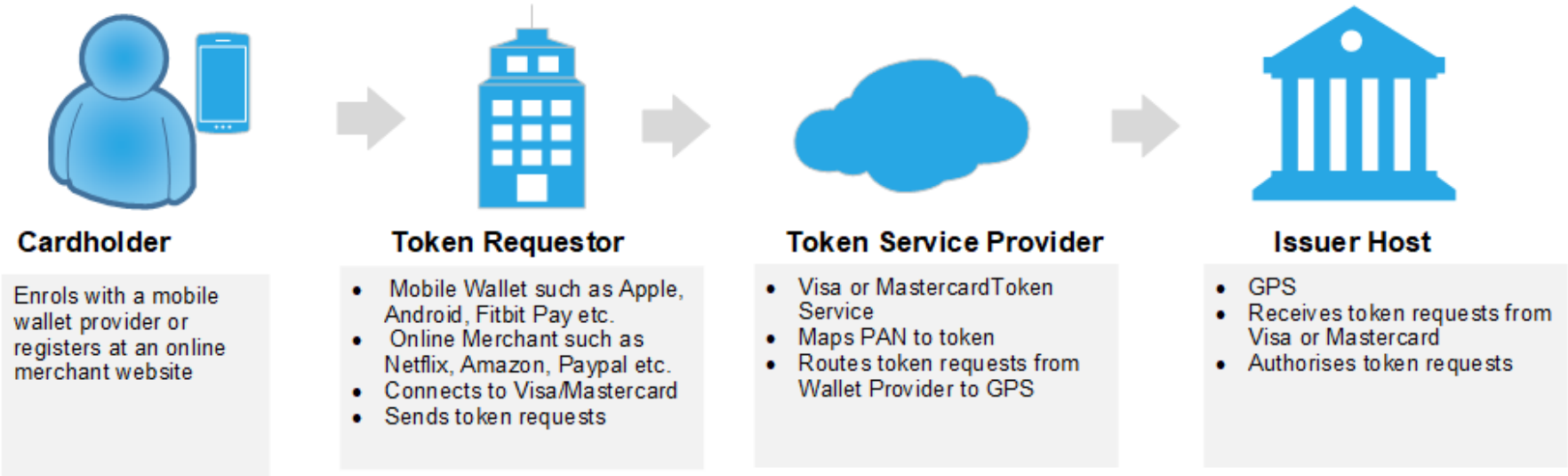


Figure 55: Parties involved in the MDES/VDEP tokenisation flow

MDES/VDEP validates the transaction, maps from the token back to the PAN and forwards it to the issuer for authorisation. For more information about tokenisation, token provisioning and use cases, see the *GPS Tokenisation Service Guide*.

## 13.1 Identifying MDES and VDEP-enabled Cards

MDES Transactions are identified as `<Merch_Name_DE43>Mastercard St. Louis MO </Merch_Name_DE43> using <MCC_Code>5969</MCC_Code>`

VISA Transactions are identified as `<Merch_Name_DE43 visa tokenisation system foster city us </Merch_Name_DE43>`

## 13.2 About the Transaction Process

This section describes the main MDES and VDEP transaction processes and processing codes you will see within Smart Client. For a detailed description of these, see the the *GPS Tokenisation Service Guide*.

### 13.2.1 VDEP transaction process

The main VDEP transaction processing codes are identified using the codes 33, 36 and 35 (which do not always follow in order):

- Token Authentication Request (TAR) — 330000
- Token Event Notification (TEN) — 360000
- Tokenisation Complete Notification (TCN) — 350000

visa tokenisation system foster city us	Auth Advice	Accepted	USD	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	Tokenisation Complete Notification	504832
visa tokenisation system foster city us	Auth Advice	Accepted	USD	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	Token Event Notification	504389
visa provisioning service	pl	Authorisation	Accepted	USD	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	Token Authentication	504389



13.2.2 MDES transaction process

The main MDES transaction processing codes are identified using the codes 33, 34, 35 and 36 (which do not always follow in order). For example, the following shows the stages involved in registering a device via Apple Pay:

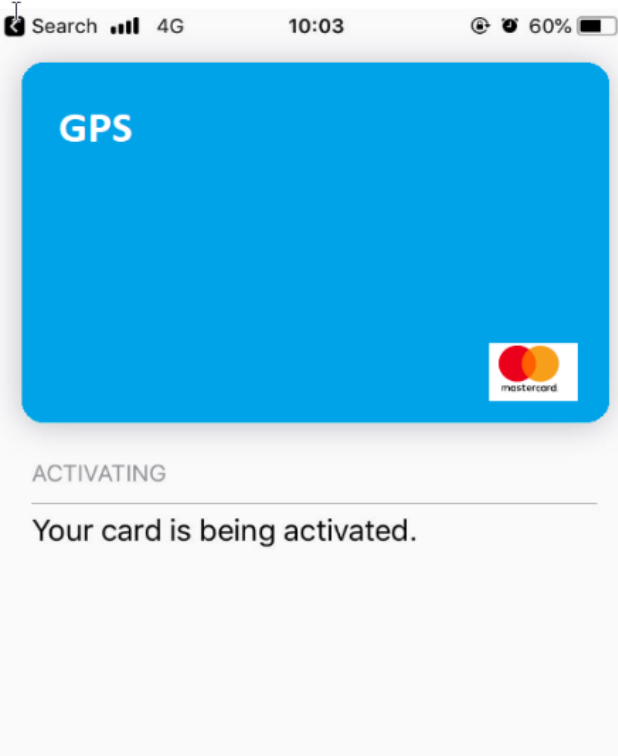
- Token Authentication Request (TAR) — 330000
- Activation Code Notification (ACN) — 340000
- Tokenisation Complete Notification (TCN) — 350000
- Debit goods and services (000000 — AVS Check)

