Smart Client Guide

Version: 3.6

29 January 2026

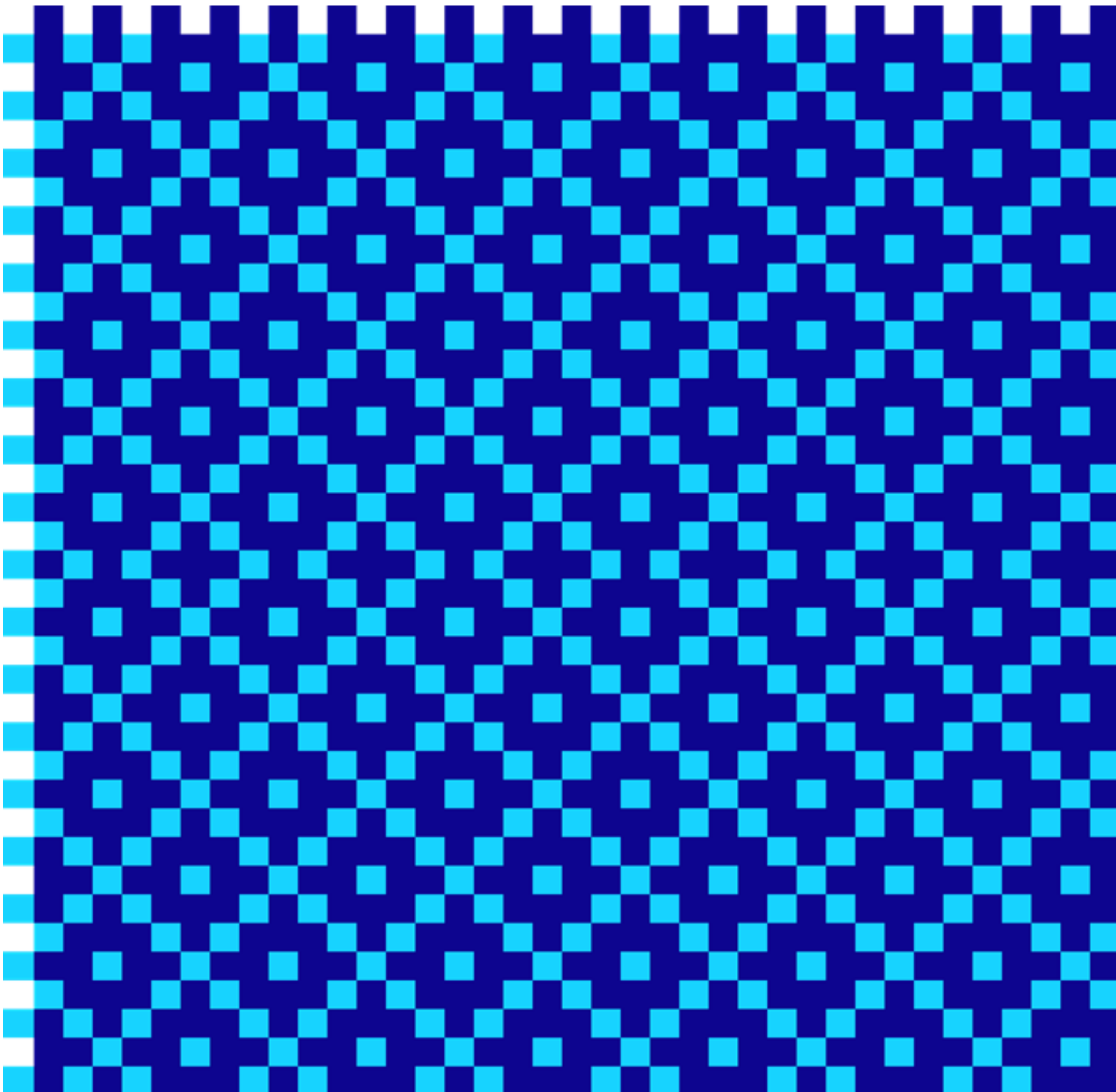
Publication number: SCG-3.6-1/29/2026

For the latest technical documentation, see the Documentation Portal.

Thredd, Kingsbourne House, 229-231 High Holborn, London, WC1V 7DA

Support Email: occ@thredd.com

Support Phone: +44 (0) 203 740 9682



Copyright

About this document

This guide describes the Thredd Smart Client portal which is part of the Thredd 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
Web Services Guide	How to use the SOAP Web Services API to integrate your applications to Thredd.
Cards API Website	How to use the REST-based Cards API to integrate your applications to Thredd.
External Host Interface (EHI) Guide	How to use the Thredd External Host Interface (EHI), and specifications on how to process and respond to messages received from EHI.
3D Secure Guide (Apata)	How to use the Thredd 3D Secure Realtime Data eXchange (RDX) service and how to implement a 3D Secure project with biometric/In-app authentication.
Fees Guide	How to set up and manage card fees for your card products on the Thredd system.
Payments Dispute Management Guide	Describes the payments dispute management process and how Thredd supports chargeback management.
Tokenisation Service Guide	About the Mastercard and Visa token services and how Thredd supports tokenisation (digital wallets).

Tip: For the latest technical documentation, see the Documentation Portal.

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.

1 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 Thredd 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.

1.1 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:

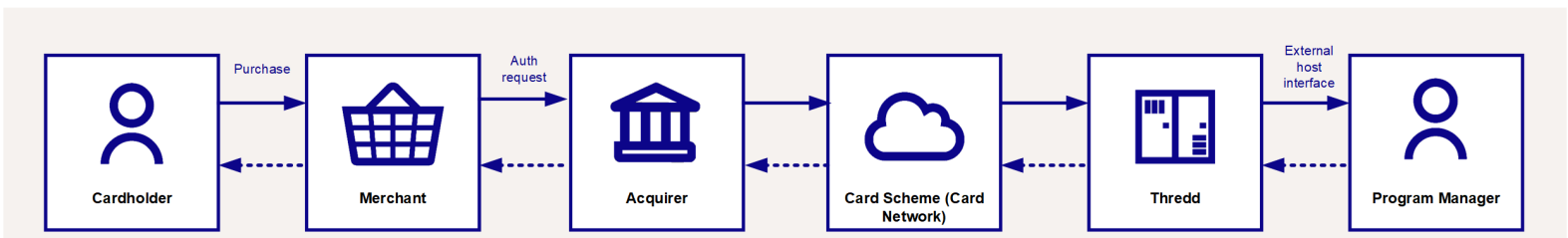


Figure 1: Parties involved in the payment process.

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 (payment network). The authorisation request is passed to Thredd 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.

1.1.1 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. Thredd 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 Thredd 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 Thredd card must hold a sufficient balance to enable a card payment.

Thredd provides web services (APIs) to create cards.

1.1.2 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.

1.1.3 Tokens

Tokens enable you to use the Thredd 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. Thredd 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 Thredd refers to as the Visa Digital Enablement Program (VDEP). Thredd supports both tokenisation services.

1.1.4 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.

1.1.5 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.

1.1.6 Thredd Platform

The Thredd Platform is a robust, scalable issuer processing platform that is certified by Mastercard and Visa. The Thredd Platform 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 Thredd platform.

1.1.7 External Host Interface (EHI)

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

1.1.8 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*.

1.1.9 Program Manager (Issuer)

A Thredd 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 (payment network).

2 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.

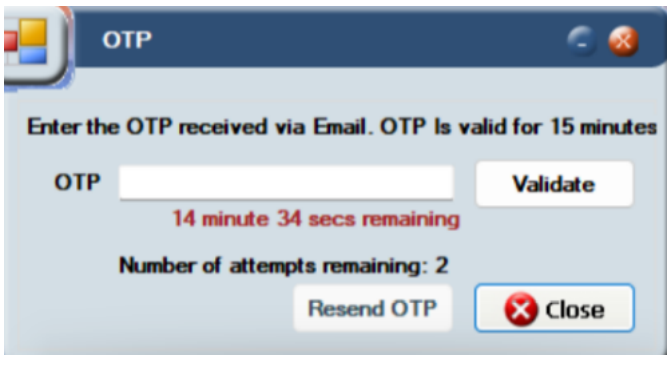
Step 1 - Install and launch Smart Client

Smart Client is installed as a desktop application and requires a secure connection to Thredd 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 - Enter OTP Code

Enter the OTP code in Smart Client to provide an added layer of protection through Multi-Factor Authentication (MFA). When logging in to Smart Client, a window displays requesting the six-digit One-Time Password (OTP) that is sent to the user's email address. This password is valid for 15 minutes and must be entered to complete the login process. When you have entered the OTP value from the email, click **Validate**.



A user has a total of six attempts to log in successfully to Smart Client. When all attempts to log in have been exhausted, the user account is locked and you will need to contact Thredd support to unlock the account.

If you do not receive an email with the OTP code, click Resend OTP to send the email again. This button is greyed out for the first 60 seconds after Thredd sends an email. You are allowed to press the button three times before the functionality to send the OTP is disabled. A message on the window displays how many attempts for resending an OTP are left.

Step 3 - 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 4 - 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 5 - 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.

3 Installing Smart Client

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

Note: Ensure you have a secure connection to Thredd in place.

3.1 System Requirements

To install the Thredd 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 5 (x64)
- Microsoft .Net Framework 4.8 (x64)
- Microsoft Visual Studio 2019 (version 16.11.31)

To install the prerequisite software, use Microsoft Edge to click on the link below that is relevant to your environment.

Environment	Url
PRD0	https://psc7rrlo4.globalprocessing.net/smartclient/publish.htm
PRD1	https://awsp1sc7rrlo9.globalprocessing.net/SmartClient/publish.htm
PRD2	https://awsp2sc7rrlo9.globalprocessing.net/SmartClient/publish.htm
PRDZ (mTLS)	https://pz-smartclient.thredd.net/publish.htm
PRDZ (non-mTLS)	https://p0sc7dr01.globalprocessing.net/SmartClient/publish.htm
PRD1 (mTLS)	https://p1-smartclient.thredd.net/publish.htm
PRD2 (mTLS)	https://p2-smartclient.thredd.net/publish.htm

To install the User Acceptance Testing (UAT) version of Smart Client:

1. Follow one of the following links using Microsoft Edge: https://sc-uat.globalprocessing.net/SmartClient/publish.htm (for non-mTLS), or https://sc-uat.thredd.net/ (for mTLS).

   Note: Thredd recommends you use Microsoft Edge.

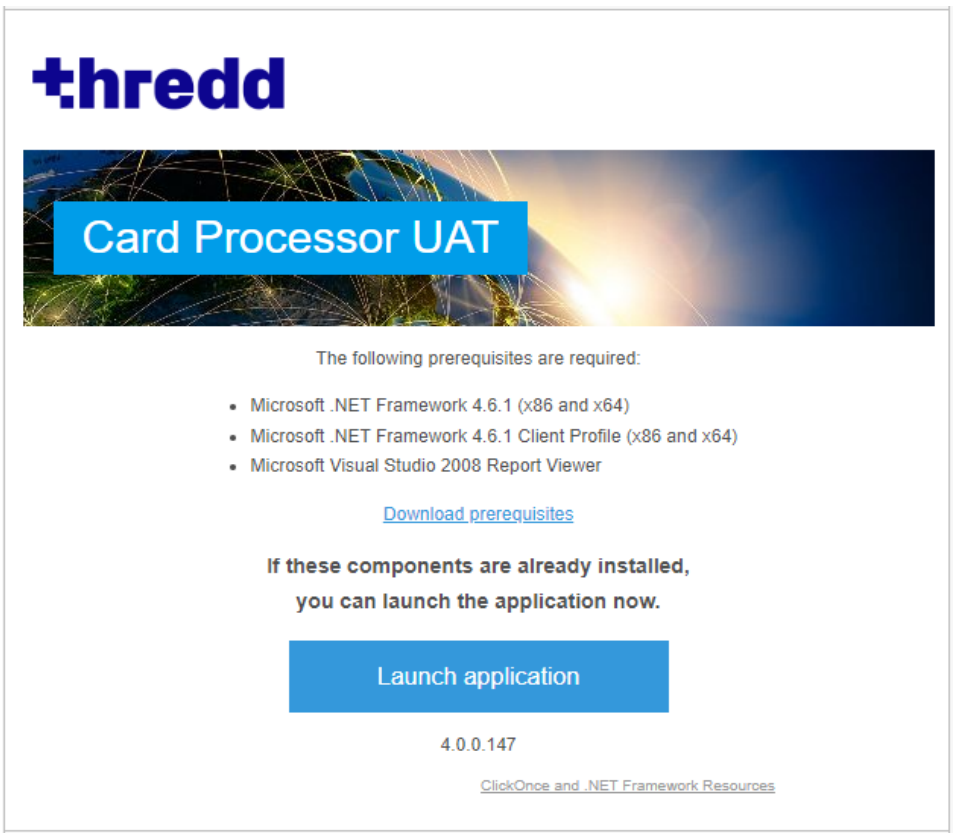


Figure 2: Smart Client application installation screen

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

4 Launching Smart Client

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

4.1 Starting Smart Client

To start Smart Client:

1. Double click the **Card Processor** desktop icon:

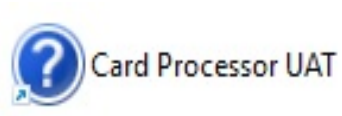


Figure 3: The Card Processor desktop icon

2. The **Restricted Access System** message is displayed. Click **OK** to continue.

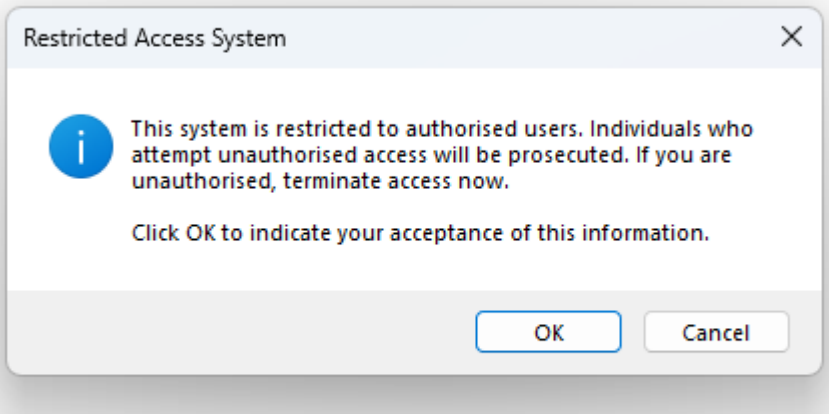


Figure 4: The Restricted Access System message.

3. At the Login screen, enter the username and password you received from Thredd.

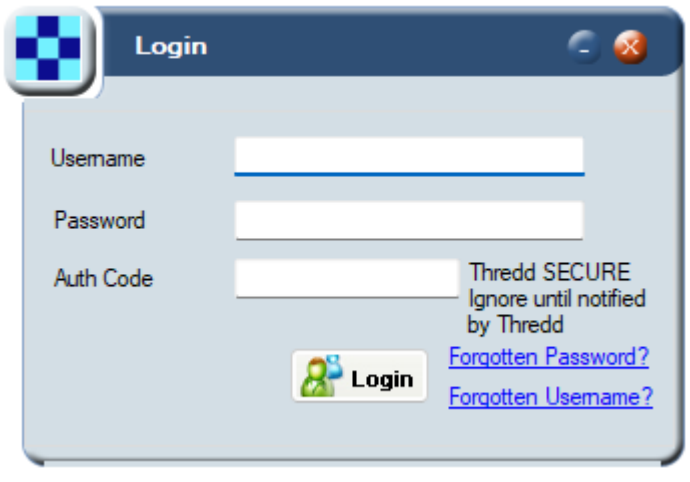


Figure 5: The Login screen

Tip: Leave Auth Code blank.

4. After entering your login credentials, click **Login** or press the Return key to display the Smart Client main screen.

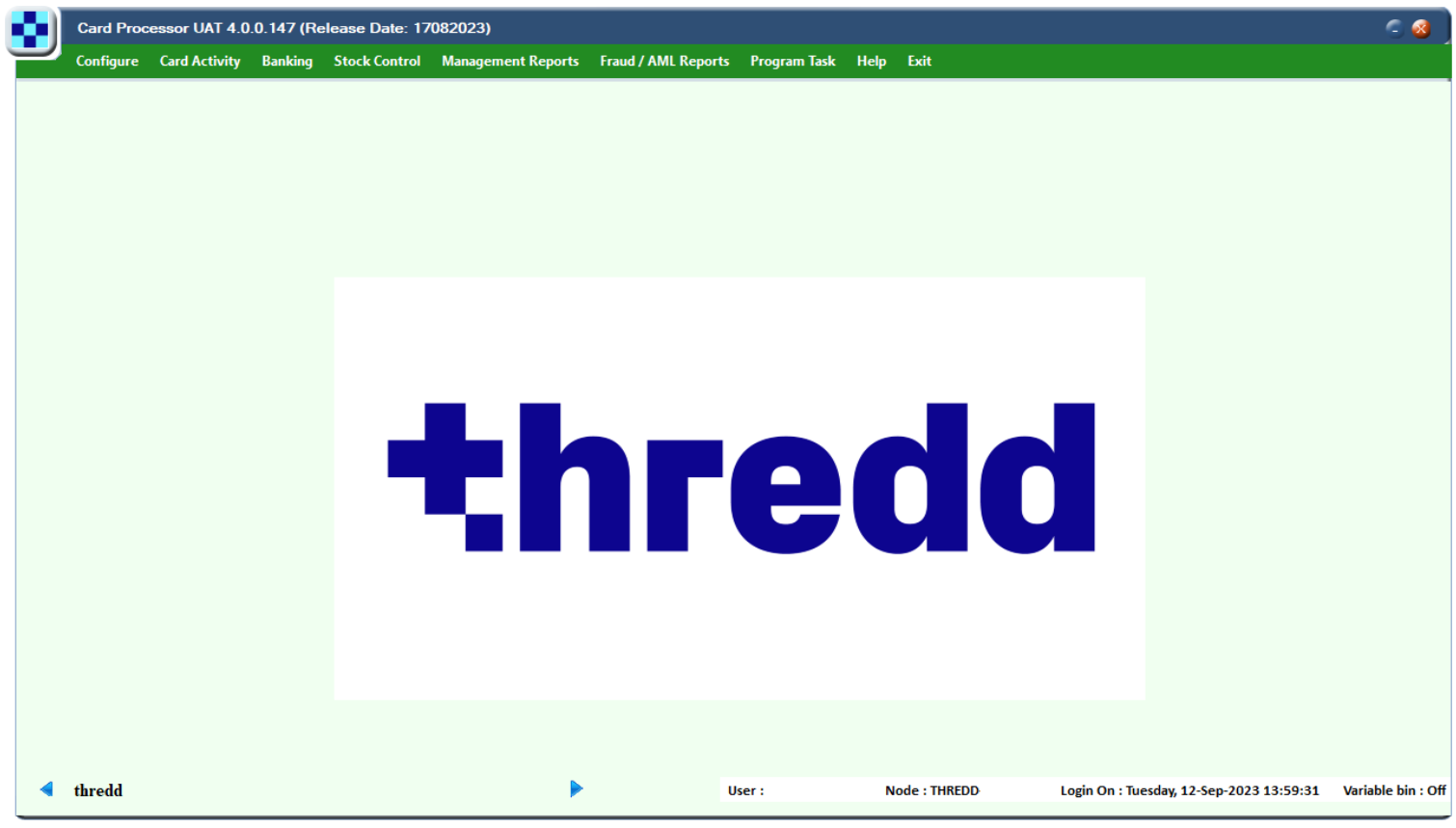


Figure 6: The main Smart Client (Card Processor) screen

4.2 About the Smart Client Display

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

- **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.

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.

4.3 About Roles and Permissions

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

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

Permissions		Customer Support 1	Customer Support 2	Manager
Configure	Change my password	✓	✓	✓
Card Activity	View Cards	✓	✓	✓
View Transactions	View Transaction Details	✓	✓	✓
	Change Card Status	✓	✓	✓
	Activate a Card	✓	✓	✓
	Tracker History	✓	✓	✓
	PIN Services	✓	✓	✓
	View Multi-Fx Cards	✓	✓	✓
	Balance Adjustment		✓	✓
	Balance Transfer		✓	✓
	Card Unload		✓	✓
	Edit Card Details		✓	✓
	Remove Authorisation			✓
	View Chargebacks			✓
	Extend Expiry			✓
	Create Chargeback Not available for all institutions; subject to Issuer Approval			✓

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

4.4 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.

5 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.

5.1 Complete a Basic Card Search

To display details about a specific card or token:

1. Select **Card Activity** > **View Cards** to display the **View Cards** screen.
2. Use the drop-down search options and filters located along the top of this screen to find cards.