Date	7	Location			Transaction	Status	T Ccy	Tx Amt	Bill Amt	Act Bal	Blk Amt	Avl Bal	F Fee	R Fee	Fx Pdg	MCC Pdg	Process	
2019-05-20 10:30:20.080		tesco stores 6346	aldgate	gbr	Authorisation	Accepted	GBP	3.00	-3.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	Debits (goods and services)	9
2019-05-20 10:03:58.383		mastercard	st. louis	mo	Authorisation	Accepted	USD	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	Tokenisation Complete Notifica...	4
2019-05-20 10:03:42.900		mastercard	st. louis	mo	Authorisation	Accepted	USD	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	Token Authentication	2

13.2.3 About the processing codes

Token Authentication Request (TAR) — 330000

The Tokenization Authorisation Request (TAR) allows GPS to provide a real-time decision as to whether the token service provider (MDES/VDEP) can digitize a card and designate a token on their behalf.



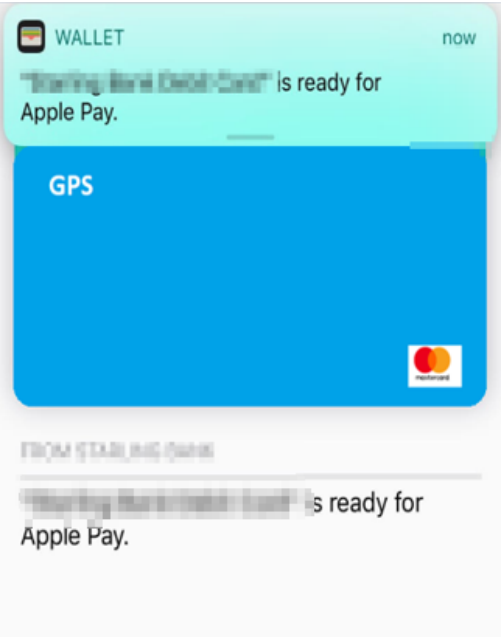
Authorisation	Accepted	USD	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	Token Authentication	
---------------	----------	-----	------	------	------	------	------	------	------	------	------	------	------	------	------	------	----------------------	--

Activation Code Notification (ACN) — 340000

This is received by GPS from Mastercard and contains the Activation Code Notification (ACN) message. This signals GPS to provide the cardholder with an authentication code as a second means of Authentication. Depending on setup, these Activation codes are sent via SMS by GPS, or provided via EHI message to indicate One Time Passcode (OTP).

mastercard	st. louis	mo	Authorisation	Accepted	USD	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	Activation Code Notification	4
------------	-----------	----	---------------	----------	-----	------	------	------	------	------	------	------	------	------	------	------	------	------------------------------	---

Tokenisation Complete Notification (TCN) — 350000



This the final step in the digitisation process to confirm the setup of the token was successful. This message, constructed in a similar format to the previous MDES/VDEP messages, contains all the details of the tokenisation including, but not limited to:

mastercard	st. louis	mo	Authorisation	Accepted	USD	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	Tokenisation Complete Notification
------------	-----------	----	---------------	----------	-----	------	------	------	------	------	------	------	------	------	------------------------------------

Token Event Notification (TEN) — 360000

Part of the post-digitisation flow, this informs the issuer of unsuccessful Activation Code entry attempts and subsequent invalidation of an Activation Code or when a token is suspended, resumed or de-activated.

13.3 Finding MDES/VDEP Data on Smart Client

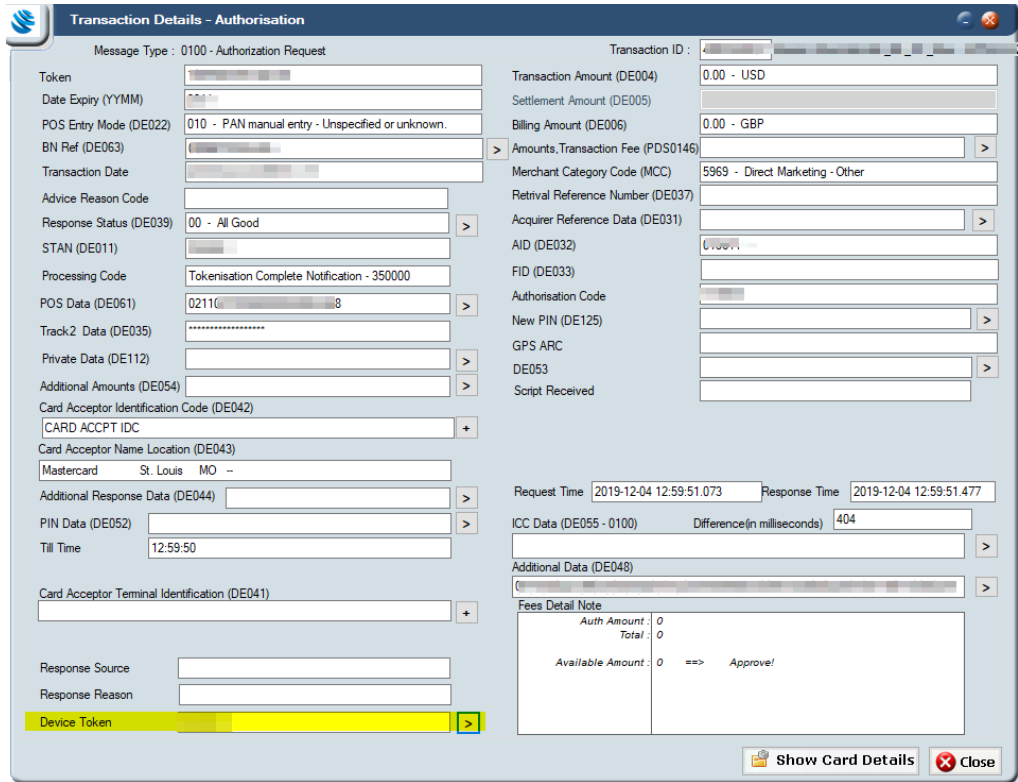
A payment token, also known as a DPAN (or Device PAN), is a new digital PAN created by Mastercard or VISA and placed on a device which is then linked to the original issuer PAN. A DPAN is the byproduct of Tokenisation Completion (TCN) which GPS references as the <Payment\_Token>.