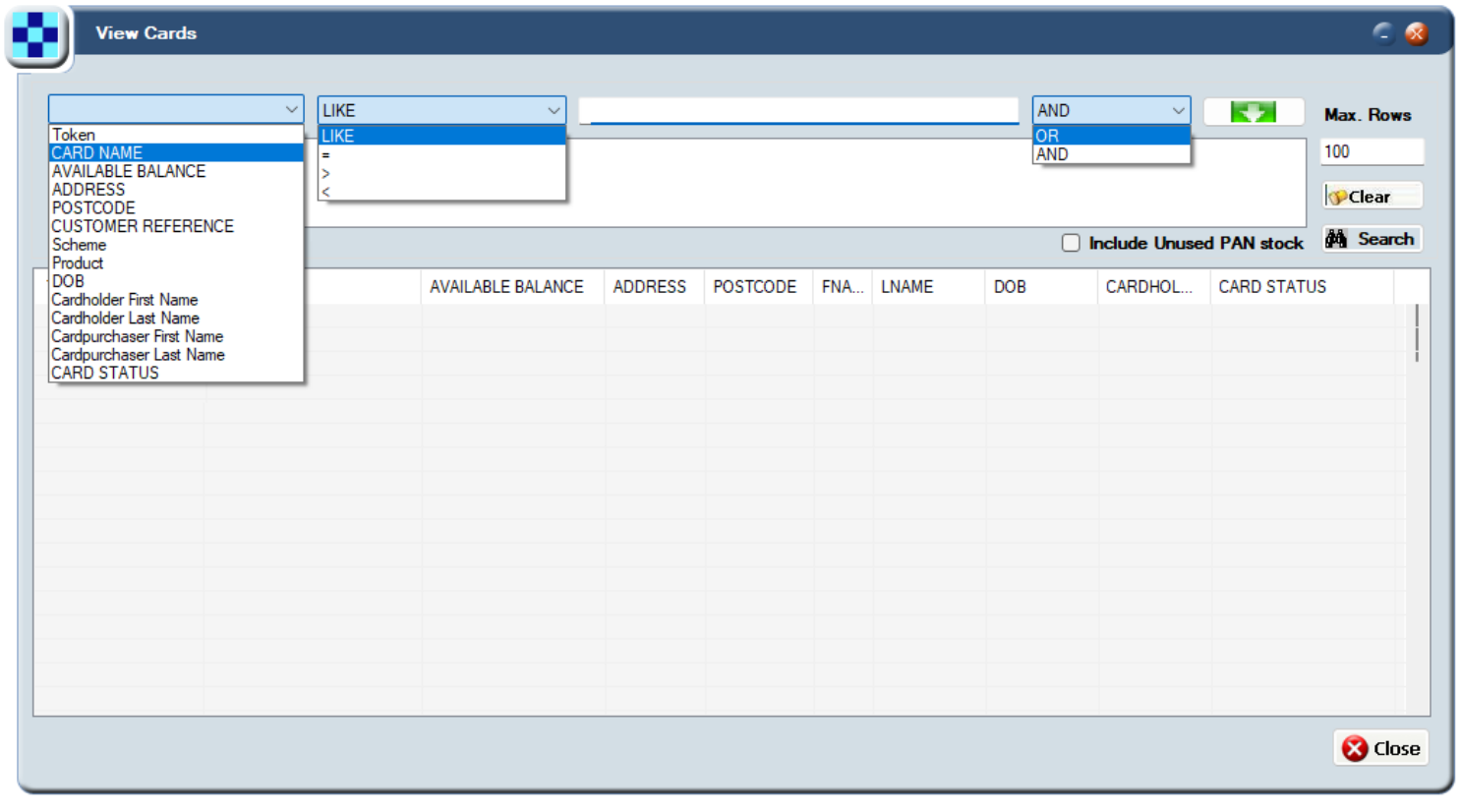


Figure 7: The View Cards screen

5.2 Add multiple parameters to a Card Search

To add multiple parameters to a card search, for example, Cardholder First Name, Cardholder Last Name, and Postcode:

1. Select **Card Activity** > **View Cards** to display the **View Cards** screen.
2. Use the drop-down search options and filters located along the top of this screen to build your search criteria.
3. Click the green down arrow to add each parameter to your search.

4. Click Search to display the results as a list below.

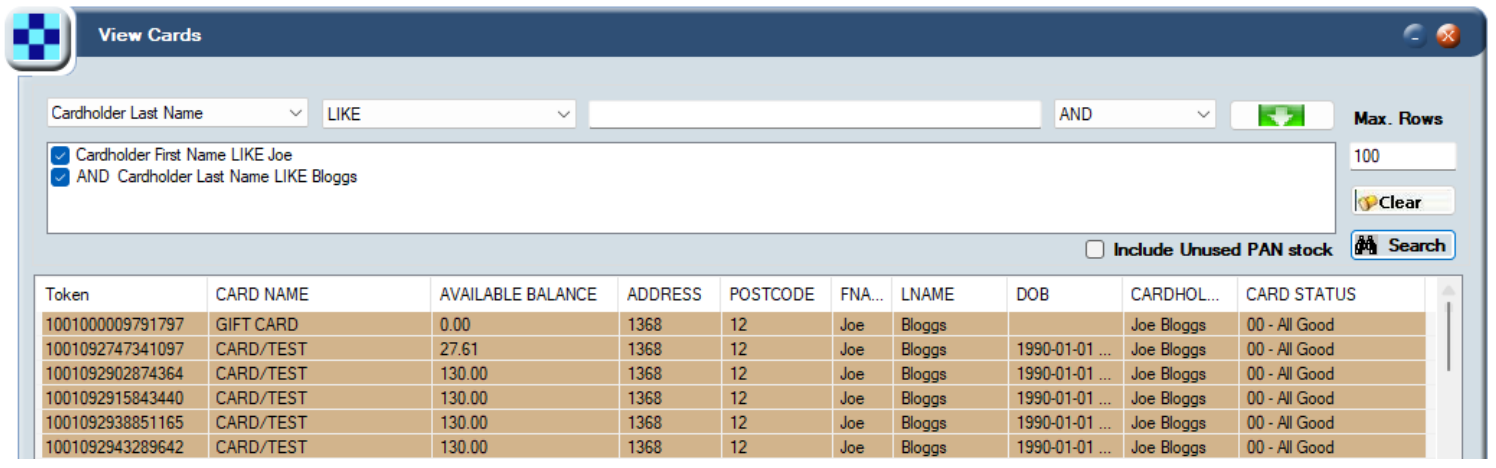


Figure 8: Adding multiple parameters to the search criteria

5. 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. To clear all selected filters, click **Clear**.

5.3 Searching for a specific token number

To search for a specific token number:

1. Select **Card Activity** > **View Cards** to display the **View Cards** screen.

   Click **Token** (this is the default)
2. Click **LIKE** and choose **=** (equals sign) from the drop-down menu.
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.

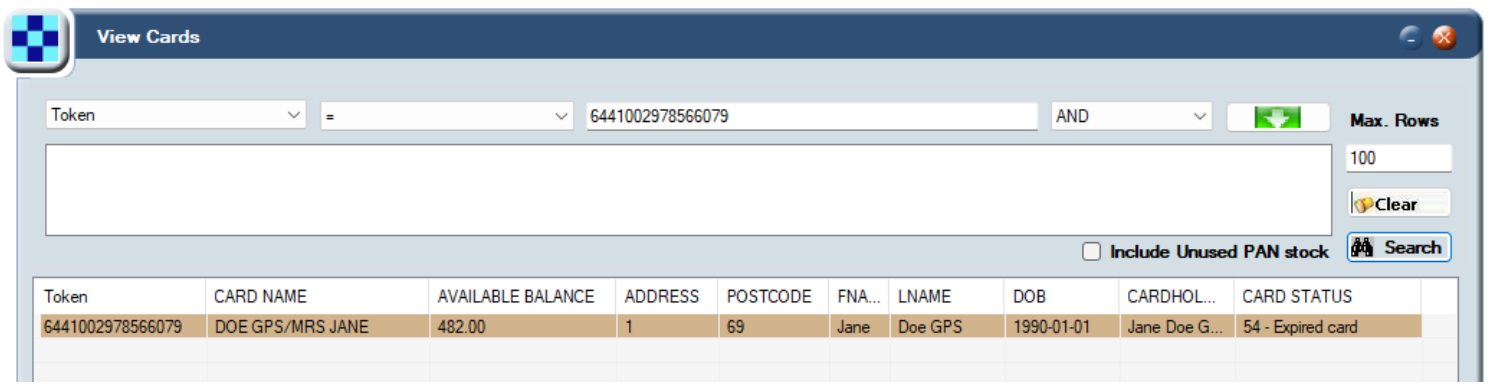


Figure 9: Searching for a token number

5.4 Searching based on a card holder's name, and address

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

1. Select **Card Activity** > **View Cards** to display the **View Cards** screen.
2. Click **Token** and choose **Cardholder First Name** from the drop-down.
3. Click **LIKE** and choose **LIKE** from the drop-down (or to find a specific name, choose **=** (equals sign) from the drop-down.
4. In the search bar, type the name you want to search for – in this example, **Jane.**
5. Click the green arrow to add this to your search:

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

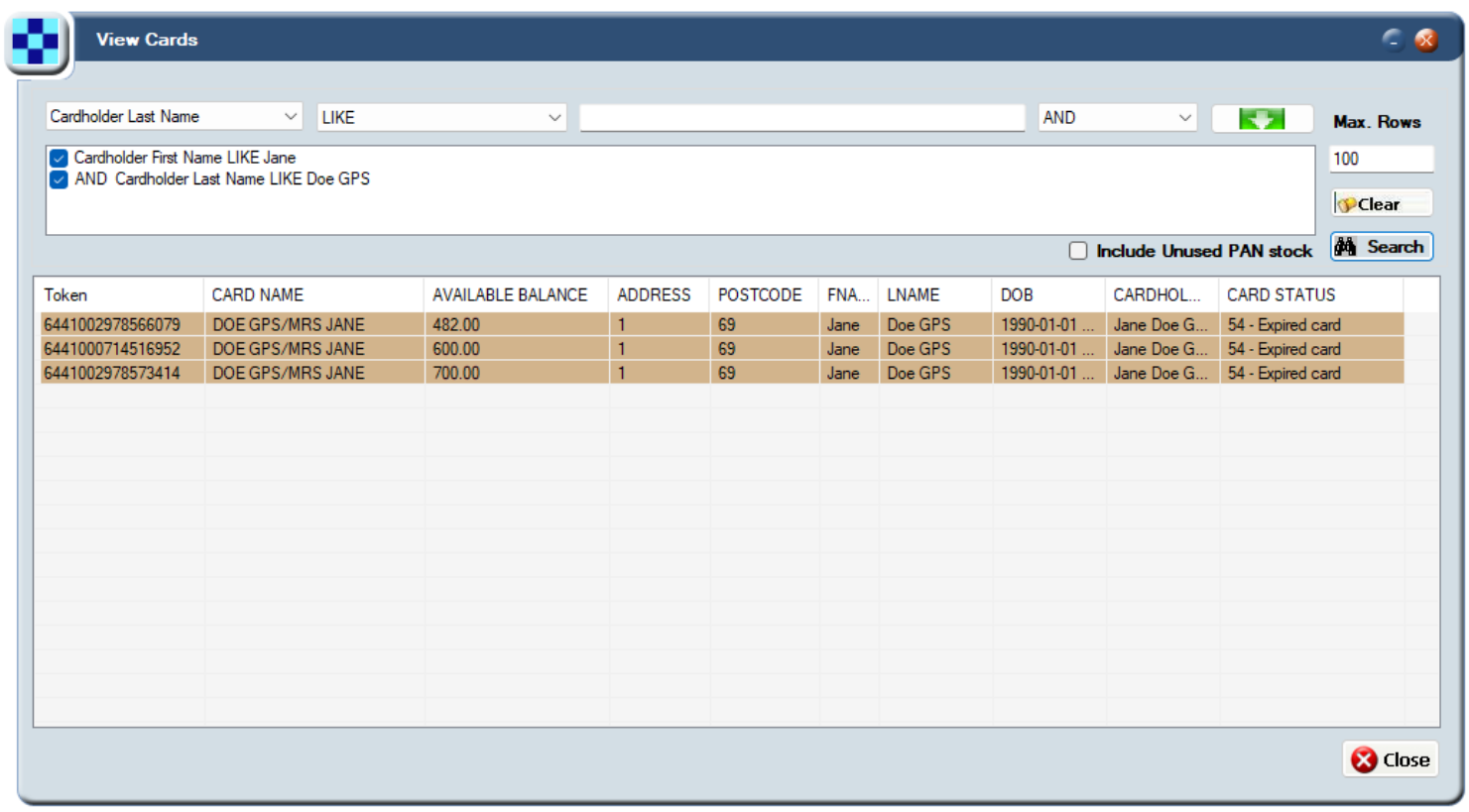


Figure 10: Searching based on a cardholder's name, and address

5.5 Viewing additional Card information

Note: Smart Client excludes status change entries prior to 2022. Card status changes before this year are no longer retrievable. If you want to retrieve card status changes prior to 2022, raise a ticket with Thredd and a member of the App Support team will deal with your request.

To see more information about a card:

1. Select **Card Activity** > **View Cards** to display the **View Cards** screen.
2. Highlight the required card in the list, and right-click to display the following options:

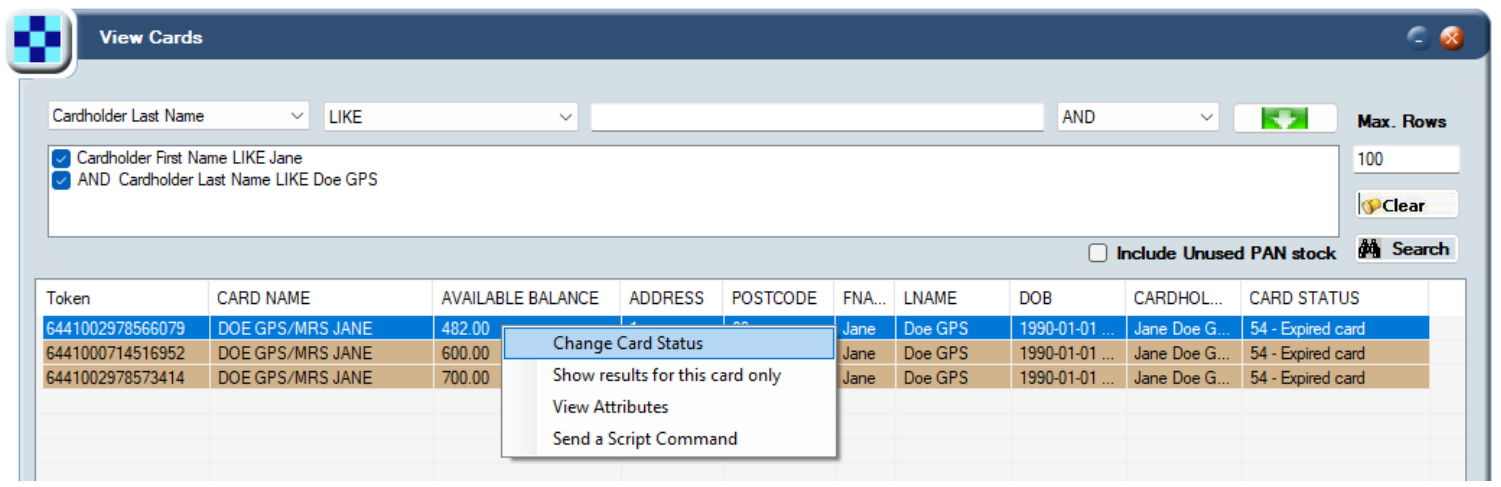


Figure 11: Available options when you select a card in the View Cards screen

3. Choose **Change Card Status** to display the **Status Change** screen and view and / or change the card status.

   Note: For more information, see Managing Cards.

4. Choose **Show results for this card only** to display the View Transactions screen and view all transactions associated with this card,

   Note: For more information, see Viewing Transaction Details.

5. Choose **View Attributes** to display the **Card Master** screen and view more details about the card, such as the card purchaser and holder's details,

   Note: For more information, see Viewing Card Details.

6 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

6.1 Finding Transactions

To search for transactions:

1. Select **Card Activity** > **View Transactions** to display the **View Transactions** screen.
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:

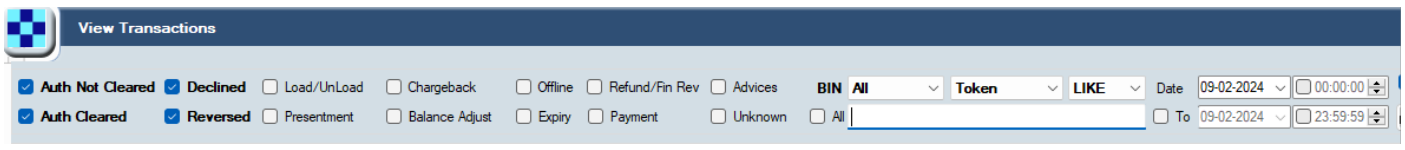


Figure 12: Available Search options on the View Transactions screen

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 take advantage of Smart Client's powerful search functions.

6.2 Searching for transaction types

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

Transaction type	Description
Auth Not Cleared	An authorisation that has not cleared (Thredd has not yet received a presentment that can be matched to the authorisation on the token). If Thredd does not receive a presentment that can be linked to the authorisation, Thredd 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.
Auth Cleared	An authorisation which has cleared (Thredd has received a presentment that could be matched to the authorisation).
Declined	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 Appendix A: Common Decline Reasons.
Reversed	An authorisation that was reversed. To find the reversal reason, right click the reversal and choose **More details** > **View transaction details**. See the **Response Status (DE039)**. 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 Mastercard *Customer Interface Specification* or *Visa Base* manual.
Load/Unload	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).

Transaction type	Description
Presentment	A transaction for authorisations that require settlement. First presentment occurs when the merchant sends a request to take either part, or all the amount previously authorised on the card.
Chargeback	Presentments that have gone through the chargeback process. For more information, see Managing Chargebacks.
Balance Adjust	An adjustment to the balance or the blocked amount. This can be a Credit or a Debit.
Offline	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).
Expiry	Transaction Expiry, response 54 'Expired Card' (Process – Debits Unload).
Refund/ Fin Rev	Presentment returning funds to the Card Holder/ Financial Reversal – Process (Credits for Refund).
Payment	Payment originating from non-card network entity, paying funds into or out of the customer account (for example, Faster Payments and BACS).
Advices	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.
Unknown	Card not found: Unknown Card. In large volumes this can indicate a BIN attack. For information, see FAQs

Note: There are 2 other transaction types that display in the View Transactions screen, but cannot be searched for. These are:

- Financial Request (Declined displays red, settled displays green)
- Financial Reversal Advice (Displays in pink)

6.3 Searching for a BIN

You can search for a single BIN at a time. To search for a specific BIN:

1. Select **Card Activity** > **View Transactions** to display the **View Transactions** screen.
2. From the **View Transactions** screen, use the BIN drop-down box to search for transactions with a specific 6-digit BIN.

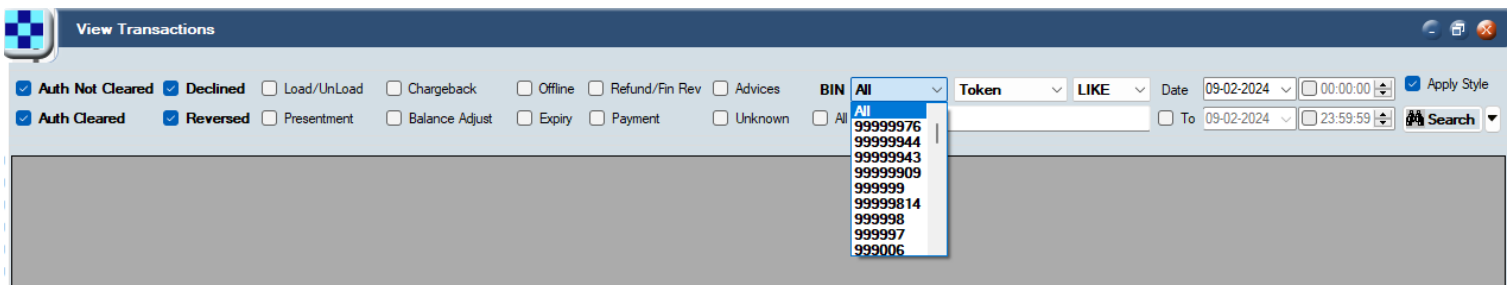


Figure 13: BIN drop-down box

6.4 Searching using other details

To search for transactions using other details:

1. Select **Card Activity** > **View Transactions** to display the **View Transactions** screen.
2. From the **View Transactions** screen, expand the drop-down box labelled **Token** (the default).
3. Select the required search parameter using other card and transaction details.

Note: You can filter your search further using the drop-down 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:

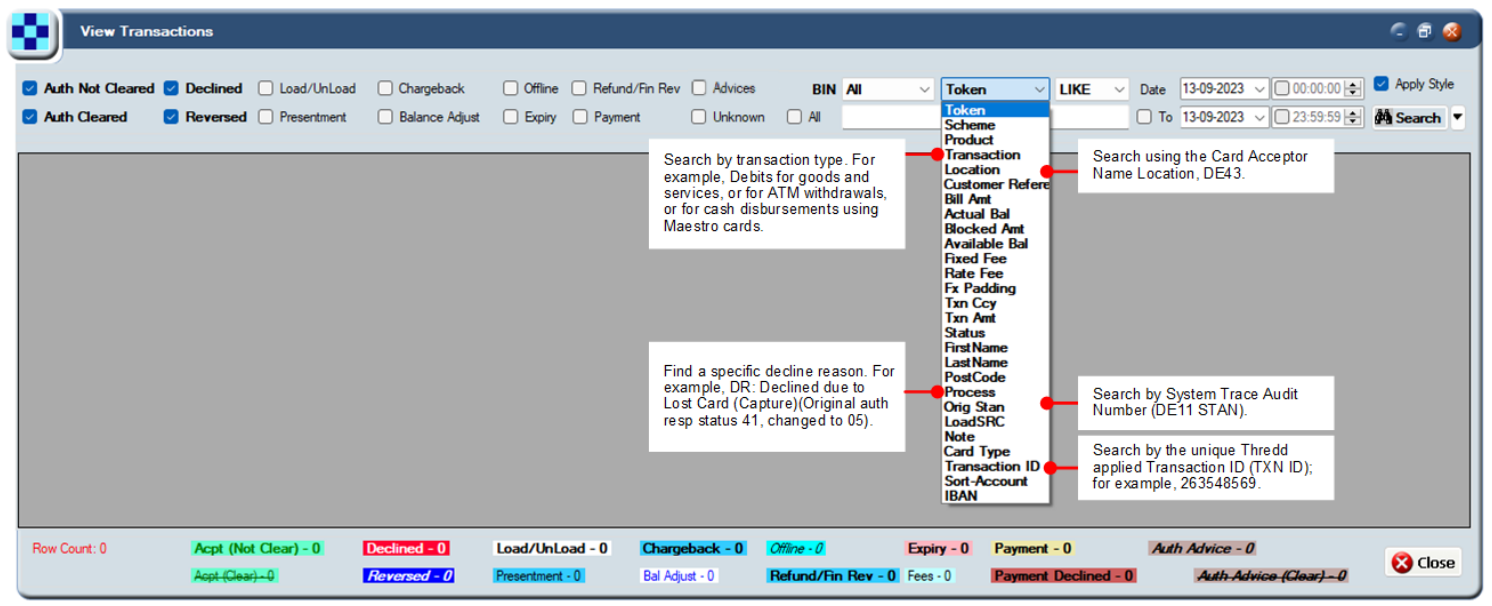


Figure 14: Search options available from the drop-down box beneath Token

6.5 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). The time is in Thredd UK server time, not the country of transaction time.

To search transactions based on the date and time:

1. Select **Card Activity** > **View Transactions** to display the **View Transactions** screen.
2. From the **View Transactions** screen, select the required date range.

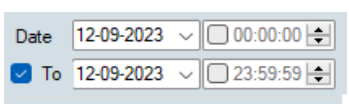


Figure 15: Available Search options for date and time.

3. Click **Search** to display the relevant transactions.

6.6 Show all transactions for a specific day

To see all transactions that occurred on a specific day:

1. Select **Card Activity** > **View Transactions** to display the **View Transactions** screen.
2. Select **All**.
3. 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:

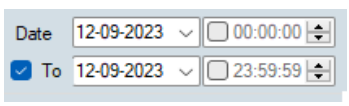


Figure 16: Available Search options for date and time.

6.7 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:

1. Select **Card Activity** > **View Transactions** to display the **View Transactions** screen.
2. From the **View Transactions** screen, click the arrow to the right of **Search**.
3. Choose **Set Ticked as Default**.

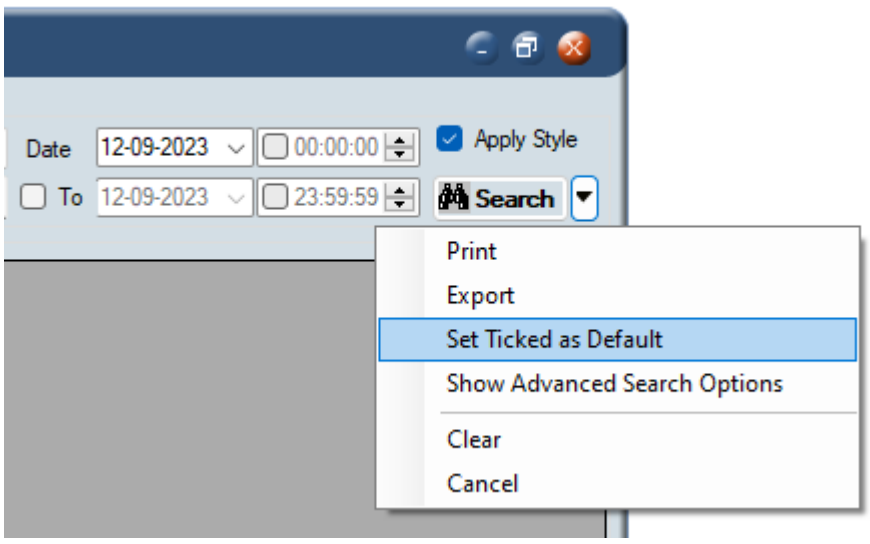


Figure 17: The menu option for setting the ticked items as default.

6.8 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.

7 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:

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

   The **View Transactions** screen appears.

   > **Note:** For information about how to search for transactions, see Searching for a Transaction.

7.1 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.

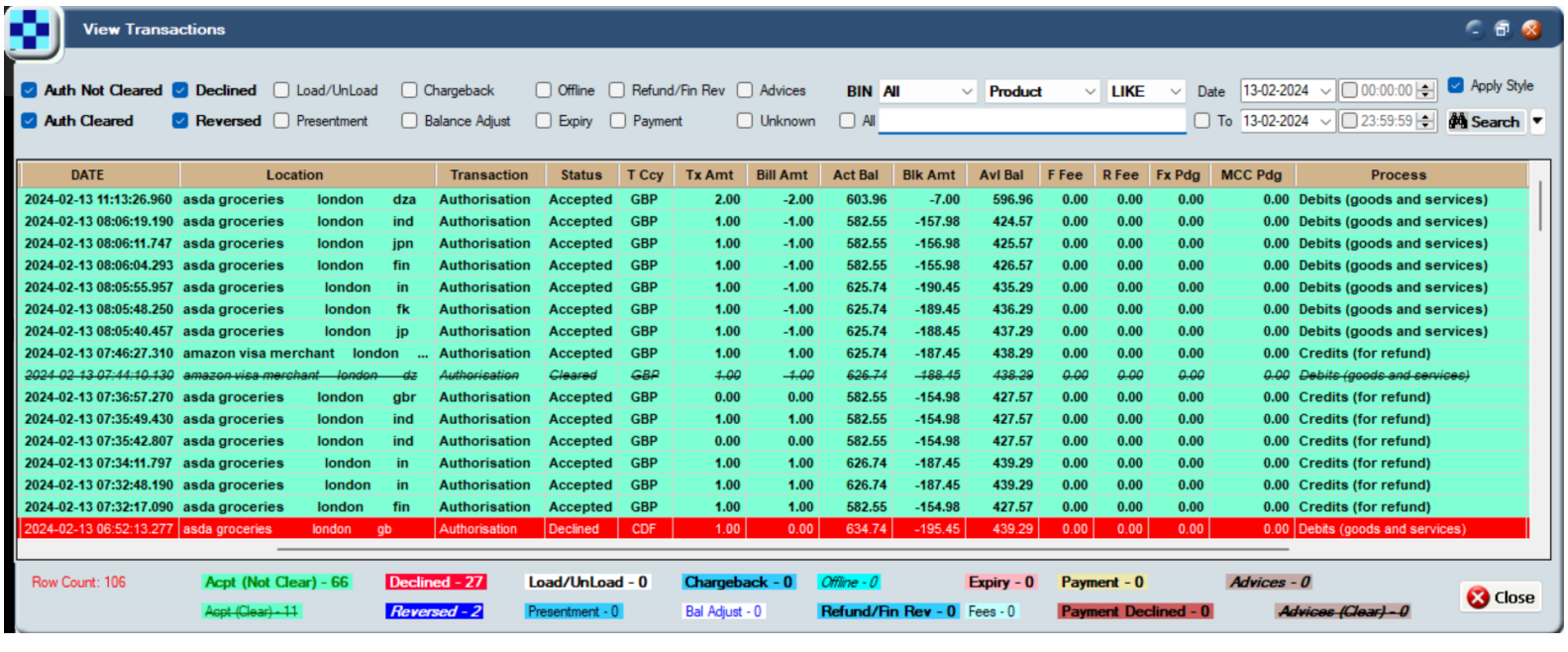


Figure 18: The View Transactions screen

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
Token	Unique Thredd 9-digit token assigned to this card.
Scheme	The scheme name configured by Thredd Implementations during set up.
Product	Specific card network's product.
Date	Date and time the transaction occurred. The time relates to Thredd time, for example, GMT.
Location	Location provided by the merchant.

Column	Description
Transaction	Type of transaction, such as authorisation, balance adjustment, presentment, and auth reversal.
Status	Transaction status, such as Settled.
T Ccy	Transaction currency.
Tx Amt	Transaction amount (in the transaction currency).
Bill Amt	Bill amount (in the currency of the card).
Act Bal	Actual balance after the transaction.
Blk Amt	Blocked amount (pending payments) after the transaction.
Avl Bal	Available balance after the transaction.
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 processing code, for example, recurring fees, balance inquiry.
Orig Stan	6-digit system trace audit number (STAN) used to link the authorisation and the presentment.
Customer ref	An alphanumeric identifier unique to the cardholder which is different to the Thredd token. This is defined in the client's web service calls.
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.

7.2 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:

1. Highlight the transaction in the **View Transactions** screen, then right-click.
2. Select **More Details** from the drop-down menu.

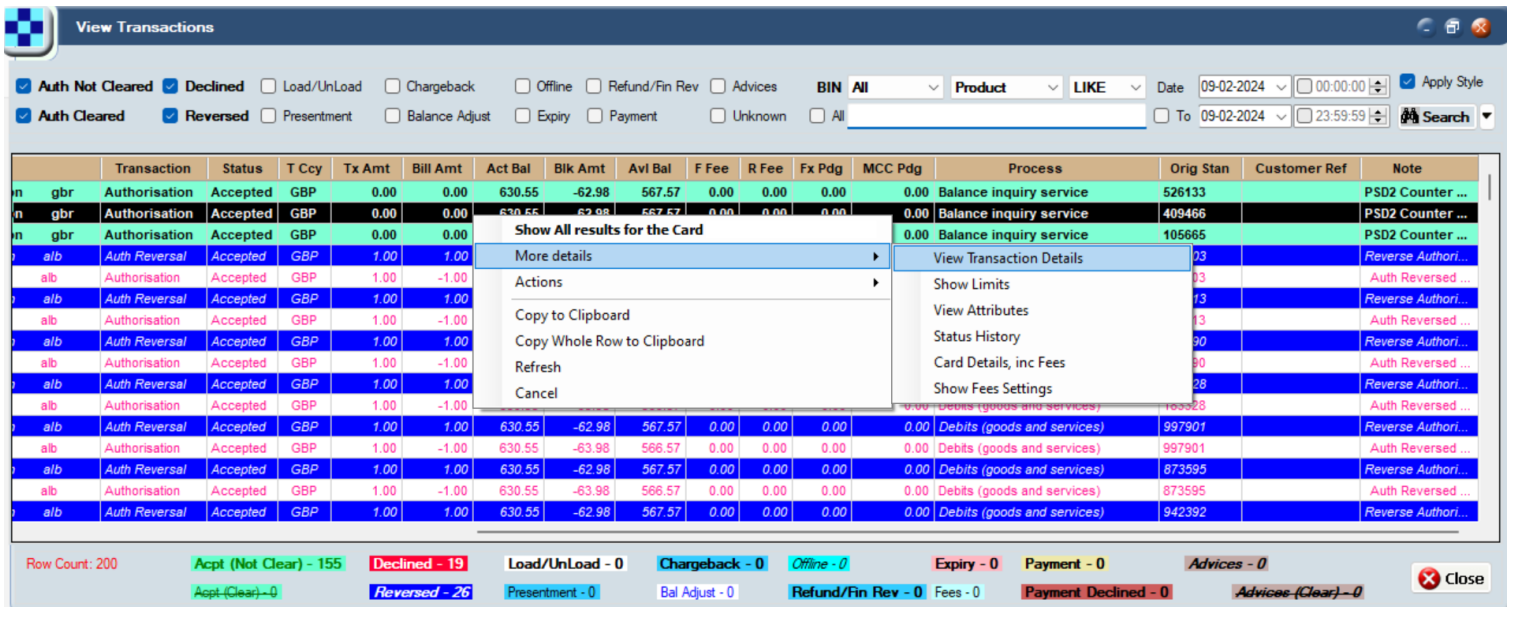


Figure 19: Further options available in the View Transactions screen

> **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.

3. Choose **View Transaction Details** to display the **Transaction Details** screen. 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 advice:

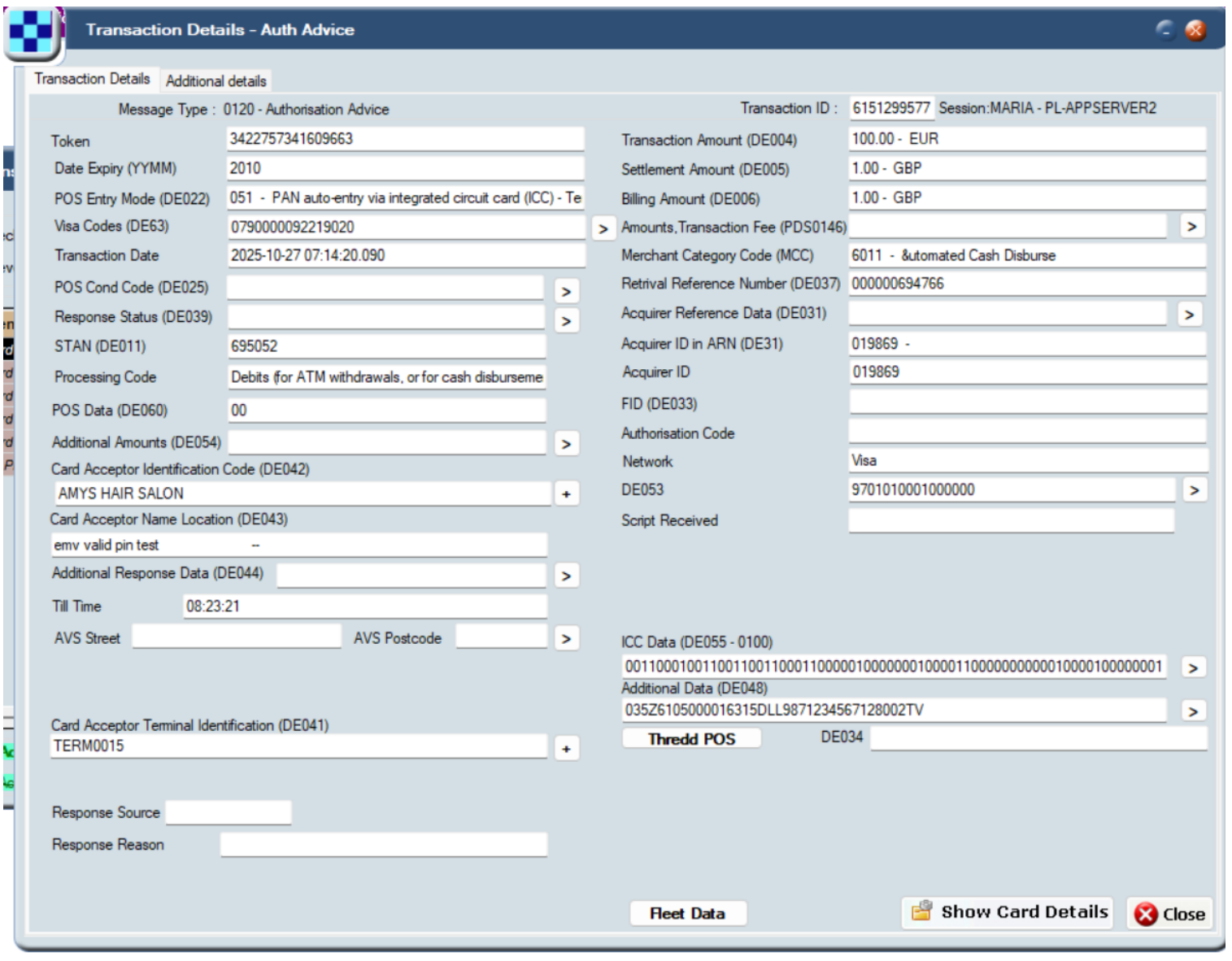


Figure 20: Transaction Details screen

> **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. The available options are explained in more details in the following section.

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, refer to 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).

Note: The available fields depends on the transaction source network and transaction type.

Field	Description
Message Type	The type of transaction, such as an authorisation or presentment.
Token	The unique token number associated with the transaction.
Date Expiry	The expiry date provided at the time of the transaction (useful to check in case the cardholder has entered an incorrect expiry date).
POS entry mode (DE022)	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.
Transaction Date	The date of the transaction. Format YYYY-MM-DD HH:MM:SS:MS.
Advice Reason Code	Mastercard Authorisation Advice Reason Code. Explains why Mastercard Stand-In processing (STIP) occurred or why an advice was created. **Note:** This field will only be present for transactions received by Thredd from Mastercard.
Visa Response Code (DE63)	Visa's Response Data, exactly as provided from Visa to Thredd. **Note:** This field will only be present for transactions received by Thredd from Visa.
Response status (DE039)	The status sent back to the merchant, for example, 05 - do not honour. Click the arrow next to this field to see more information.
STAN (DE011)	System Trace Audit Number. This links the authorisation and presentment (note this number is not unique).
Processing code	Indicates the type of transaction, for example, a debit.
POS data (DE061)	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.
Additional Amounts (DE054)	Contains additional amount information for the transaction, if relevant. For example, for purchase with cashback transactions, the additional amounts field will be present with the cashback amount.
Card Acceptor Identification Code (DE042)	Code relating to the specific Point of Sale (POS) terminal.
Card Acceptor Name Location (DE043)	Merchant's details.
Additional Response Data (DE044)	Visa's Additional Response Data, exactly as provided from Visa to Thredd. This will only be present for transactions received by Thredd from Visa Base1, if DE44 was present. It provides information on Visa's validation checks of data in the message. This will only be set for Visa online authorisation transactions.

Field	Description
Till Time	Time provided by the merchant (can be incorrect but matches what is on the receipt).
Card Acceptor Terminal Identification (DE041)	Uniquely identifies the terminal which accepted the card. Always present if the card data was read by a terminal.
Response Source	Indicates which system sent the 0110 or 0210 response to the terminal. Normally present only for some Authorisation advices and Authorisation reversals.
Response Reason	Indicates the reason why the Response Source sent a response to the terminal. Normally present only for some Authorisation advices and Authorisation reversals.
Transaction ID	Identifier for tracing a specific transaction and narrowing a search. This a unique identifier generated by Thredd to help identify and search for transaction in the Thredd platform.
Transaction Amount (DE004)	Transaction amount and currency.
Settlement Amount (DE005)	Settlement amount and currency.
Billing Amount (DE006)	Amount applied to the account in the currency of the card.
Amounts, Transaction Fee (PDS0146)	The fee charged (for example, by the acquirer) for transaction activity in the transaction currency code. This field is only applicable to presentments.
Merchant Category Code (MCC)	Code that describes a merchant's primary business activities.
Retrieval Reference Number (DE037)	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.
Acquirer Reference Data (DE031)	Acquirer Reference Number/Data. ISO 8583 field 31. The acquirer reference number exists for clearing messages only (Financial advices/notifications, and Chargeback advices/notifications (and reversals of)).
Acquirer ID in ARN (DE31)	Acquirer ID found in the Acquirer Reference Number (ARN).
Acquirer ID	Acquiring Bank ID as assigned by the network. Note that the format differs depending on whether this is an Authorisation or a Financial type message. For Authorisation messages: • 2 digits length of Acquirer ID (01 to 09) • Acquirer ID For Financial messages: • 6 digit Acquirer ID (possibly with leading zeros)
FID (DE033)	Identifies the acquiring institution forwarding a Request or Advice message.
Authorisation Code	Authorisation code generated by Thredd for approved and declined authorisation requests.
Network	The network that processed the transaction.
DE053	The Security-Related Control Information provides specific information about PIN block encoding and PIN data

Field	Description
	encryption in processing PINs entered at the point of interaction.
Request Time	The time when Thredd receives this authorisation, in the local time zone of the Thredd servers.
Response Time	The time when Thredd sends the response (the difference between the request and response times is shown below in milliseconds), in the local time zone of the Thredd servers. Note that the response time in milliseconds is the time for the *entire* transaction to complete across all parties.
ICC Data (DE055 - 0100)	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.
Difference (in milliseconds)	The difference, in milliseconds, between the request time and the response time of the transaction.
Additional data (DE048)	Information about 3D Secure (payer authentication) for online transactions. Click the arrow next to this field to see more information. For more information, see Viewing 3D Secure details.
DE034	The Primary Account Number (PAN), Extended, identifies a customer account or relationship. This is only used when the PAN begins with a 59 BIN.
Fees Detail Note	Shows any fees applied to this transaction.
Function Code	The Function Code data element is the code indicating the specific purpose of the message within the message class. **Note:** Only visible for Discover Global Network authorisations. This setting is not displayed in the above screenshot.
Surcharge Fee	This field contains the data to support transaction-level information when a Service Establishment assesses a surcharge on a Card Sale. **Note:** Only visible for Discover Global Network authorisations. This setting is not displayed in the above screenshot.
Additional Authorization Data DGN	This data element contains multiple tags with unique functions. Please refer to the table for details. **Note:** Only applies to Discover Global Network. This setting is not displayed in the above screenshot.
Transaction Destination IIC	The Transaction Destination Institution Identification Code (IIC) data element is the code identifying the institution that is the transaction destination. **Note:** Only applies to Discover Global Network. This setting is not displayed in the above screenshot.
Transaction Originator IIC	The Transaction Originator Institution Identification Code (IIC) data element is the code identifying the institution that is the transaction originator. **Note:** Only applies to Discover Global Network. This setting is not displayed in the above screenshot.

7.2.1 Viewing all transactions for the card

To display a list of all the transactions for the specified token:

1. Highlight the transaction in the **View Transactions** screen, then right-click and choose **Show All results for the Card**.