13.3.1 Locating Device Token Data

To find information about the device token in Smart Client:

1. Select an Authorisation in the **View Transactions** screen, right-click and select **More details > View Transaction Details**.

The **Transaction Details** screen appears.



2. Expand the arrow next to **Device Token** (bottom left). Device token details are displayed.

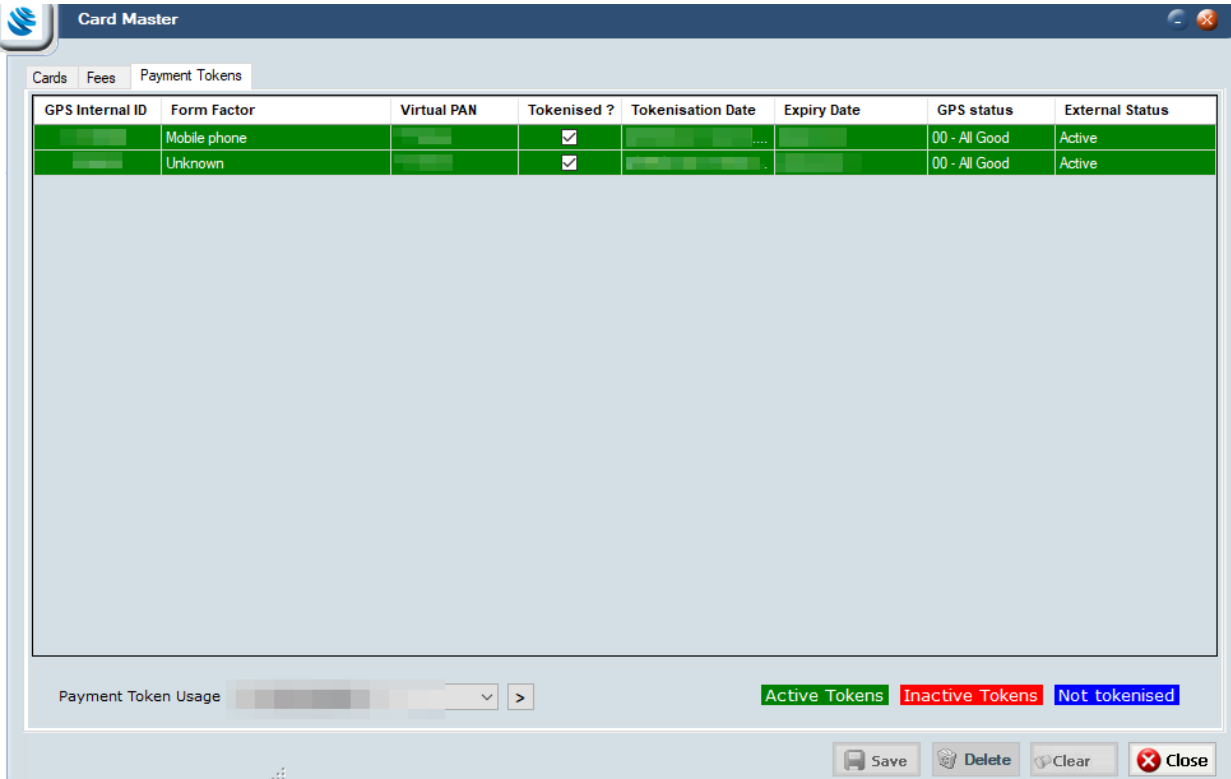
**Note:** Depending on how your product is set up, the status of the physical/virtual card is taken into consideration during the authorisation process. For example, the card status may be ignored, or if the card status is anything other an 00 (All Good), the authorisation is declined.