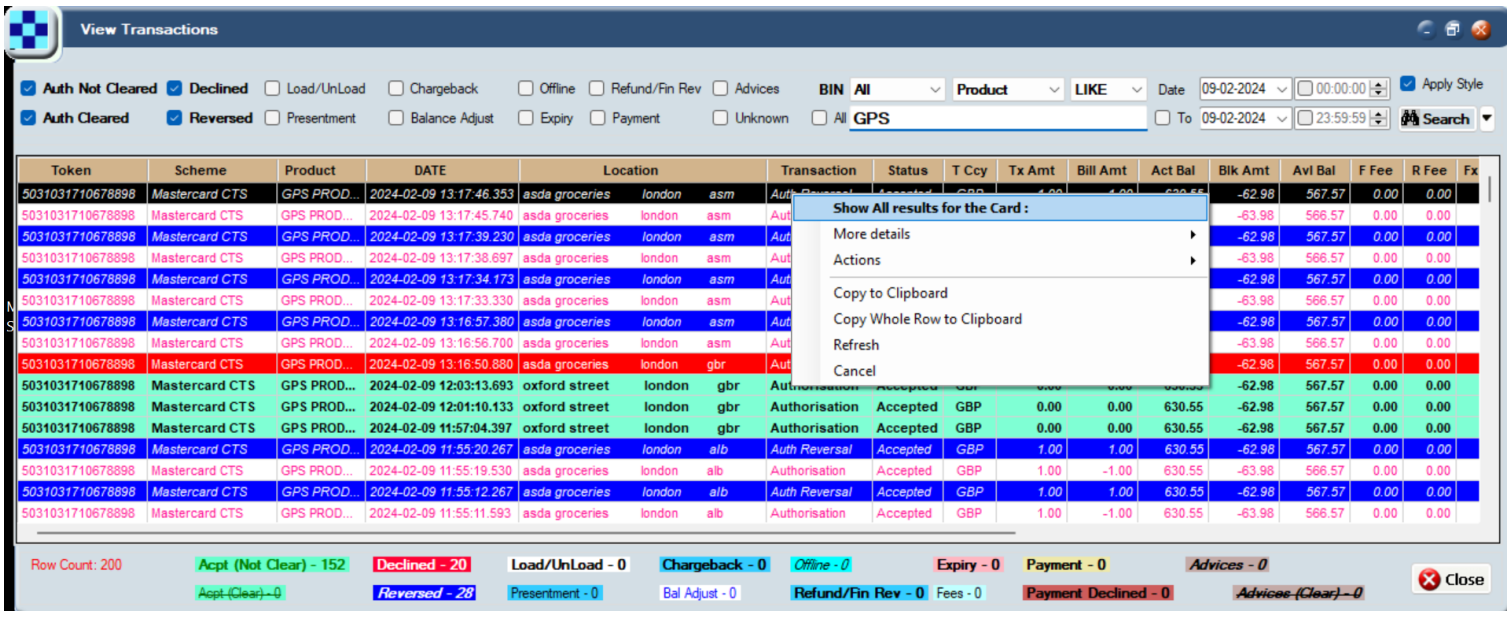


Figure 21: Show All results for the Card menu option

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

2. Review all the activity for the specified card in the **View Transaction** screen.

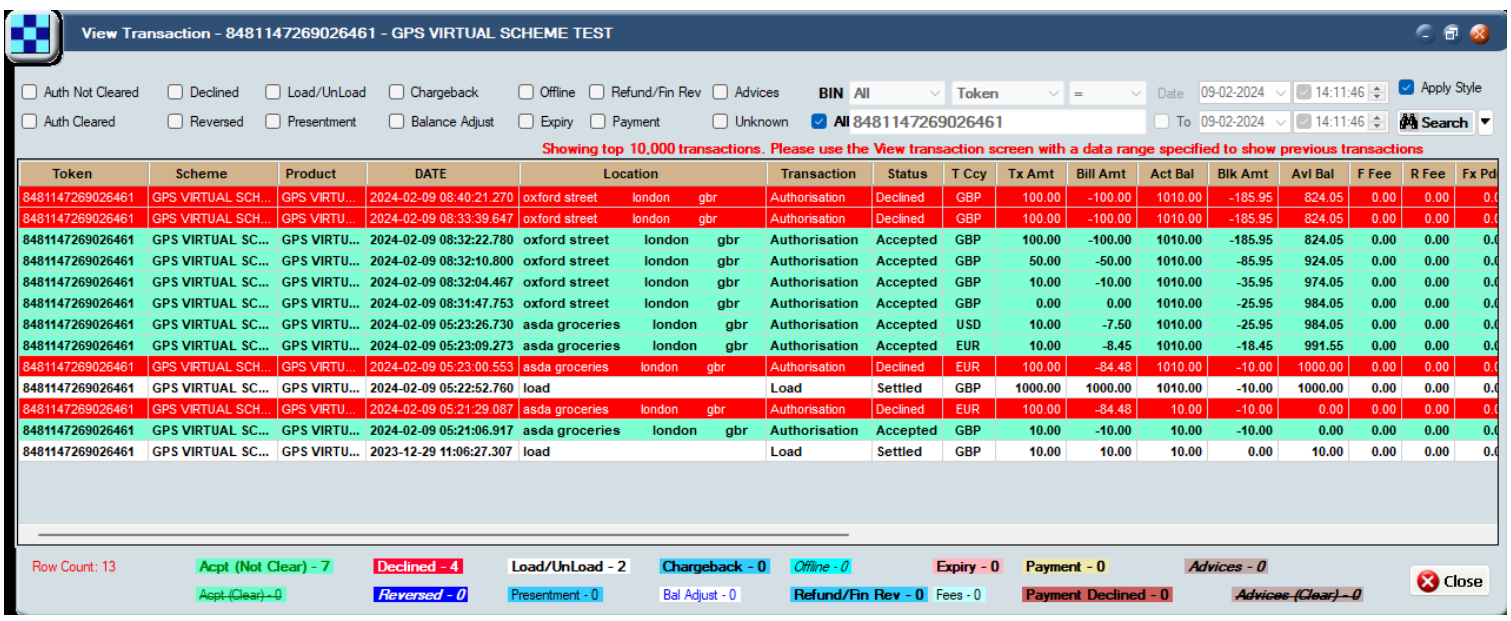


Figure 22: View all activity for the selected card

7.2.2 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 **More Details** > **View Transaction Details**.
2. In the **Transaction Details** screen, inspect the **Additional Data (DE048)** field (bottom right).

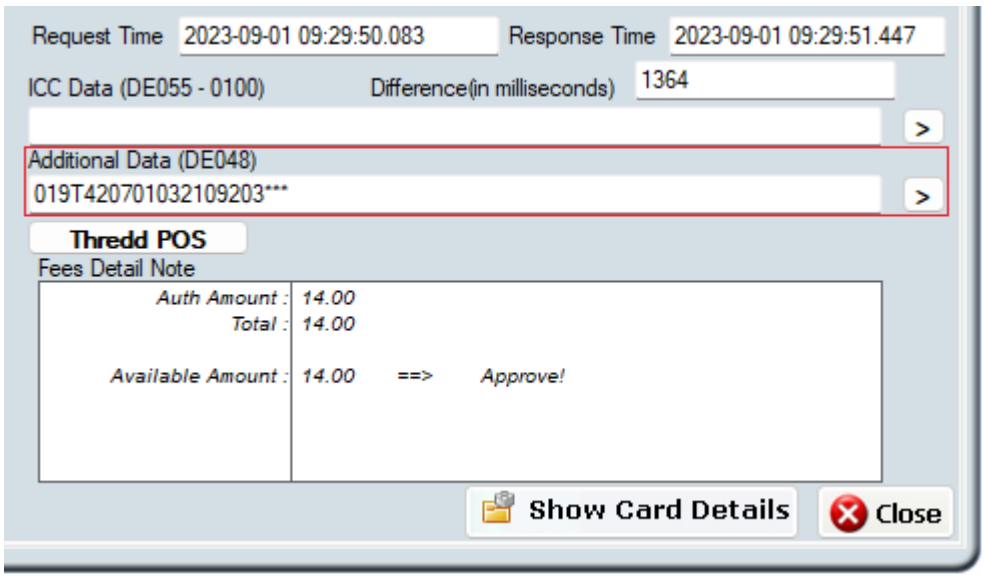


Figure 23: Additional Data (DE048) field on the Transaction Details screen

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

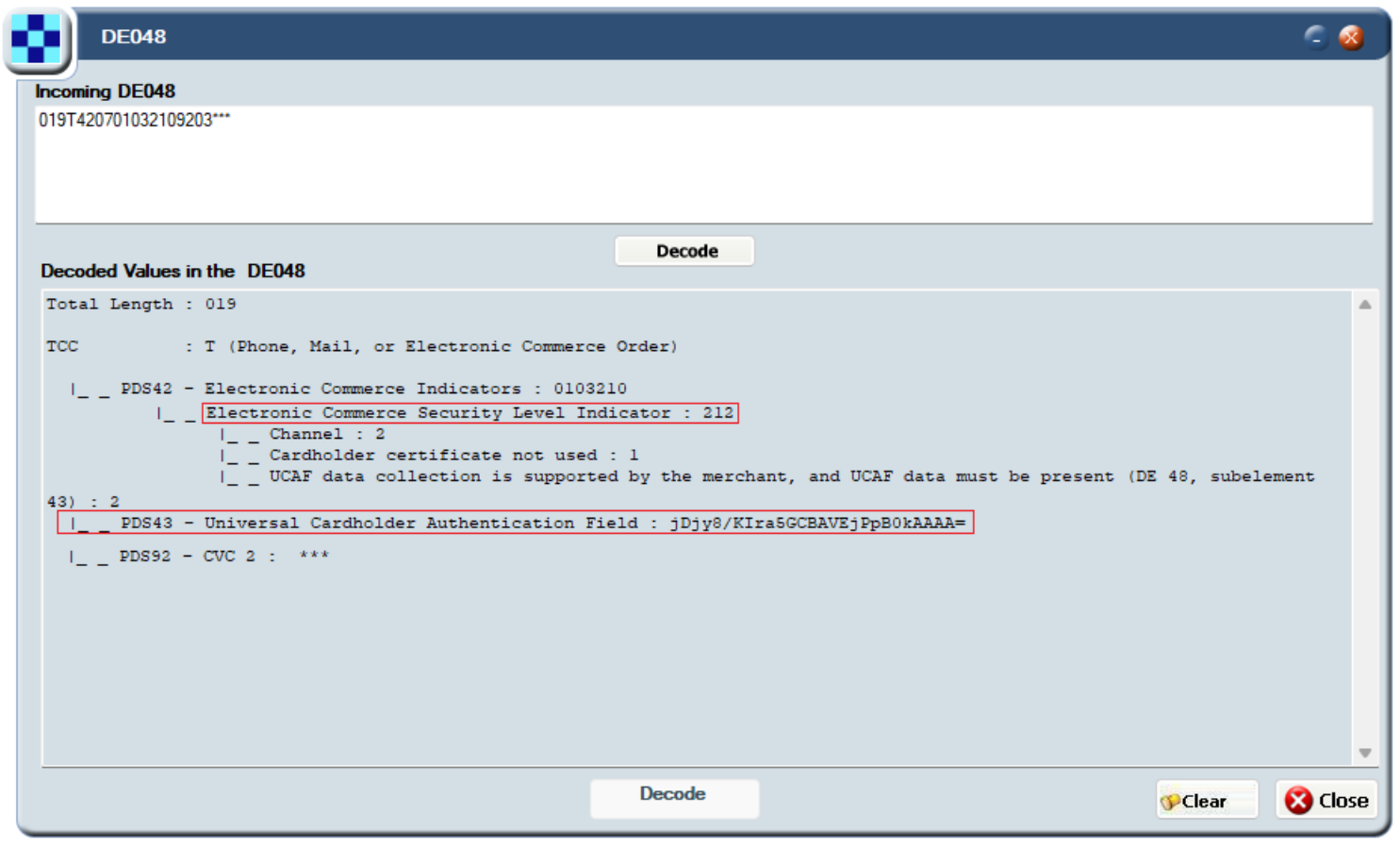


Figure 24: Decoded values in the DE048 field on the Transaction Details screen

Note:
- **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: External Host Interface (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 **More Details** > **View Transaction Details**.
2. In the **Transaction Details** screen, inspect the **Additional Response Data (DE044)** field (left side of the screen).

Figure 25: Additional Response Data (DE044) field on the Transaction Details screen

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

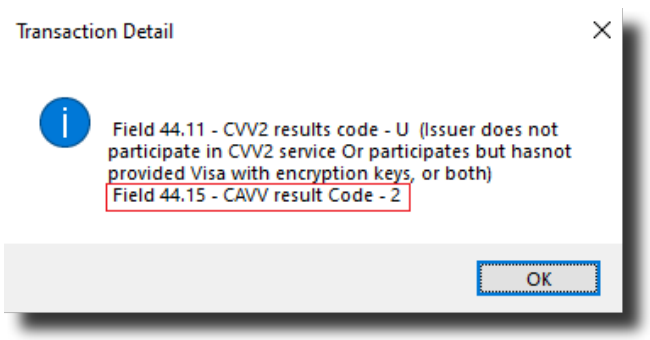


Figure 26: Transaction Detail message displayed when the Additional Response Data (DE044) field is expanded.

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

Tip: EHI data also provides 3D Secure Authentication results containing AAV data, for example: `<cavv>AAABBBQ5KVcglogDBDkpEFQKZyo==</cavv>`. For more information, see the External Host Interface (EHI) Guide.

8 Viewing Card Details

This topic explains how to view more information about cards and how to drill down into the details.

8.1 Display the Card Master

You can access card details either through the **View Cards** screen or the **Transaction Details** screen.

1. Display the Card Master using:
    a. Either **Card Activity** > **View Cards** > **View Attributes**
    b. Or **Card Activity** > **View Transactions** > **More details** > **View Transaction Details** >**Show Card Details** > **Show Card Attributes**

8.2 View Card Details using the Card Information

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** to display the **Card Master** screen.

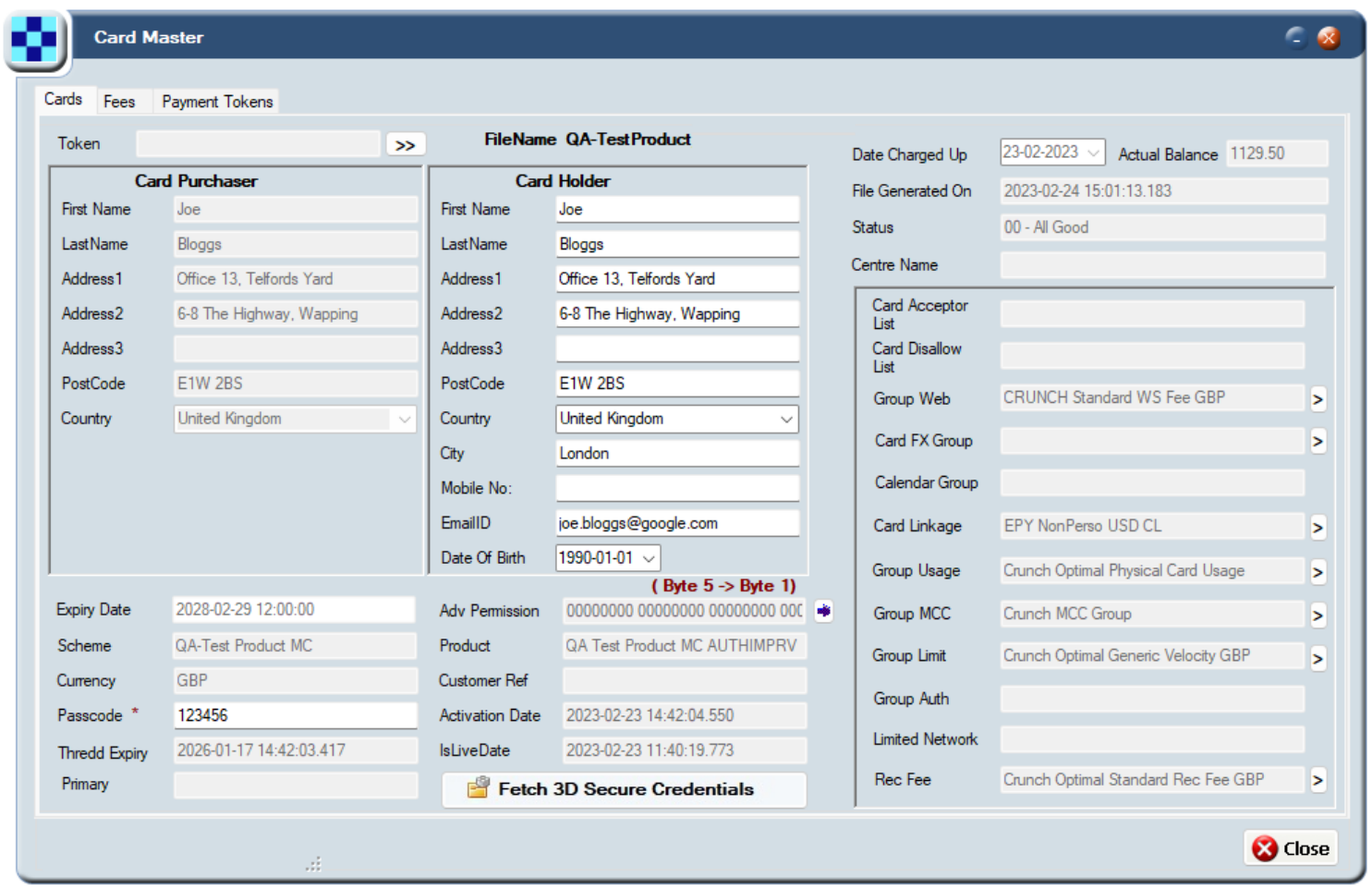


Figure 27: The Card Master screen

8.3 View the Card Details from a Transaction

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.

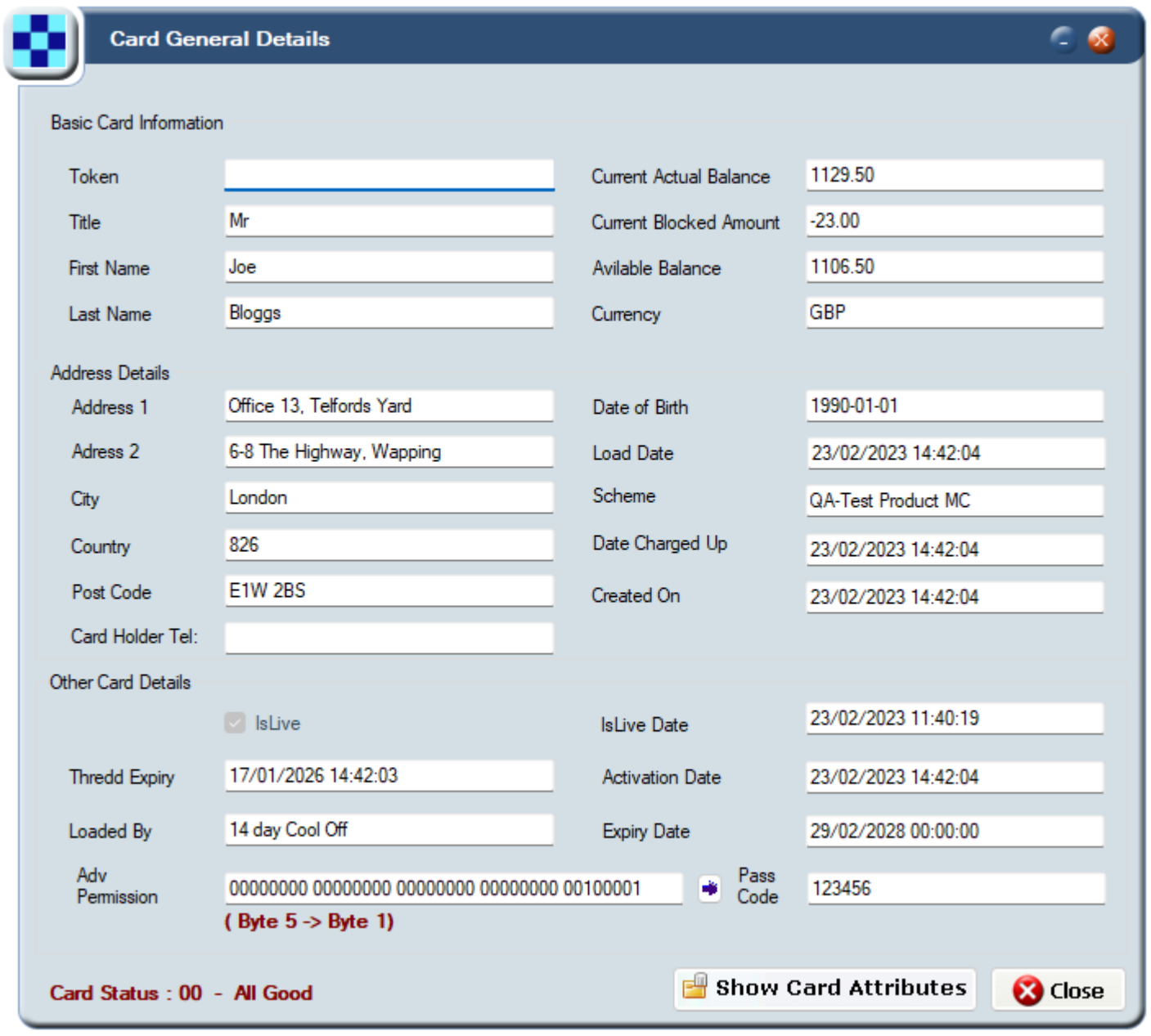


Figure 28: The Card General Details screen

4. Click the **Show Card Attributes** button (bottom of screen) to display the **Card Master** screen with details about the cardholder and card purchaser for the selected token.

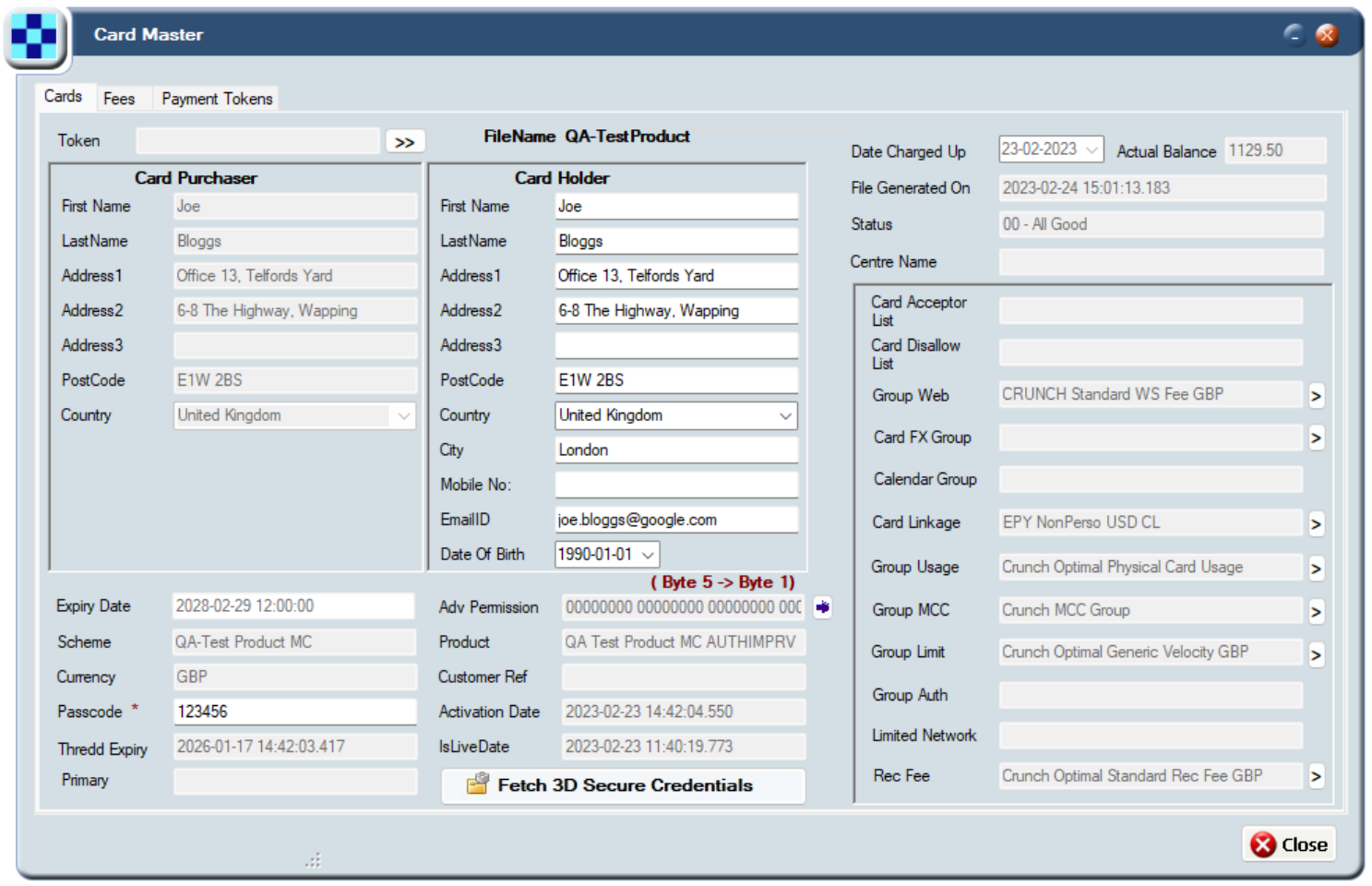


Figure 29: The Card Master screen

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

5. Click **Close** when you have finished reviewing the Card Details on the Card Master screen.

8.4 About the Card Details

The following table explains the main card information and useful fields in the **Card Master** screen:

Field	Description
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 Thredd API, then this information appears here. For details, see: • Cards API Website (REST). (**Note**: The `fulfilment` object fields are used to specify card purchaser details – where a separate delivery address is specified for the card manufacturer to deliver the card. If no details are supplied in the fulfilment object, then Card Purchaser is populated from the Cardholder address fields.) • Web Services Guide (SOAP). (**Note**: The `Delv_` fields are used to specify card purchaser delivery details – where a separate delivery address is specified for the card manufacturer to deliver the card. If no details are supplied in the delivery address fields, then Card Purchaser is populated from the Cardholder address fields .)
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 Thredd API. For details, see: • Cards API Website (REST) • Web Services Guide (SOAP).
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.
Activation Date	Date the card was activated (if blank, the card is not activated yet)
Thredd Expiry	Card expiry date held on the Thredd platform

Note: 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.

Viewing 3D Secure Enrolment Details

To view the 3D Secure Enrolment Details:

1. Display the Card Master.
2. In the **Card Master** screen, click the **Fetch 3DS Credentials** button (bottom middle of screen) to display the 3the **3DS Credentials** screen. This screen contains a list of the 3D Secure authentication methods that the card is enrolled in (e.g., OTP SMS, KBA or biometric).

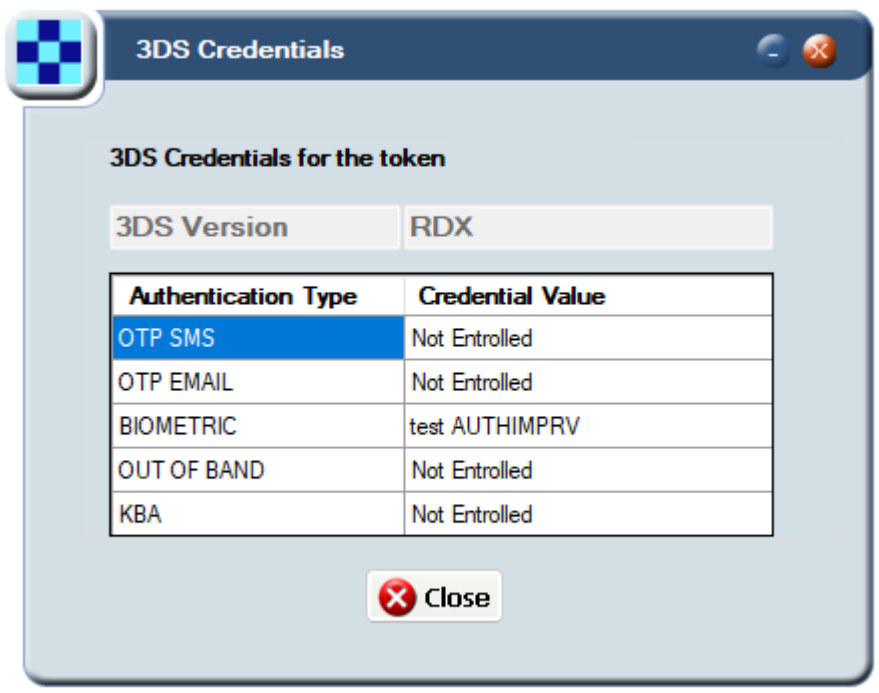


Figure 30: The 3D Credentials screen

Note: For more information on 3D Secure, see the 3D Secure Guide.

8.5 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. 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**.

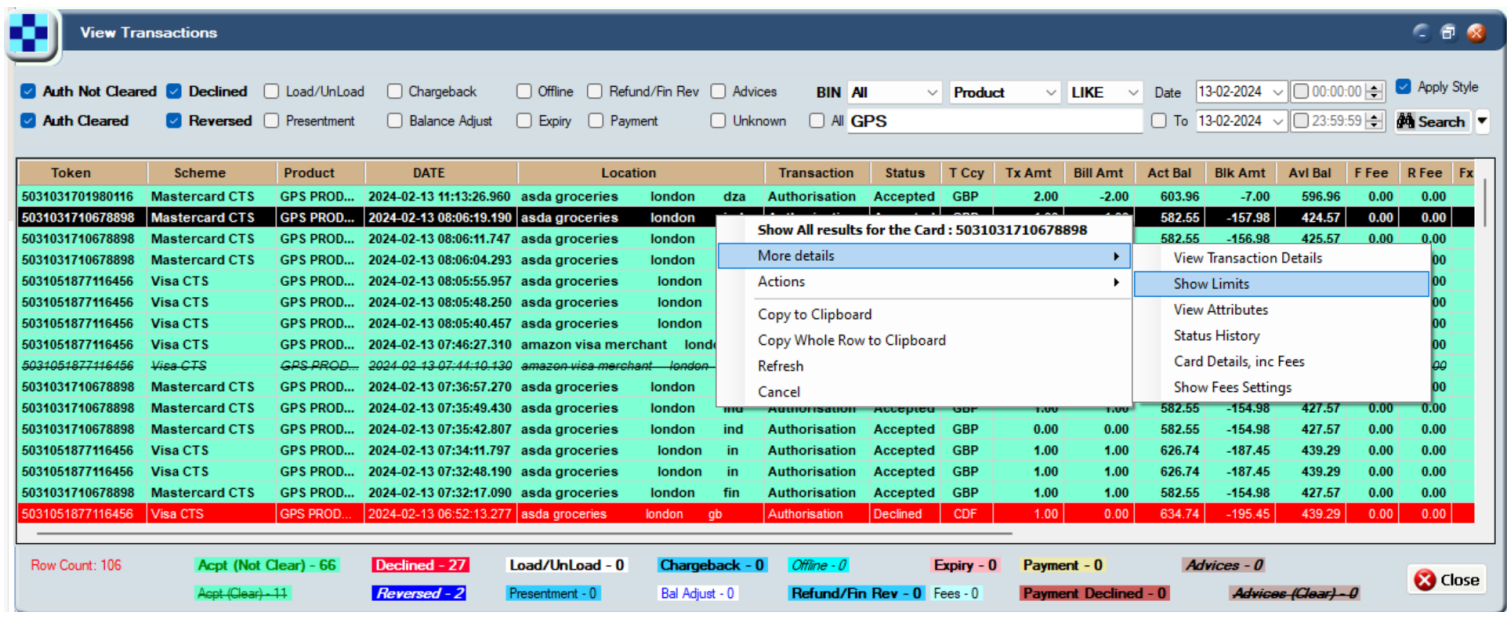


Figure 31: The Show Limits menu option

2. Choose **Show Limits** to display the **Limit Graph**.

   The following example shows the data by day, every 31 days, and 365 days. The cumulative time periods are configurable.

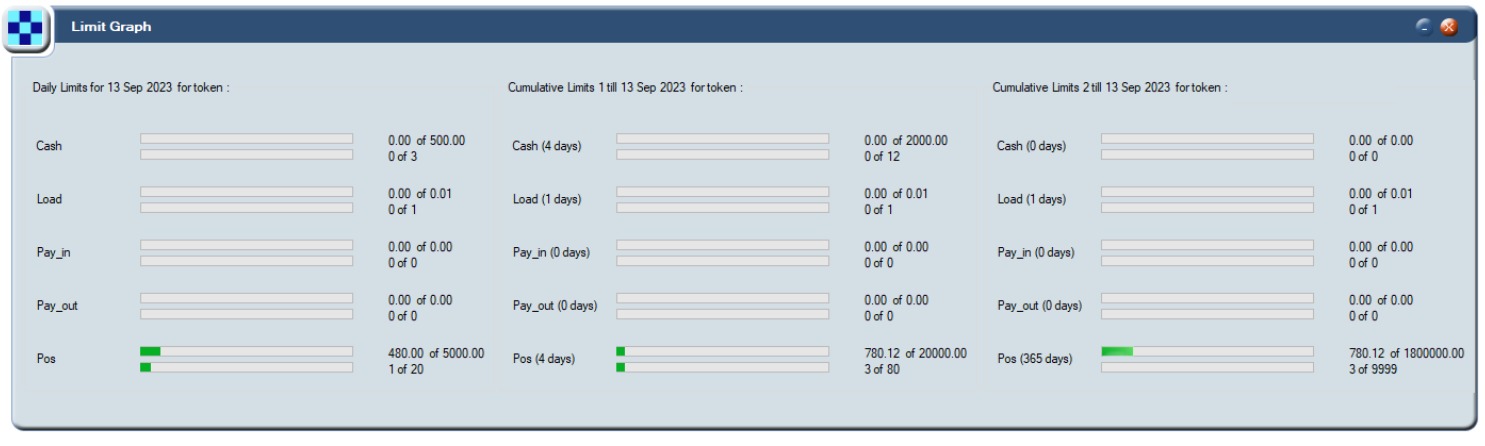
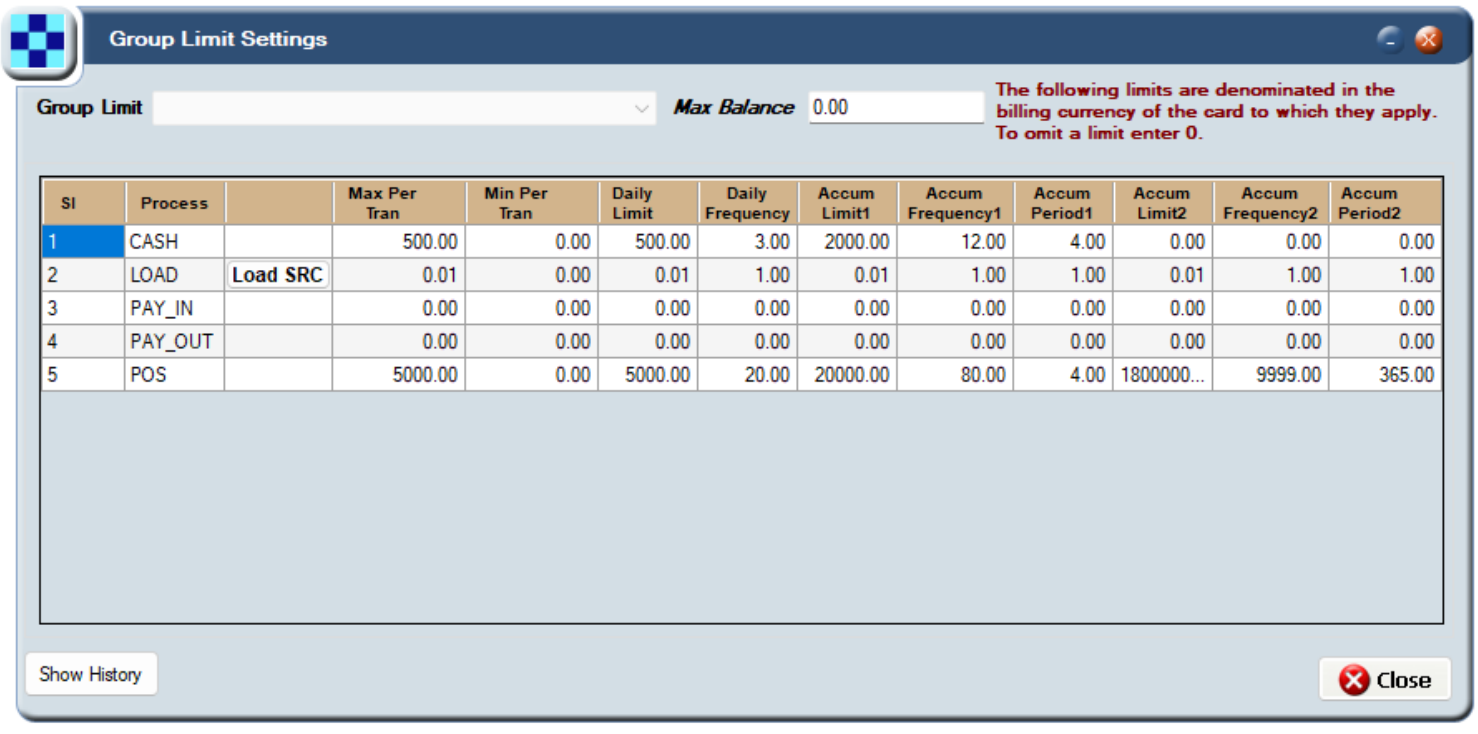


Figure 32: The Card Limits Graph

8.6 Viewing the Card Limits

The card limits are based on the **Group Limit** settings in the **Card Master** screen. See Display the Card Master for instructions on how to navigate to the Card Master screen.

From the Card Master screen, click the arrow next to **Group Limit** in the **Card Master** screen to see the limits configured. For example:



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		500.00	0.00	500.00	3.00	2000.00	12.00	4.00	0.00	0.00	0.00
2	LOAD	Load SRC	0.01	0.00	0.01	1.00	0.01	1.00	1.00	0.01	1.00	1.00
3	PAY_IN		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
4	PAY_OUT		0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
5	POS		5000.00	0.00	5000.00	20.00	20000.00	80.00	4.00	1800000...	9999.00	365.00

Figure 33: The Group Limit Settings screen showing an example of typical limits

8.7 Viewing Card Status History

Using the **Card Status History** screen, you can see a history of the activities completed 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.

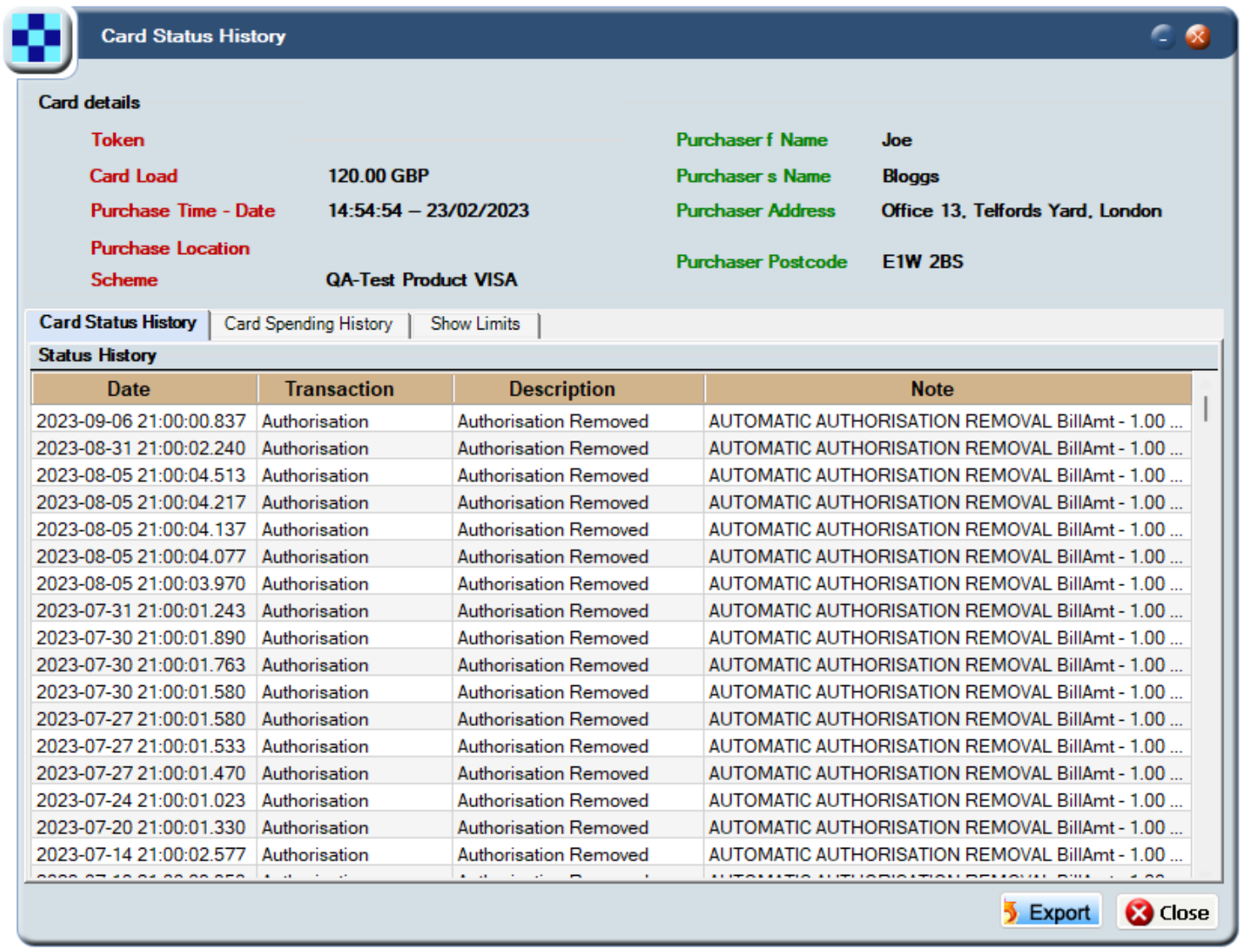


Figure 34: The Card Status History screen

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.

8.7.1 Viewing spending history

To view the spending history of a card:

1. View the Card Status History screen. See Viewing Card Status History for instructions.
2. From the **Card Status History** screen, click the **Card Spending History** tab. A history of spending activity appears.