13.3.2 Locating MDES/VDEP Device Status

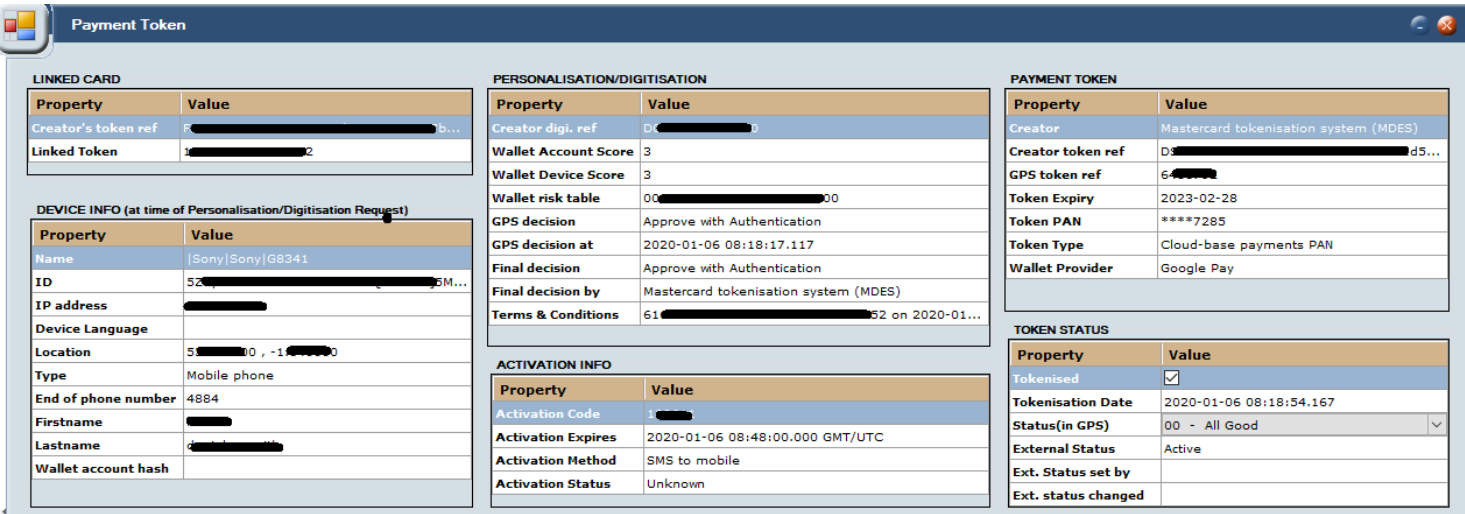
Using SmartClient, you can identify how many devices a token has been registered to and the status of the wallet on each of those devices. You can also update the status of the token.

To find information about the device status:

1. Select an Authorisation in the **View Transactions** screen, right-click and select **More details > Card Details, inc Fees**.
- **Form Factor** shows the type of device being used for the wallet (for example, a mobile phone, tablet or watch).
  - The colour indicates whether the device is active, inactive or not tokenised (cancellation). The colours are explained in the key at the bottom of the screen.



2. Double-click a green entry to open the Payment Token. Information similar to the following is shown:



3. Update the token status if necessary.

13.4 MDES/VDEP EHI Considerations

MDES messages are also sent through GPS's Authorisation system and are processed as transactions and sent through EHI (External Host Interface). The attributes remain unchanged, such as:

- MTID = 0100
- Txn\_Type = A
- Transaction Amount = 00

For more information, see the *External Host Interface (EHI) Guide*.

## 13.5 Using MDES/VDEP Web Services

Currently, GPS offers two Web Service APIs relating to MDES/VDEP:

- `Ws_Payment-Token_StatusChange` — use this to change the status of an MDES and VDEP Payment Token Card.
- `Ws_Payment-Token_Get` — use this to get the details for MDES Payment Token Cards.

For more information, see the *Web Services Guide*.

# General FAQs

This section provides answers to frequently-asked questions.

## Smart Client Setup

### Q. Does Smart Client work on a Mac?

Smart Client is not currently supported on Apple OSX. For more information, see [System Requirements](#).

### Q. Why can't I see a function in Smart Client?

What you can see and do in Smart Client depends on your role and permissions. If you cannot see a menu option, this may be because you do not have the appropriate permissions. For more information, see [About roles and permissions](#).

## Searching and Filtering

### Q. Why can't I see a transaction in Smart Client?

If the authentication process fails before a transaction reaches the GPS system, the transaction will not show up in Smart Client. For example, if a transaction is authenticated through a 3-D Secure (3DS) provider (for example, Cardinal Consumer Authentication), and fails, it will not appear in Smart Client. Similarly, if a customer removes their card from a card reader too quickly, the authentication process fails and the transaction will not show up.

Archived tokens and transactions also do not appear within Smart Client – see below for more information.

### Q. How do I retrieve archived tokens and transactions?

Depending on product set up, transactions are typically archived after 90 days. Dormant cards with a particular status (such as card destroyed or expired) are also archived after a period of inactivity.

To retrieve tokens and transactions from the archive so you can view information about them using Smart Client, raise a ticket with GPS.

### Q. How do I match transactions?

You can match transactions such as authorisations to presentments using the **Show transaction lifecycle** option. This displays all transactions that match the one you have selected.

**Note:** This option appears only if there is a matching transaction. If Smart Client does not find a matching transaction, this option is not visible.

- Select a transaction, right click and choose **More details > Show transaction lifecycle**.

Alternatively, to find matching transactions in Smart Client, search on fields such as the System Trace Audit Number (STAN), Trace-id or Approval ID. Avoid trying to match fields that can change across transactions, such as location. For more information about matching logic, see the *External Host Interface (EHI) Guide*.