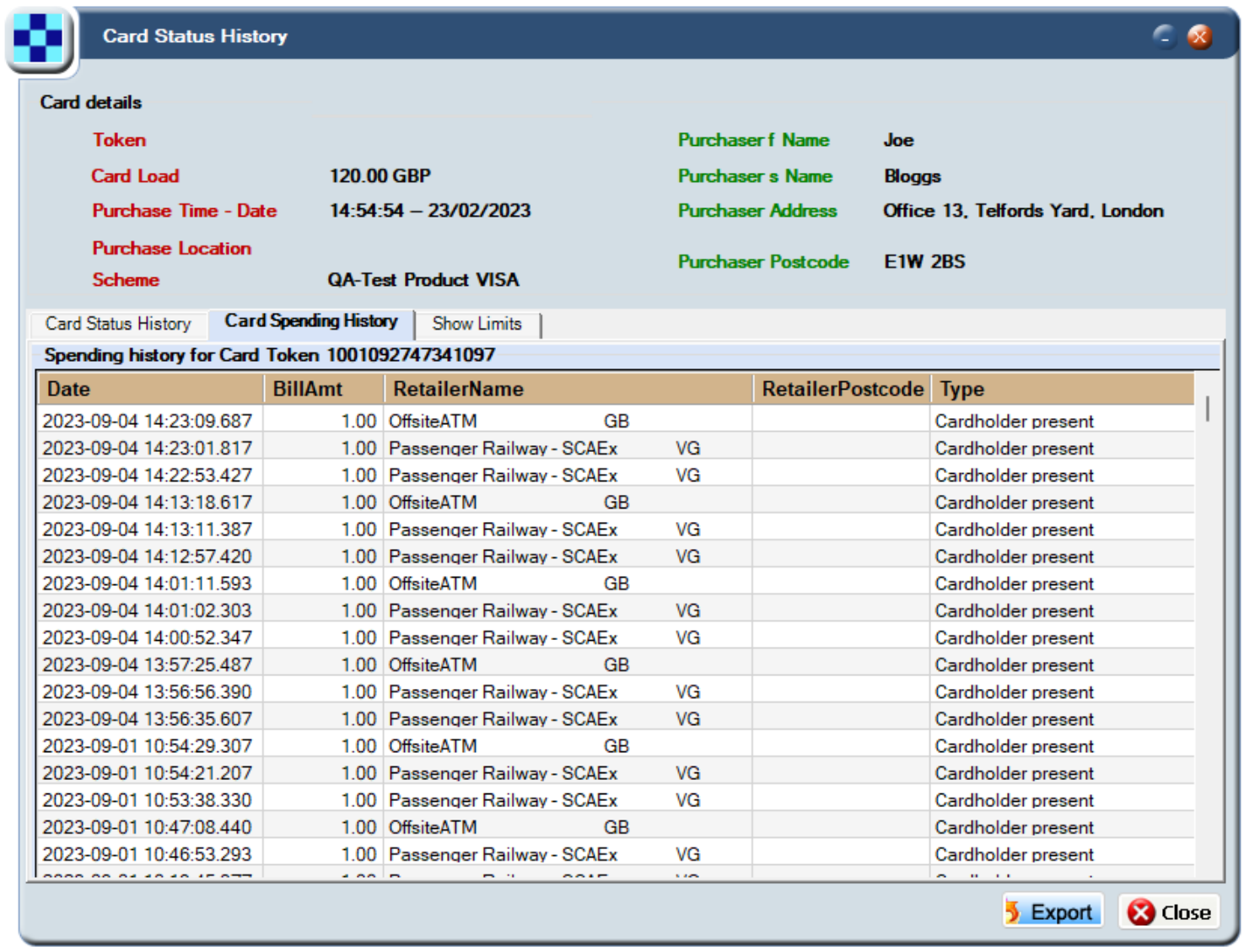


Figure 35: The Card Spending History tab on the Card Status History screen

8.7.2 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:

1. View the Card Status History screen. See Viewing Card Status History for instructions.
2. 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.

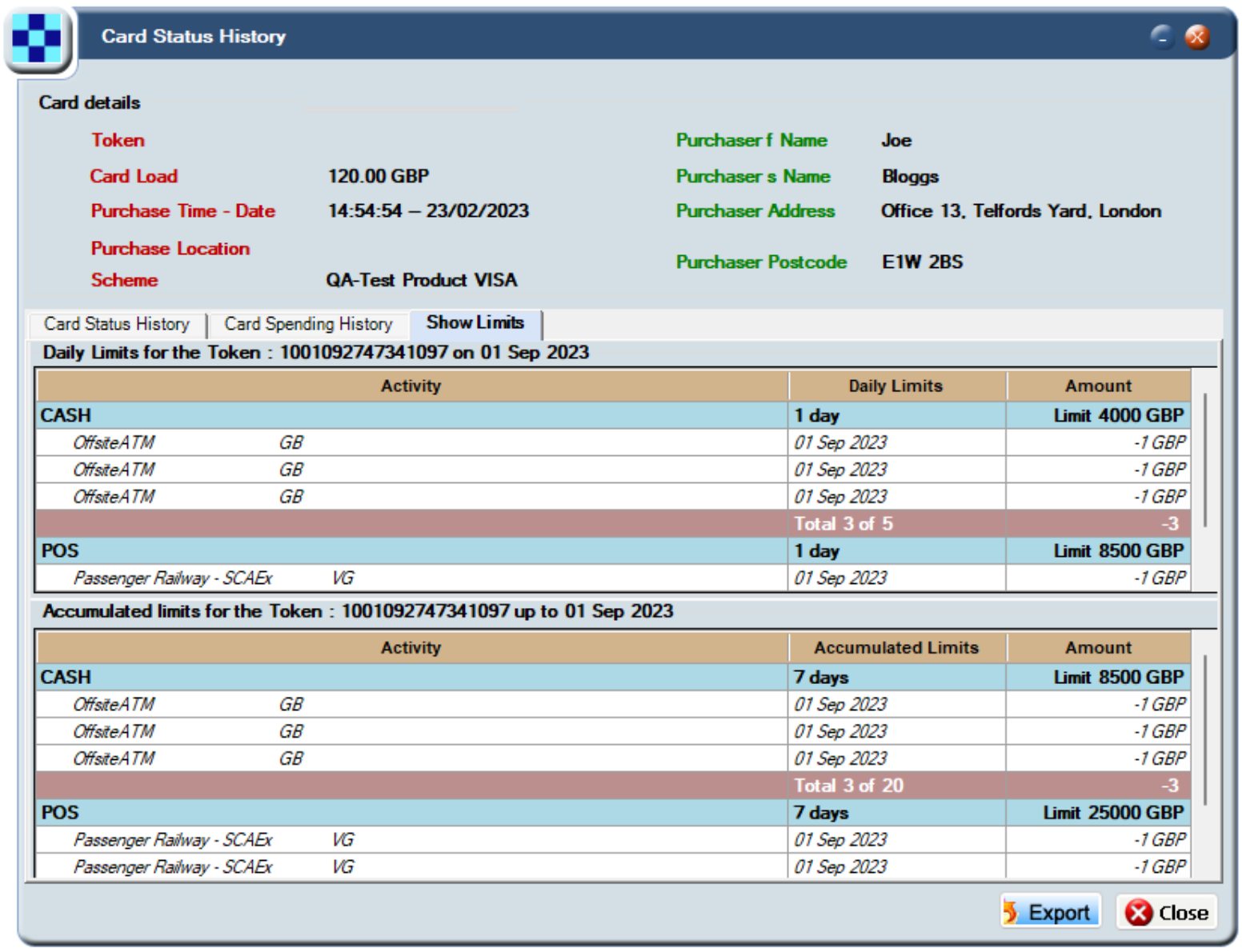


Figure 36: The Show Limits tab on the Card Status History screen

8.8 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 the setting up of fees, see the Thredd Fees Guide.

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** to display the **Card Master** screen with two additional tabs.

   Note: For more information about the details shown in the **Card Master** screen, see: Viewing Card Details.
3. Click the **Fees** tab to view the fees associated with the card.

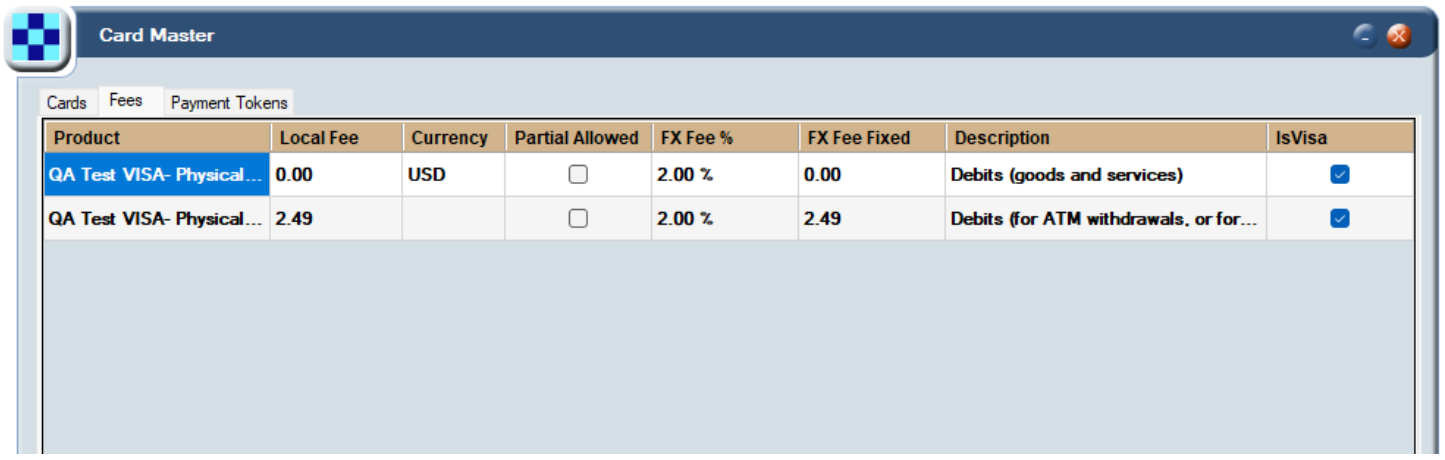


Figure 37: The Fees tab on the Card Master screen

Note:

- Fees can only be altered using a Change Request. You cannot update fees using Smart Client. Contact your Thredd Account Manager for more information.
- 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 fifty pence in their account, only a partial fee of 0.50 can be claimed.

8.9 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** to display the **Card Master** screen 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.

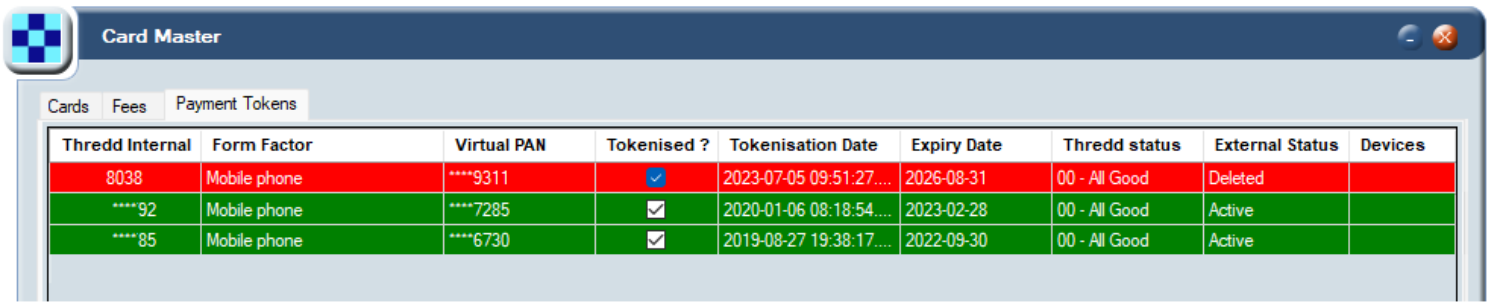


Figure 38: The Payment Tokens tab on the Card Master screen

4. Double click the required Payment Token to open the Payment Token screen.

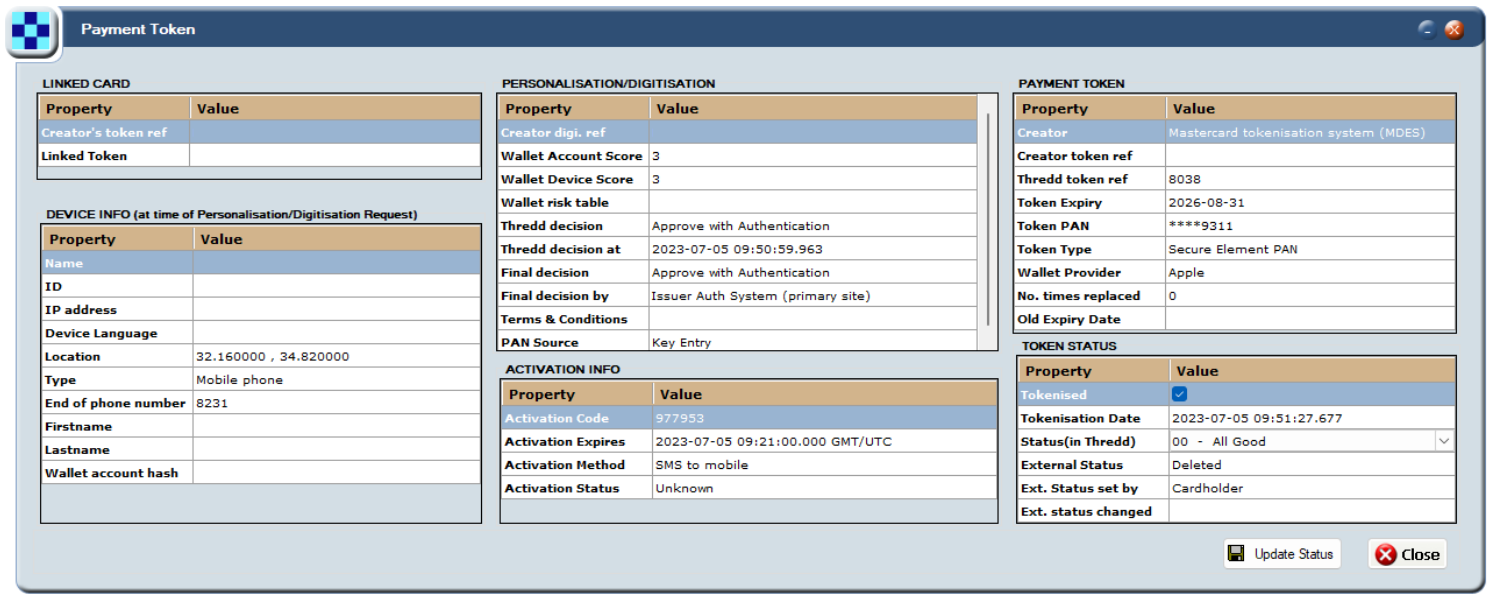


Figure 39: The Payment Token screen

Note: For more information, see Managing MDES/VDEP cards.

8.10 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.

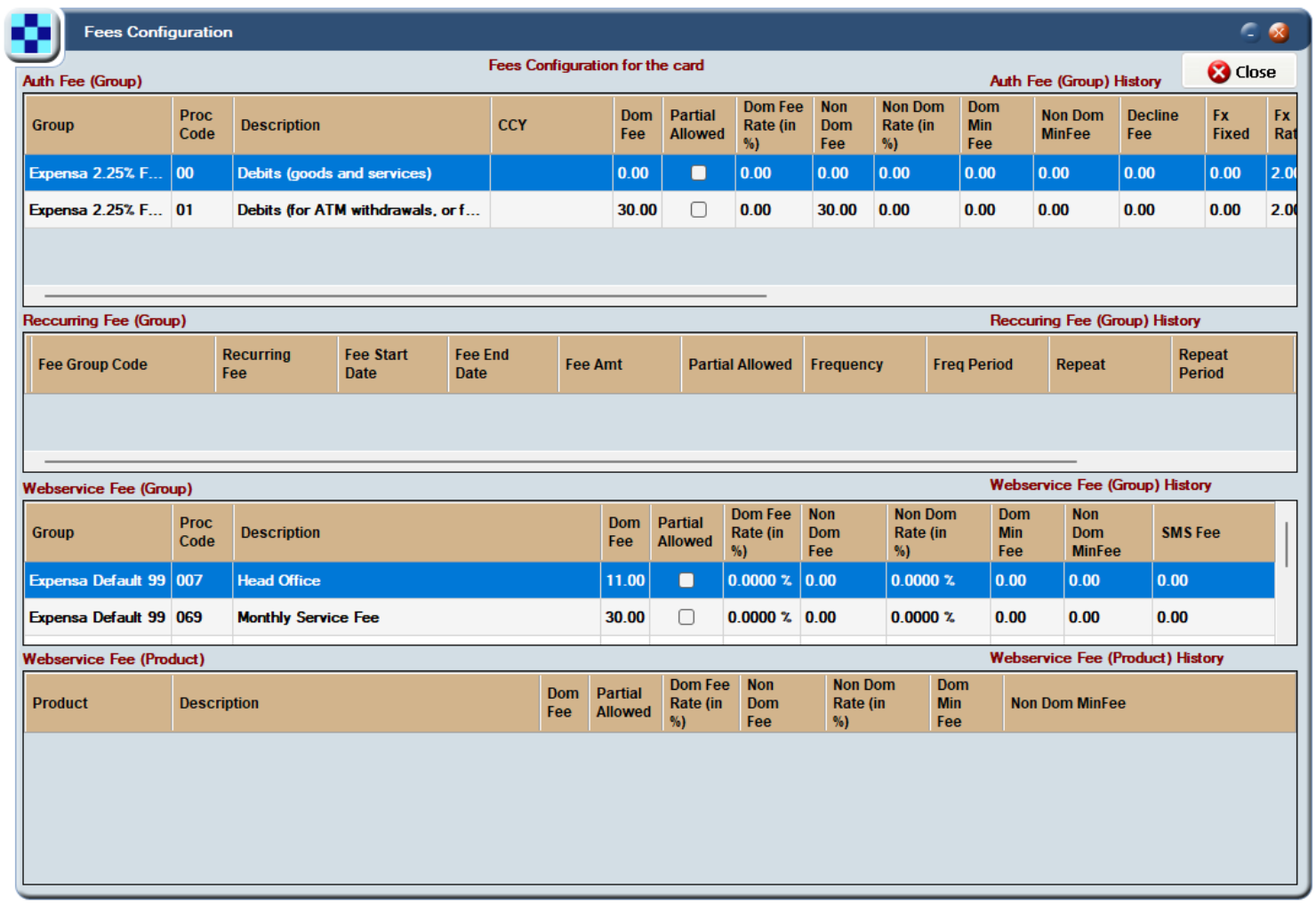


Figure 40: The Fees Configuration screen

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

The Fee Groups displayed in the Fees Configuration screen are:

- **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.
- **Webservice Fee (Group and Product)** – Displays any fees triggered by Web Services.

8.11 Next Steps

For information about managing cards and transactions, such adjusting a balance, or activating a card, see Managing Cards. For more information on fee setup, see the Thredd Fees Guide.

9 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.

9.1 Viewing Card Actions

To display the **Actions** menu:

1. Highlight a transaction in the **View Transactions** screen, then right click.
2. Select **Actions** to display the available actions. The options shown depend on the type of transaction, so the actions available on authorisations will differ from those for presentments. For example:

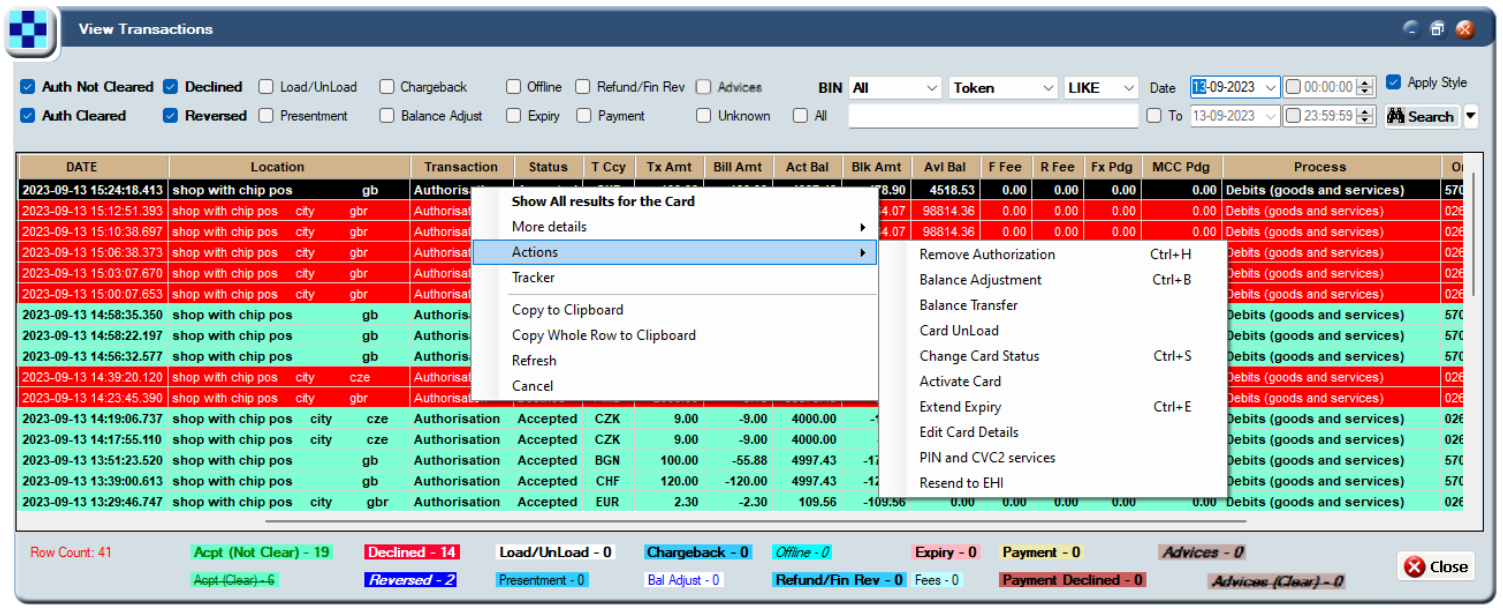


Figure 41: Options available on an authorisation

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.

9.2 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 presentment 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. Highlight a transaction in the **View Transactions** screen, then right click.
2. Select **Actions** to display the available actions, then select **Remove Authorisation**.
3. Add a note, including the JIRA reference, for the audit trail so colleagues can see why an authorisation was removed.
4. Click **Remove Now**.

Figure 42: Remove Authorisation screen

9.3 Adjusting a Balance

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

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

To adjust a balance:

1. Highlight a transaction in the **View Transactions** screen, then right click.
2. Select **Actions** to display the available actions, then select **Balance Adjustment**. The **Balance Adjustment** screen appears.

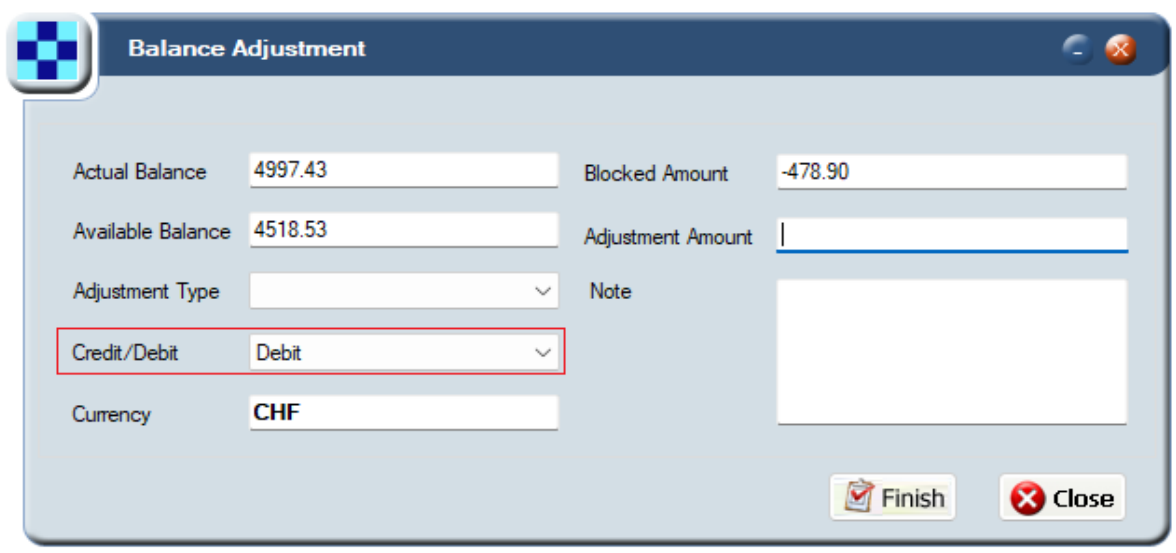


Figure 43: Balance Adjustment screen

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

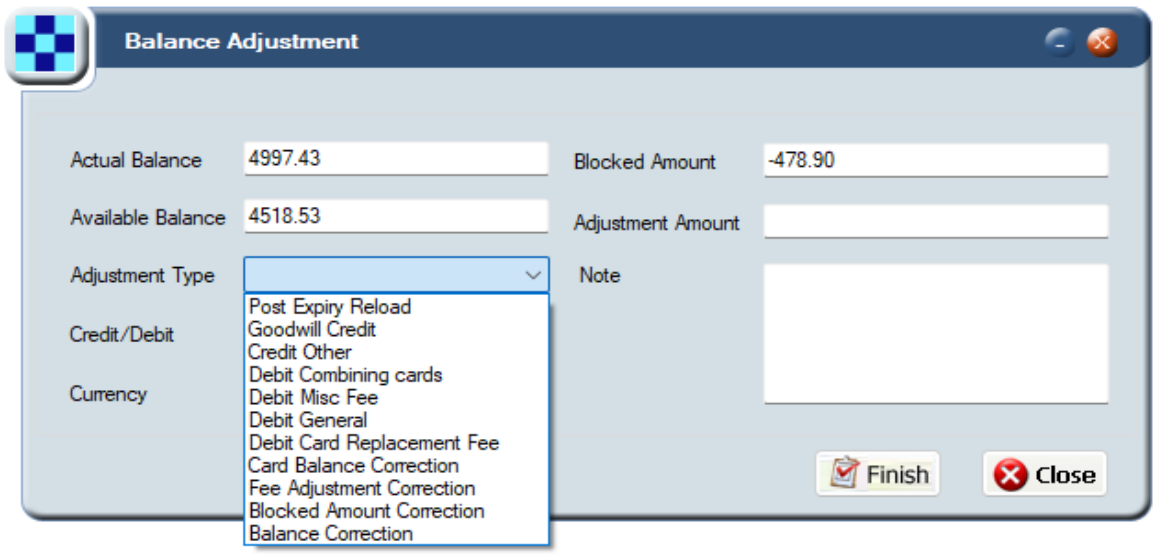


Figure 44: Balance Adjustment screen showing adjustment types

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

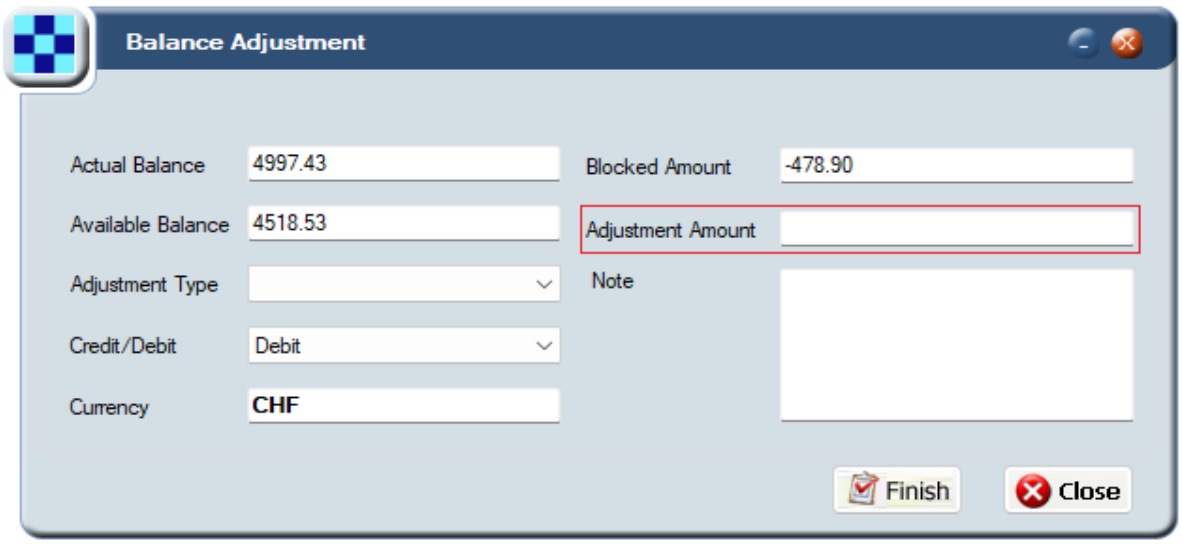


Figure 45: Balance Adjustment screen showing adjustment amount

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

6. In the **Note** field, add the reason for the adjustment, including the Jira reference. This is required for audit purposes.
7. Click **Finish**.

9.4 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. Highlight a transaction in the **View Transactions** screen, then right click.
2. Select **Actions** to display the available actions, then select **Balance Transfer**. The **Balance Transfer** screen appears showing the actual and available balance on the card, and any blocked amount.

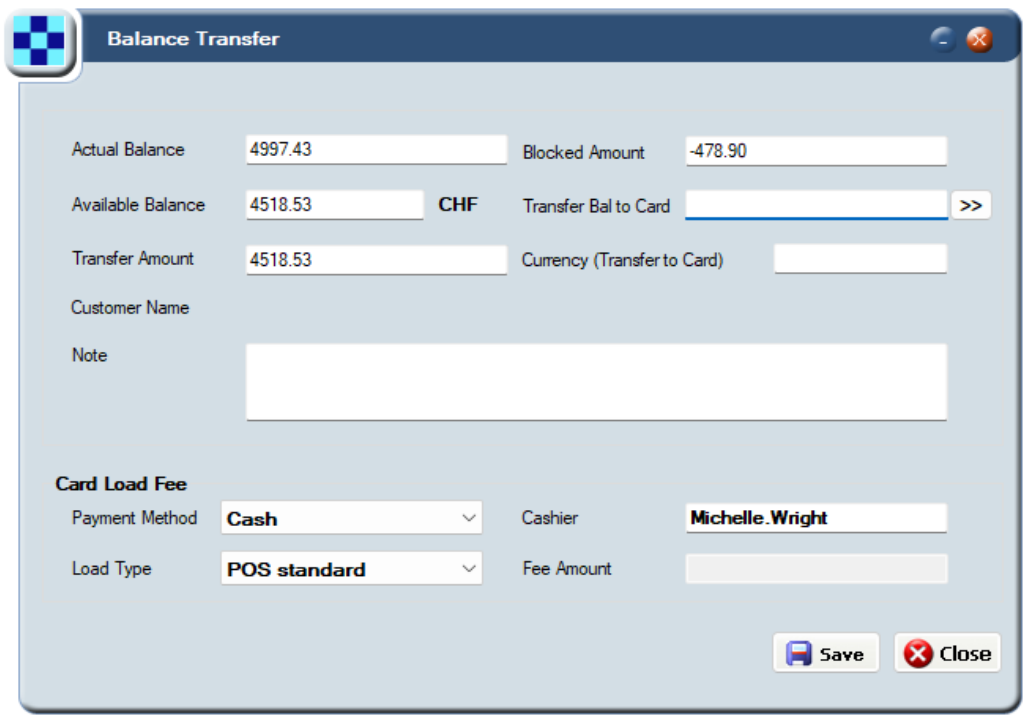


Figure 46: Balance Transfer screen

3. Enter the amount you want to transfer in **Transfer Amount**.
4. In **Transfer Bal to Card**, click the arrow and specify the token you want to transfer the balance to.
5. 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.
6. Click **Save**.

9.5 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. Highlight a transaction in the **View Transactions** screen, then right click.
2. Select **Actions** to display the available actions, then select **Card Unload**. The **Card Unload** screen appears.

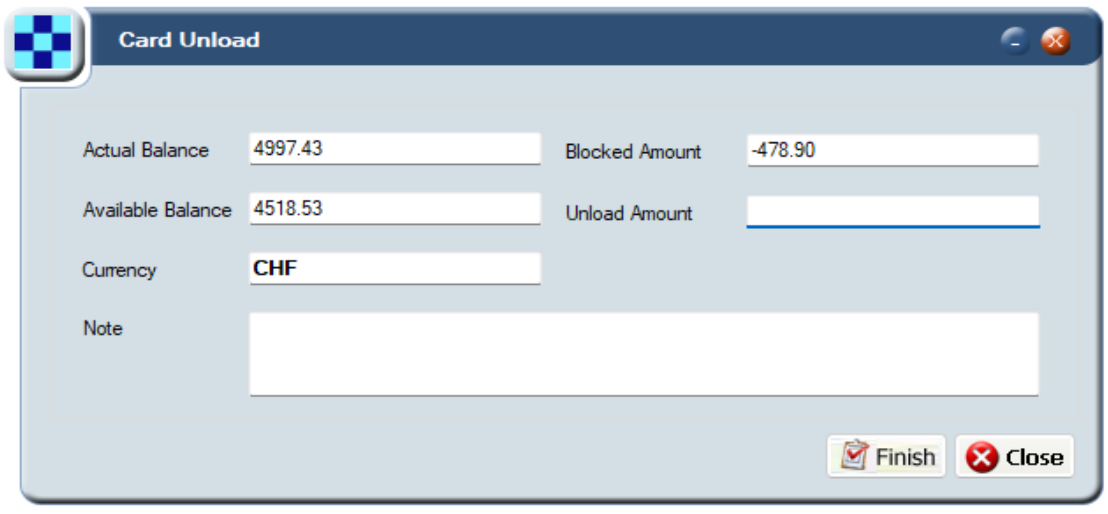


Figure 47: Card Unload screen

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

9.6 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 Thredd Web Service APIs to do this (Ws_StatusChange). For more information, see the *Web Services Guide*.

To change the status of a card:

1. Highlight a transaction in the **View Transactions** screen, then right click.
2. Select **Actions** to display the available actions, then select **Change Card Status**. The **Status Change** screen appears.
3. From the **Change Card Status To** drop-down box, select a card status.

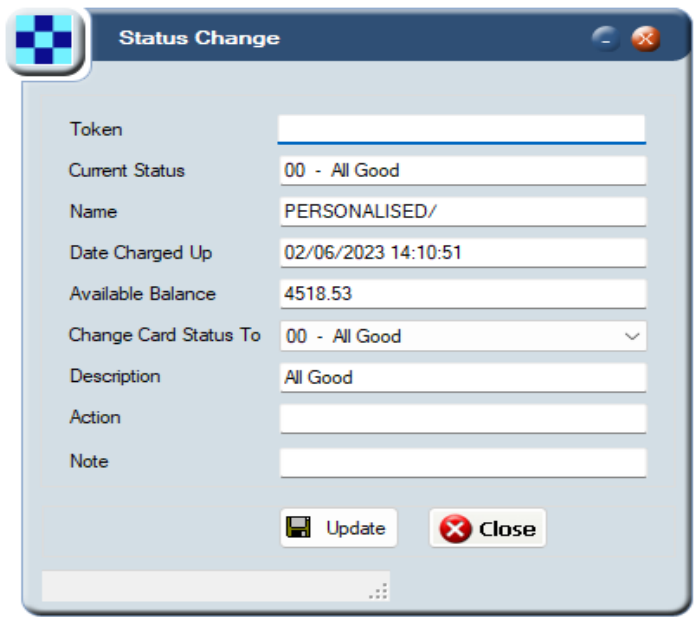


Figure 48: Status Change screen

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.

4. Add a note for audit purposes.
5. Click **Update** to apply the status change.

Note:

- 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 Thredd 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).

9.7 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. Highlight a transaction in the **View Transactions** screen, then right click.
2. Select **Actions** to display the available actions, then select **Activate Card**.

Figure 49: Activate Card screen

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

9.8 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 Thredd 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. Highlight a transaction in the **View Transactions** screen, then right click.
2. Select **Actions** to display the available actions, then select **Extend Expiry**.

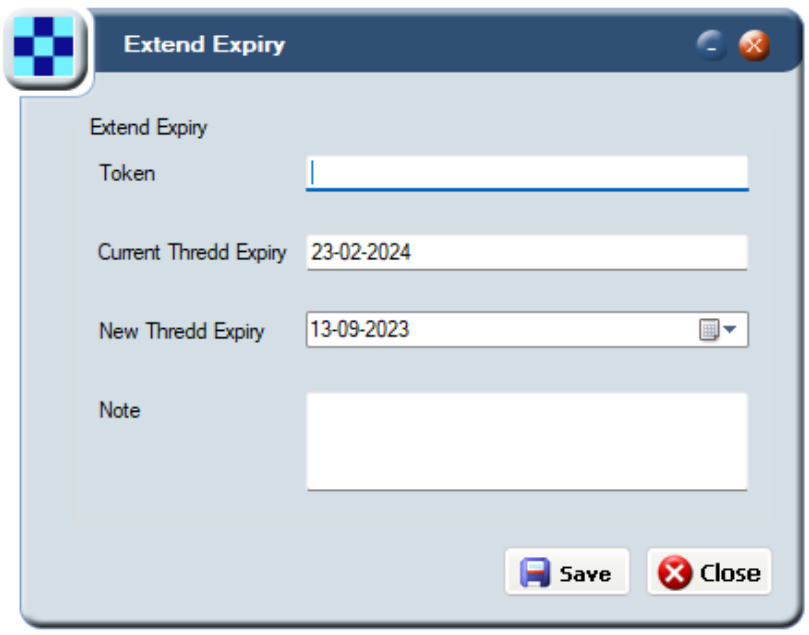


Figure 50: Extend Expiry screen

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

9.9 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. Highlight a transaction in the **View Transactions** screen, then right click.
2. Select **Actions** to display the available actions, then select **Edit Card Details**. The **Card Master** screen appears.

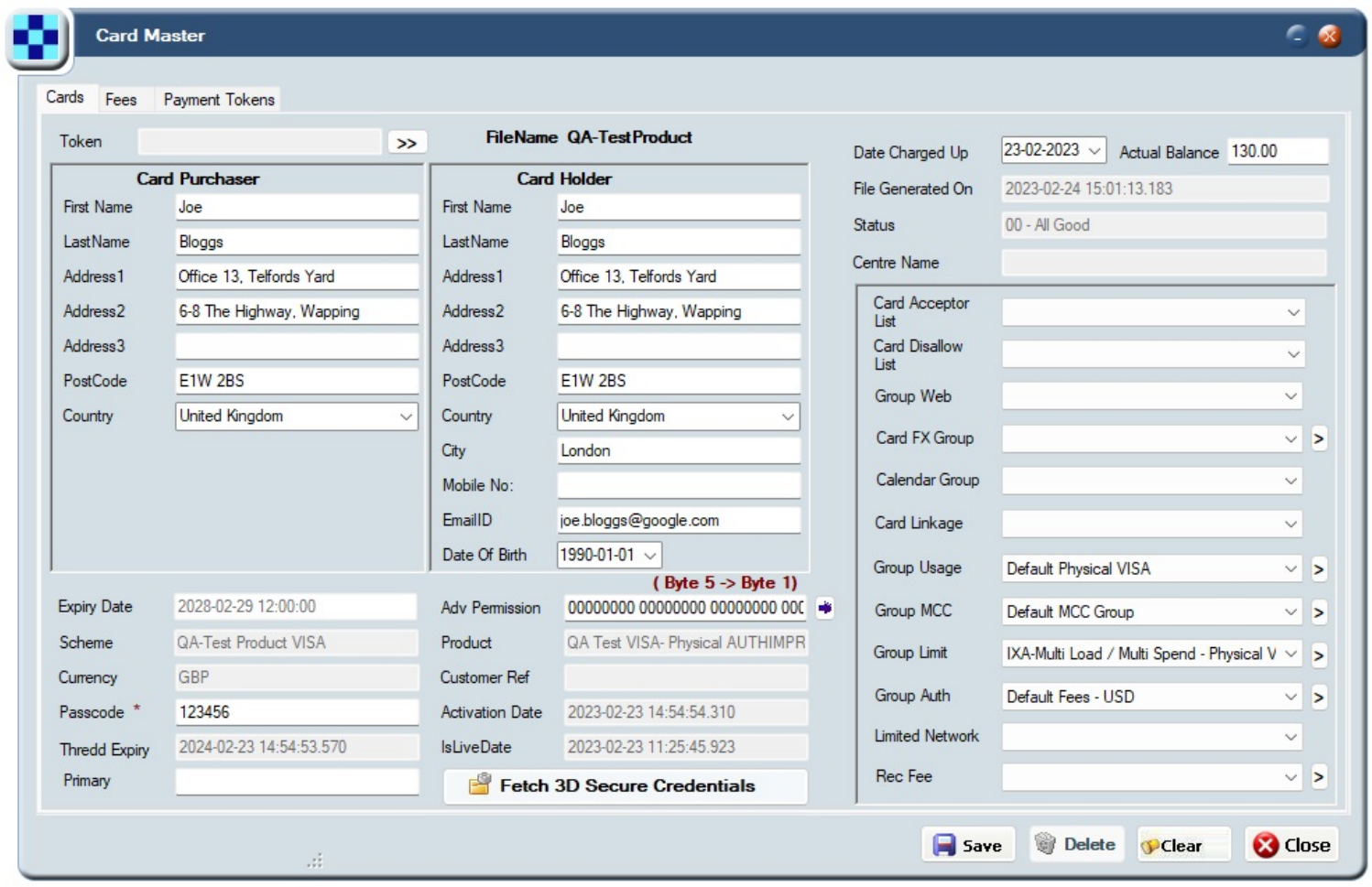


Figure 51: Editable Card Master screen

Note: 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**.

3. 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.

9.10 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 Thredd system is the online PIN.

To unblock a PIN:

1. Highlight a transaction in the **View Transactions** screen, then right click.
2. Select **Actions** to display the available actions, then select **PIN and CVC2 Services**.

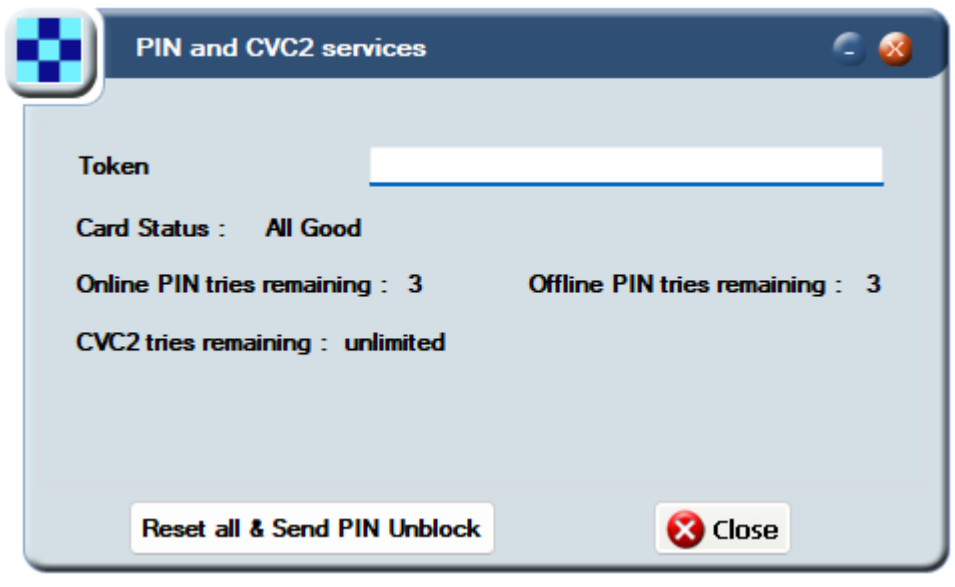


Figure 52: PIN and CVC2 services screen

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 three consecutive incorrect attempts. Online PIN checks are counted when the PIN is checked against the PIN stored in the Thredd system, not the PIN of the chip.
- **Offline PIN tries remaining** – the number of offline PIN attempts left as received from the card on the last online transaction. The actual value is held inside the chip and could be different to the last one sent to Thredd. The limit is three 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 Thredd system is updated only when the card is used at an online EMV-capable terminal.