**Note:** If more than 30 days has elapsed between the authorisation and presentment, you will be unable to match these.

## Managing Tokens and Transactions

### Q. Can I reset card limits?

You can view the limits that apply to a card which were configured during product setup, however, you cannot change these limits in Smart Client. To change card limits, contact your Account Manager.

### Q. What do I do if I suspect a BIN attack?

The BIN is the first 6 digits of a card number which correspond to a card scheme. A BIN attack is when a fraudster attempts to identify a valid card by using the BIN, randomly changing the remaining ten digits and flooding the system with transactions. If a response (such as 'incorrect expiry date') is returned, this indicates a genuine card and the fraudster may attempt to use this card number to access funds illegitimately.

In the event of a BIN attack, Smart Client displays a high volume of declined transactions with a Response Status (DE039) '14 - Invalid card number (no such number)'. Typically, these transactions have the same BIN, merchant name, and Acquirer ID (AID) and the Notes field shows the reason for the decline as unknown card number, unknown PAN and unknown token.

Where a specific merchant location is used for BIN attacks, although no valid transactions are observed there across the entire GPS client portfolio, GPS blocks the merchant location. This will prevent successful transactions should a fraudster generate valid card details as part of a BIN attack using that merchant location.

## Notes

- GPS will not block merchant locations where there is a mix of fraudulent and seemingly valid transactions as this would impact legitimate cardholder transactions.
- GPS will also not block merchant locations where only a small volume of transactions synonymous with a BIN attack are observed.
- Fraudsters are likely to switch merchant locations but this measure will frustrate their efforts as it will affect merchants where controls are weakest or where there may be collusion.
- This is an additional proactive step GPS applies on exceptional occasions based on dual review. This should not in any way reduce the fraud prevention tools and practices Issuers and Program Managers have in place, nor does it imply any responsibility on the part of GPS for fraud prevention outside of the normal processor remit.
- This block will apply across all GPS client programmes.

GPS recommends the use of GPS Protect to help guard against fraud. GPS can also offer 3D Secure using Adaptative Authentication which reduces friction in the transaction process versus traditional 3D Secure. For information about these products, contact your GPS Account Manager.

### Q. How do I change the status of a card to Card Destroyed?

You can change the status of a card to prevent it from being used by setting the card status to 83—Card Destroyed. You can set the status in Smart Client or by using Web Services (Ws\_StatusChange). For example, you may want to destroy a card if you suspect fraudulent behaviour. This will block most functions on the card, such as authorisations and loads, rendering the card unusable. However, presentments and refunds, because they are part of the financial record, will continue to process on cards with this status.

**Note:** Changing a card's status to '83—Card Destroyed' is not reversible.



# Troubleshooting FAQs

This section provides answers to common troubleshooting issues.

## General Issues

### Cannot Download or Install Smart Client

- Solution 1: Ensure that your Popup-blocker/Antivirus allows you to launch the software.
- Solution 2: Use Internet Explorer or Microsoft Edge, as there are multiple software settings and software versions that can cause conflicts and prevent a successful installation. Currently, you cannot download and install Smart Client on Apple OSX.

### Smart Client does not start

- Solution: Uninstall Smart Client and then reinstall it. For more information, see [Installing the Smart Client application](#).

### Forgotten username and/or password

If you forget your username or password, use the links in the GPS Smart Client Login screen to retrieve and reset these.

#### Forgotten Password?

1. Click **Forgotten password?** to go to the reset screen.
2. Provide the email address configured for GPS Smart Client and your GPS Smart Client username.  
Provided the credentials are valid a One-Time Temporary Password (OTP) is automatically sent to your email.
3. After logging in with the OTP, change your password immediately before proceeding.

#### Forgotten Username?

1. Click **Forgotten Username?** to go to the reset screen.
2. Provide the email address configured for GPS Smart Client.

Provided the email address is valid, a username reminder is sent automatically to your email.

**Note:** If you have been restricted from using the application due to multiple incorrect login attempts, contact the GPS OPS24 team at [ops24@globalprocessing.net](mailto:ops24@globalprocessing.net) (operational 24x7 everyday).

### Cannot log into Smart Client

- Solution 1: Check that your credentials are correct. Please raise a JIRA ticket or email the GPS OPS24 team at [ops24@globalprocessing.net](mailto:ops24@globalprocessing.net).
- Solution 2: Check that the computer is connected to a whitelisted VPN (Virtual Private Network)
- Solution 3: For security reasons, Smart Client will not run two instances of the program at the same time on one machine, nor will it run on two machines that share the same computer name. Refer to your Microsoft Windows documentation for information about how to check the name of your computer or rename it.

### Card declined due to failed AVS check although address details appear correct

If only a delivery (Card Purchaser) address is specified during card creation and not a cardholder address, the transaction may be declined if the customer attempts to use it for ecommerce and telephone transactions where the merchant performs an address check. This is because the address (AVS) check is performed on the cardholder address which is blank.

Typically, you'll spot this in the View Cards screen where the address is blank and the post code is 0 (zero). This indicates GPS does not hold a cardholder address and, as a result, will be unable to conduct an AVS Check (Address Verification Service).

To fix the issue for an affected card, you can use Web Services to update the cardholder address (`Ws_Update_Cardholder_Details`). For more information, see the *Web Services Guide*.

To fix the issue for an affected card using Smart Client, the customer needs to have made a transaction which will enable you to access the **Edit Card Details** option where you can update the address.

**Note:** If the customer has yet to make a transaction, use Web Services to update the cardholder address or contact GPS Support.

1. Right-click the transaction, choose **Actions > Edit Card Details**. The **Card Master** screen appears.
2. Click anywhere on the **Card Holder** pane, and then click **Save**. The Cardholder address is automatically populated with the purchaser (delivery) address, and the card will immediately be updated for AVS checks.

**Note:** If there is a requirement to later amend the Cardholder address, you can repeat this process.

**Tip!** To prevent similar issues from occurring, ensure GPS is always provided with a cardholder address during the card creation process.

## Known Issues

For a list of known issues, contact your Implementation Manager.

# Appendix A: Common Decline Reasons

This topic provides details about common card decline reasons.

Decline	Reason
DR: Auth Amount : XX.00 Total : XX.00 Available Amount: Y.00 ==> Decline!	The cardholder does not have sufficient funds to cover the transaction amount.
DR: Card expiry check failed with Emboss Expiry date (DE014)	The expiry date entered by the cardholder does not match the expiry date of the card.
DR: Exceeds Max Per Transaction limit	The attempted transaction amount exceeded the limit per single transaction amount for the card/product.
DR: Incorrect PIN	The cardholder entered an incorrect PIN.
DR: Declined due to Lost Card (Capture) (Original auth resp status 41, changed to 05)	The card's status was changed to "Lost Card (Capture)" and the card can no longer be used.
DR: Declined due to CardUsageGroupCheck GroupUsageID-42 [Card Acceptance Method (A) - Card Not Present - E-Commerce - Failed]	The card/product is not permitted to be used for e-commerce transactions.
DR: Declined due to CardUsageGroupCheck GroupUsageID-476 [Card Acceptance Method (A) - Chip PAN Entry - Signature Verification - Failed]	The card/product is not permitted to be used for signature verification authorisations.
Card CVV2 not matching with cvv2 in auth request	The CVV value entered by the cardholder is not matching the CVV value of the card.
DR: Declined due to voided card (Original auth resp status 99, changed to 05)	The status of the card was changed to "Card Voided" and the card can no longer be used for authorisations.
DR: Declined due to GroupMCCCheck	The card/product is not permitted to use this type of merchant (MCC = Merchant Category Code).

## Appendix B: Card Status Codes

This topic provides details about card status codes.

Status Code	Description	Who can set?	Functions permitted for the card	Functions blocked for the card	Example of use	Reversible
00	All Good	PM	All	None	Normal operation	YES
04	Capture Card	PM		Auths	Stolen or fraudulent use	YES
05	Do not honour	PM	Balance Adjustment	Auths	Generally, set by issuer request	YES
41	Lost card	PM		Auths, Activation	Card was lost but not stolen	YES
43	Stolen card	PM		Auths, Activation	Card was stolen	NO
46	Closed account	PM		Auths, Activation	PM closes the account	YES
54	Expired card	GPS Only		Auths, Activation	Expiry date has passed	YES
57	Transaction not permitted to cardholder	PM		Auths	POS and/or ATM can be prohibited in system settings	YES
59	Suspected fraud	PM		Auths, Activation	Suspected fraudulent use	YES
62	Restricted card	PM	Balance Adjustment	Load, Auths, Activation	Can be restricted due to rules from the PM or Issuer	YES
63	Security Violation	PM, Issuers	None	Load, Balance Adjustment, Auths	AML, KYC issue for the cardholder	YES
70	Cardholder to contact issuer	Issuer	Load, Balance Adjustment	Auths	Set by the issuer for compliance reasons	YES
83	Card Destroyed	Issuer, PM	NONE <sup>1</sup>	Auths, Activation, Load, Balance Adjustment	Set by PM	NO
98	Refund given to Customer	PM		All (check if it can be loaded)	Gift cards	YES
99	Card Voided	PM		Auths	Account is fine but card voided	YES
G1	Short-term debit block	PM	Credits	Auths (except credits) <sup>2</sup>	PM chooses this card status	YES
G2	Short-term full block	PM		Auths <sup>2</sup>	PM chooses this card status	YES
G3	Long-term debit block	PM	Credits	Auths (except credits) <sup>3</sup>	PM chooses this card status	YES
G4	Long-term full block	PM		Auths <sup>3</sup>	PM chooses this card status	YES
G5	GPS Protect short-term debit block	GPS Only	Credits	Auths (except credits) <sup>2</sup>	GPS Protect sets this status based on various criteria	YES
G6	GPS Protect short-term full block	GPS Only		Auths <sup>2</sup>	GPS Protect sets this status based on various criteria	YES
G7	GPS Protect long-term debit block	GPS Only	Credits	Auths (except credits) <sup>3</sup>	GPS Protect sets this status based on various criteria	YES
G8	GPS Protect long-term full block	GPS Only		Auths <sup>3</sup>	GPS Protect sets this status based on various criteria	YES
G9	Interactive Voice	IVR		Auths, Activation	Cardholder phoned the IVR	YES

Status Code	Description	Who can set?	Functions permitted for the card	Functions blocked for the card	Example of use	Reversible
	Response (IVR) Lost/Stolen Block (like 41 Lost)				automated phone line to block their card	

- Notes:**
- 1. For card status 83 - Card Destroyed; presentments and refunds, because they are part of the financial record, will continue to process on cards with this status.
  - 2. Merchants told to retry
  - 3. Merchants told not to retry

## Appendix C: Usage Groups

The table below describes the different types of Card Acceptance Methods available in the form of Usage groups. Rules can be set to dictate levels of Card Acceptance, such as MCC Group acceptance.

Group Type	Purpose
Card Acceptor List	You can specify at the merchant ID level where authorisations will be accepted. (Based on DE42). For example, you can allow a card to be used only in specific shops or locations. This can be applied via web services.
Card Disallow List	You can specify at the merchant ID level where authorisations will be declined. (Based on DE42). For example, you can prevent a card from being used in specific shops or locations. This can be applied via web services.
Group Web	You can charge a fee for specific web services such as a PIN change request.
Card FX Group	You can upload and manage your own Foreign Exchange rates which can be applied to authorisations and pre-sentments.
Calendar Group	You can restrict card acceptance based on specific time and date parameters. For example, a trucking company may restrict card use to weekdays from 9 until 5 to allow employees to pay for fuel. Some usage cases include religious observances or working hours.
Card Linkage	Used to link primary and secondary cards. You can apply card linkage on a shared balance or a separate balance.
Group Usage	<p>You can apply the specific “Card Usage Rules” which dictate card behaviour such as PAN entry method rules, card-holder verification, regional based rules and transaction types.</p> <p><b>Tip:</b> Check the usage rules if a card has been declined; for example, to show if transactions are prevented from going through on an unknown acceptance method.</p>
Group MCC	You can allow or disallow card acceptance (auths) based on one or more merchant category codes (MCC). For example, you can disallow gambling sites.
Group Limit	Displays specific limits assigned to that token; for example, the maximum balance permitted to be held on the card.
Group Auth	You can apply a fee to Authorisations based on the processing code; for example, an authorisation to check a balance.
Limited Network	<p>You can restrict card acceptance to a limited network only; for example, a gift card may be limited to merchants in a particular shopping centre only. This rule is based on 3 different data elements:</p> <ol style="list-style-type: none"> <li>1. DE42 – Merchant ID</li> <li>2. DE43 – Address, text field for the merchant ID</li> <li>3. DE61 – Postcode</li> </ol>
Rec Fee	You can apply fees based on rules or actions you set on the card. For example: inactivity fees and/or dormancy fees. These are configured by GPS.



# Document History

This section provides details of what has changed since the previous document release.

Version	Date	Reason	Who
3.1	12/10/22 01/10/22 24/01/22	Added a note about how card status of the card is taken into consideration during the authorisation process for tokenised cards. See <a href="#">Finding MDES/VDEP Data on Smart Client</a> . Added additional <a href="#">Card Status Codes</a> to the appendix. Added <a href="#">Case Filing</a> content.	AL
3.0	02/09/21	New version, with new content and layout.	AL
2.9	05/01/21	Formatting Updated screenshots. Updated 3D Secure.	DS
2.8	26/08/20	Updated screenshots. Chargebacks updated for Mastercom. Re-sending EHI transactions.	DS
2.7	31/01/20	Various updates including: <ul style="list-style-type: none"><li>• Removed 'Unload' from Status Code 63</li><li>• 3D Secure CAVV result</li><li>• MDES/VDEP updates</li><li>• Chargeback Updates</li></ul>	DS TB
2.6	16/04/19	Added Password reset, Balance Adjustment and Token retrieval from archive.	MB
2.5	12/06/18	Formatting. Additional functionality. Additional screenshots.	AP

# Contact Us

Please contact us if you have queries relating to this document. Our contact details are provided below.

**Global Processing Services Ltd.**  
**Support Email:** ops24@globalprocessing.com  
**Support Phone:** +442037409682

## GPS Offices

UK Central Office	Singapore	Australia	Dubai, UAE
6th Floor, Victoria House Bloomsbury Square London WC1B 4DA	Republic Plaza 9 Raffles Place Singapore 048619	Stone & Chalk Level 4, 11 York Street Wynyard Green Sydney, NSW, 2000	EO 10, Ground Floor, Building 1 Dubai Internet City Dubai, United Arab Emirates

## Technical Publications

If you want to contact our technical publications team directly, for queries or feedback related to this guide, you can email us at: [docs@globalprocessing.com](mailto:docs@globalprocessing.com).

# Glossary

This page provides a list of glossary terms used in this guide.

## 3

### 3D Secure (3DS)

3D Secure is a technical standard adding an extra layer of security to Visa and Mastercard transactions over the Internet (eCommerce)

## A

### AccBal

Account Balance

### ACN

Activation Code Notification (340000)

### 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 card-holders.

### Act Bal

Actual Balance

### AFD

Automated Fuel Dispenser

### AID

Acquiring Institution Identification Code

### API

Application Programming Interface

### ARQC

Authorisation Request Cryptogram

### Authentication

This includes checks to confirm the cardholder identity, such as PIN, CVV2 and CAVV.

### 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.

### Automated Fuel Dispenser (AFD)

Automatic fuel dispensers (AFDs) are used at petrol or gas stations for customer self-service fuel payments. Typically the customer inserts their card and enters a PIN number and the AFD authorises a fixed amount (e.g. £99). Once the final payment amount is known, the AFD may reverse the authorisation and/or request a second authorisation.

### AvlBal

Available Balance

### AVS

Address Verification Service

## B

### Base Currency

Typically considered the domestic currency or accounting currency for the card

### Bill Amt

Billing Amount

### Billing Currency

The currency you choose to be billed in

### BIN

Bank Identification Number (First 6 digits of the 16-digit PAN)

### BlkAmt

Blocked Amount

C

**Card Scheme**

Card network, such as MasterCard or Visa, responsible for managing transactions over the network and for arbitration of any disputes

**Cardholder**

Consumer or account holder who is provided with a card to enable them to make purchases

**Case filing**

A feature through which an issuer or an acquirer can raise a concern with Mastercard.

**CAVV**

Cardholder Authentication Verification Value

**CB**

Chargeback

**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 File/Clearing Transaction**

GPS receive batch clearing files from the card networks, containing clearing transactions, such as presentments and network fees. The card issuer transfers the requested settlement amount to the acquirer and 'clears' the amount on the card, reducing the available card balance accordingly.

**CRI**

Card Request Interface

**CS**

Customer Support

**CVC**

Card Validation Code

D

**DCC**

Dynamic Currency Conversion

**DE000-DE999**

Data Element (000-999) number. For full details of each element, see the card scheme customer interface specification manual

**DPAN**

Device Primary Account Number

E

**EH**

External Host Interface

**EMV**

EMV originally stood for "Europay, Mastercard, and Visa", the three companies which created the standard. EMV cards are smart cards, also called chip cards, integrated circuit cards, or IC cards which store their data on integrated circuit chips, in addition to magnetic stripes for backward compatibility.

**External Host**

The external system to which GPS sends real-time transaction-related data. The URL to this system is configured within GPS per programme or product. The Program Manager uses their external host system to hold details of the balance on the cards in their programme and perform transaction-related services, such as payment authorisation, transaction matching and reconciliation.

F

**F Fee**

Fixed fee

**Fee Groups**

Groups which control the card transaction authorisation fees, and other fees, such as recurring fees and GPS web service API fees.

**FID**

Forwarding Institution Identification Code

**FPAN**

Funding Primary Account Number

**FX**

Foreign Exchange

**FX Market**

The currency market in which the FX Provider operates, such as London or the US. Currencycloud only operate in the one market

**FX Provider**

The currency conversion rate provider, such as Currencycloud

**FxPdg**

Foreign Exchange Padding - padding for currency conversion, to compensate for any fluctuations in currency exchange rates between the authorisation and the presentment

**Issuer**

The card issuer, typically a financial organisation authorised to issue cards. The issuer has a direct relationship with the relevant card scheme.

**Mastercom**

Create and manage dispute claims in Mastercom

**MCC**

Merchant Category Code - The type of merchant

**MCC Pdg**

Merchant Category Code Padding - padding for particular merchants who do the pre-authorisations

**MDES**

Mastercard Digital Enablement Service

**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 identify the type of account provided to them by their acquirer.

**MX**

Multi-Currency Card

**MultiFX**

A GPS feature for seamless currency conversion. MultiFX lets customers hold different balances in different currencies simultaneously in one wallet

**MVC**

Master Virtual Card

**Offline Transaction**

This is often used in scenarios where the merchant terminal is not required to request authorisation from the card issuer (for example for certain low risk, small value transactions used by airlines and transport networks). The card CHIP EMV determines if the offline transaction is permitted; if not supported, the terminal declines the transaction. Note: Since the balance on the card balance is not authorised in real-time, there is a risk that the card may not have the amount required to cover the transaction.

**OTP**

One Time Passcode/ Activation code sent to the cardholder for use in authenticating

**PAN**

Primary Account Number

**PM**

Program Manager

**PoS**

Point of Sale

**POSFX**

A GPS feature which makes spending abroad easy with realtime and transparent point-of-sale FX rates

**Presentment**

The payment has been financed and taken by the merchant bank

**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.

**R**

**R Fee**

Rate fee - Fee based on the transaction amount

**S**

**SC**

Smart Client (Card Processor Front End)

**Smart Client**

Smart Client is GPS's user interface for managing your account on the GPS Apex system. It is also called Smart Processor GPS. Smart Client is installed as a desktop application and requires a VPN connection to GPS systems in order to be able to access your account.

**STAN**

System Trace Audit Number

**Stand In Processing (STIP)**

The card network (Visa and Mastercard) may perform approve or decline a transaction authorisation request on behalf of the card issuer. Depending on your GPS mode, GPS may also provide STIP on your behalf, where your systems are unavailable.

**T**

**TAR**

Token Authentication Request (330000)

**TCcy**

Transaction Currency

**TCN**

Tokenisation Complete Notification (TCN) - 350000

**TEN**

Token Event Notification (TEN) - 360000

**Token**

The obfuscated 16 or 9-digit Card Number

**Triple DES**

Triple DES (3DES or TDES), is a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block to produce a more secure encryption.

**TxAmt**

Transaction Amount

**Txn**

Transaction

**V**

**Validation**

Checks to confirm the card is valid, such as CHIP cryptograms, mag-stripe data (if available) and expiry date

**VDEP**

Visa's Digital Enablement Program

**VPN**

Virtual Private Network

**VROL System**

Visa Dispute Resolution Online system, provided by Visa for managing transaction disputes.