9.10.1 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.

9.10.2 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 does not 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)

1. Highlight a transaction in the **View Transactions** screen, then right click.
2. Select **Actions** to display the available actions, then select **PIN and CVC2 Services**
3. Click **Reset all and send PIN unblock**.

9.11 Resending a Transaction to EHI

Note: This feature is available on request. For information, contact your Thredd 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. For more information, see the External Host Interface (EHI) Guide.

To resend a transaction to EHI:

1. Highlight a transaction in the **View Transactions** screen, then right click.
2. Select **Actions** to display the available actions, then select **Resend to EHI**.

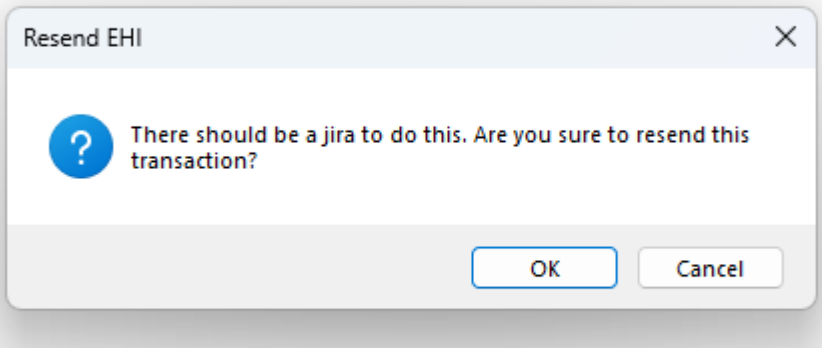


Figure 53: Resend to EHI message.

3. Click **OK** to proceed. The transaction's EHI message is resent to your host.

9.12 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:

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

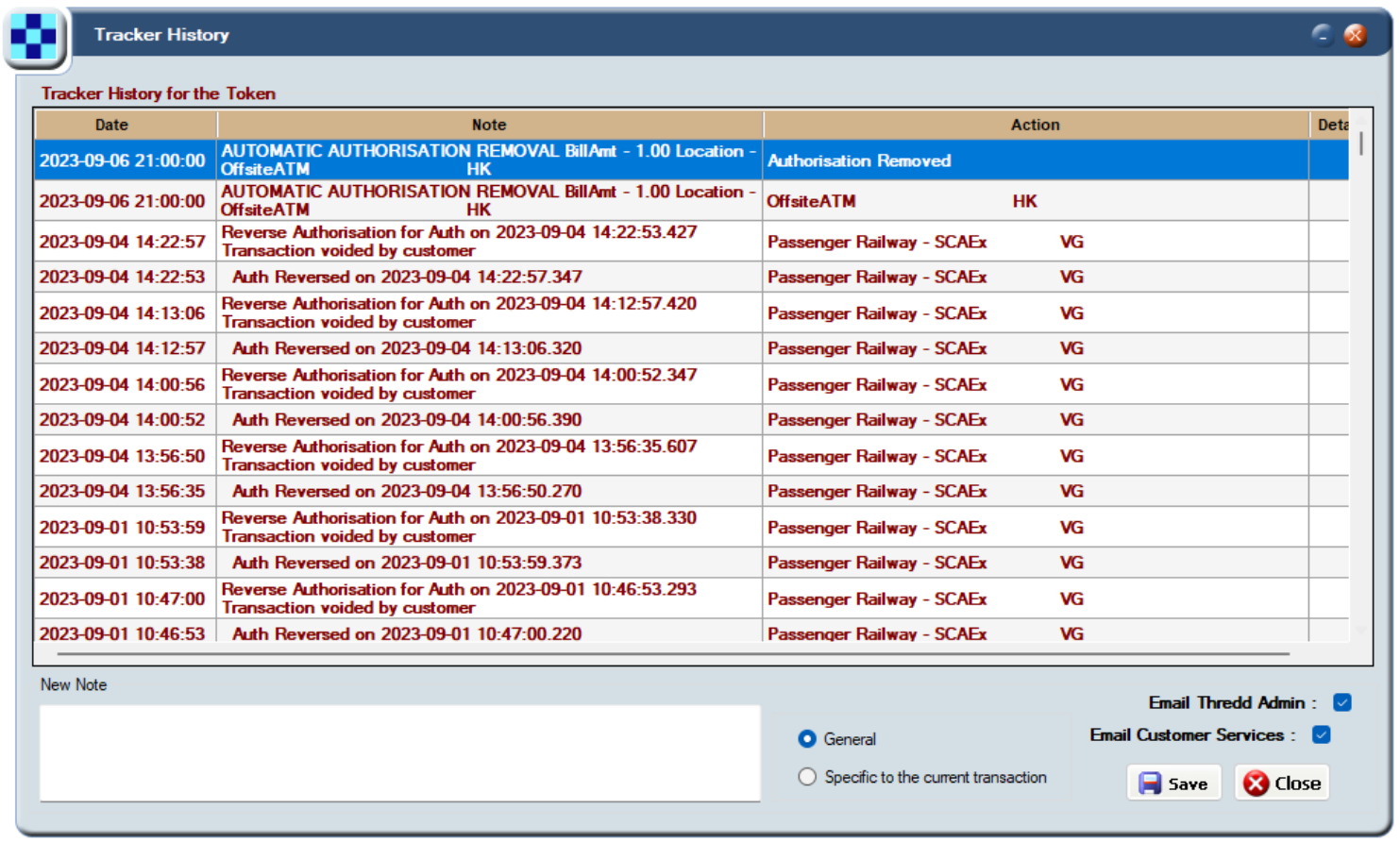


Figure 54: Tracker History screen showing a history of all the actions applied to a token

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

9.12.1 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. Highlight a transaction in the **View Transactions** screen, then right click.
2. Select **Tracker** to display the **Tracker History** screen.
3. Input the message into **New Note** (bottom-left of the screen).

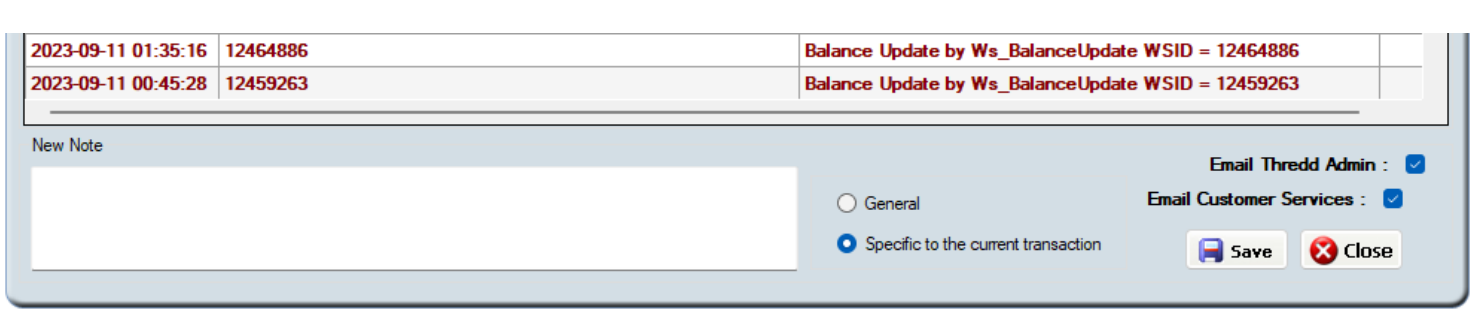


Figure 55: Adding a new note to a transaction in the Tracker History screen.

4. To apply the note to this particular transaction, select **Specific to the current transaction**.
5. Click **Save**. The note is appended to the transaction.

10 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 Thredd to use the Mastercom API data feed for your BIN codes.
- Costs for the service must be agreed with your Thredd Account Manager and added as an addendum to your Thredd 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.
- 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 Thredd Support for details.

10.1 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.

1. From the Smart Client menu, select **Card Activity** > **View Transactions** to view the **Transactions** screen.
2. From the **View Transactions** screen, right-click the transaction being disputed by the cardholder and select **Actions** > **Create Chargeback**.

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).

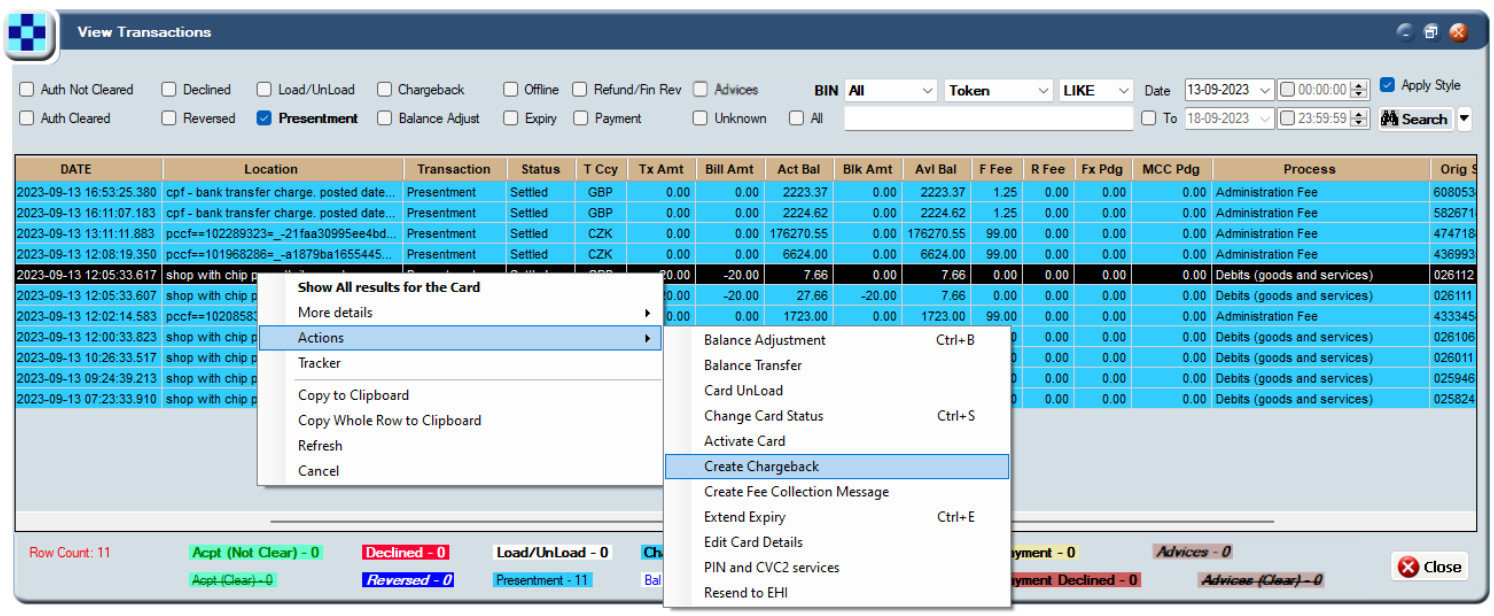


Figure 56: Create Chargeback menu option

3. From the **Chargebacks** screen, enter the details of the chargeback. Refer to the table in the section Handling error codes.

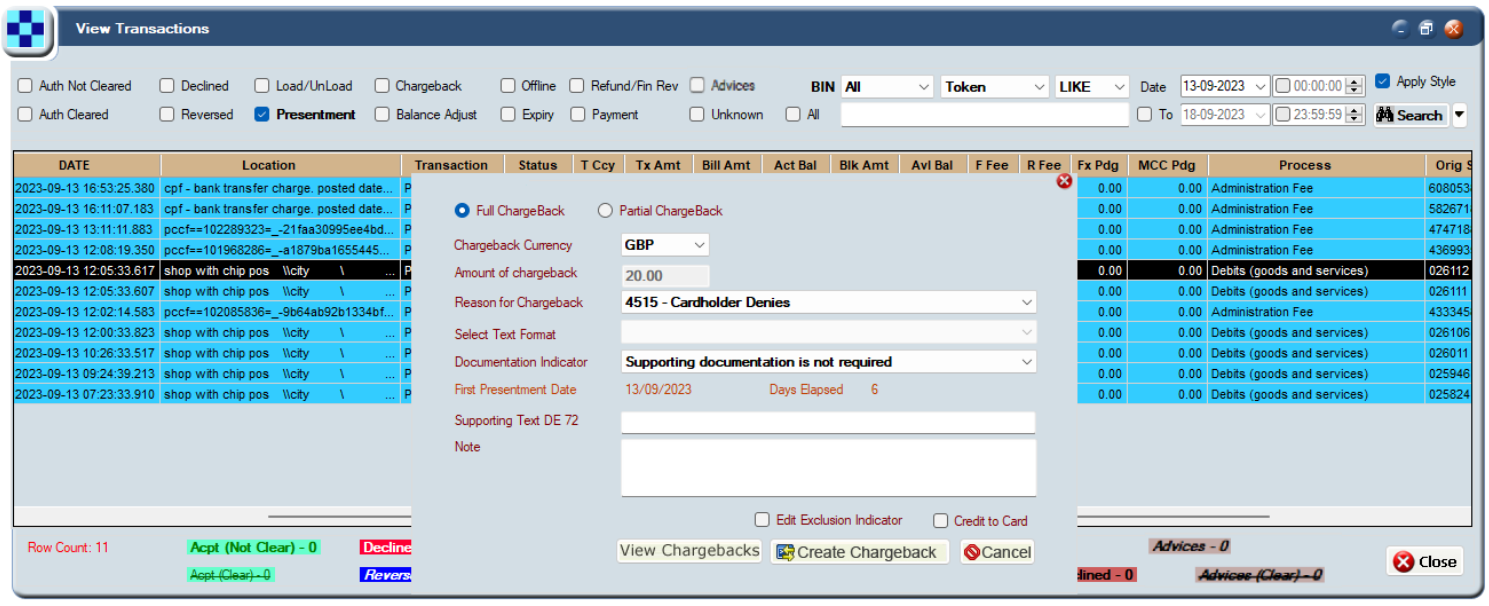


Figure 57: Create Chargeback screen

4. 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.

   Note:
   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.

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 Thredd processing of the chargeback request. You can try fixing the details and resending the chargeback request or contact Thredd 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 *Mastercard Chargeback Guide*. **Note:** If the reason is fraud related, you must create a SAFE Report before issuing the chargeback.

Chargeback Option	Description
Select text format	The available text format options depend on the Reason for chargeback previously selected. Some chargeback reasons do not provide a default text format. If you are unsure as to which format to select, check with your Account Manager. Depending on the selection, this reason is also populated in the Supporting Text DE 72 field.
Documentation Indicator	Select how documentation to support this chargeback will be supplied: • Supporting documentation is not required • Supporting documentation will follow Refer to the *Mastercard Guide* for details of the types of Chargeback Reason Codes that require supporting documentation.
Days Allowed	Read-only field indicating the number of days allowed to process the chargeback. This varies between region and chargeback reason code. Typical values are 90 days, 120 days, and 540 days.
Days Remaining	Read-only field indicating the number of days remaining to process the chargeback. If this number is negative, it indicates the period in which to submit the chargeback has been exceeded. If you submit the chargeback, Mastercom will reject it.
Supporting Text DE 72	Add a description, to be displayed in the DE 72 field of the chargeback message sent to Mastercom. This field can also be populated with a standard message as selected in the Select Text Format field.
Note	Free text field to enable you to add an internal note about the chargeback request. This note is not passed on to Mastercom.
Edit Exclusion Indicator	Check this option to indicate to Mastercom they should ignore the Days Allowed/Days Remaining indicator. This enables you to still raise a chargeback, even if the Mastercard default eligibility period has expired. **Note:** This functionality is not yet released. Check with your Thredd Account Manager for details.
Credit to Card	If you check this option, the chargeback amount will be credited back to the card.

10.2 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**.

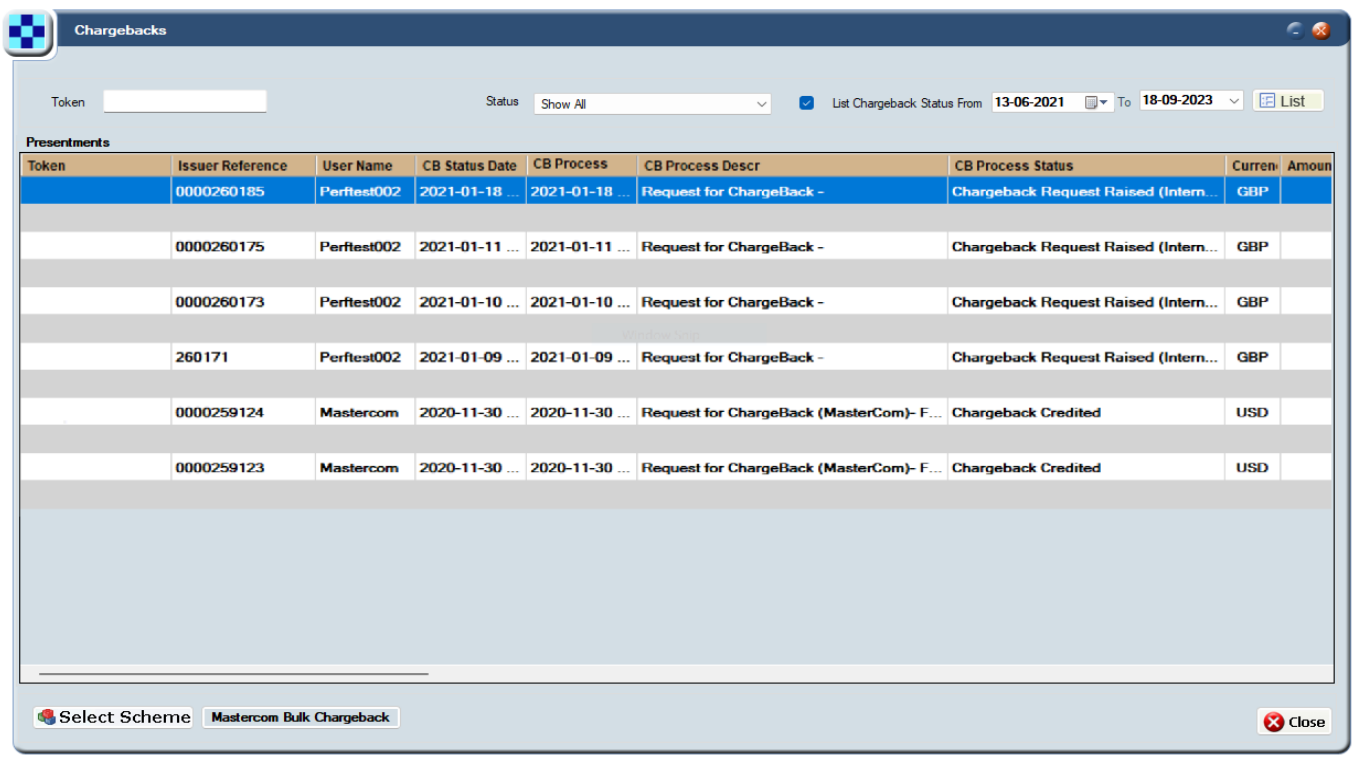


Figure 58: Chargebacks screen

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:

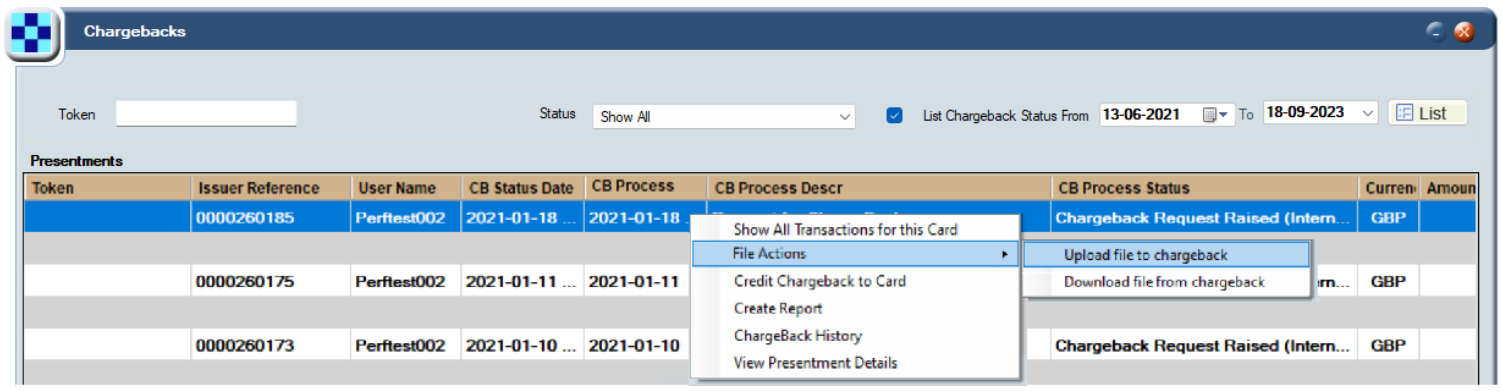


Figure 59: Further actions available on a chargeback

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. Card schemes are also known as payment networks.

10.3 Viewing Chargeback Transactions

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

10.3.1 Showing all Transactions for a Card

You can display all transactions for a card linked to a chargeback.

To show all transactions for a card linked to a chargeback:

1. From the Smart Client menu, select **Card Activity** > **Chargebacks** to view the **Chargebacks** screen.
2. From the **Chargebacks** screen, right-click the required transaction and select **Show All Transactions for this Card**.

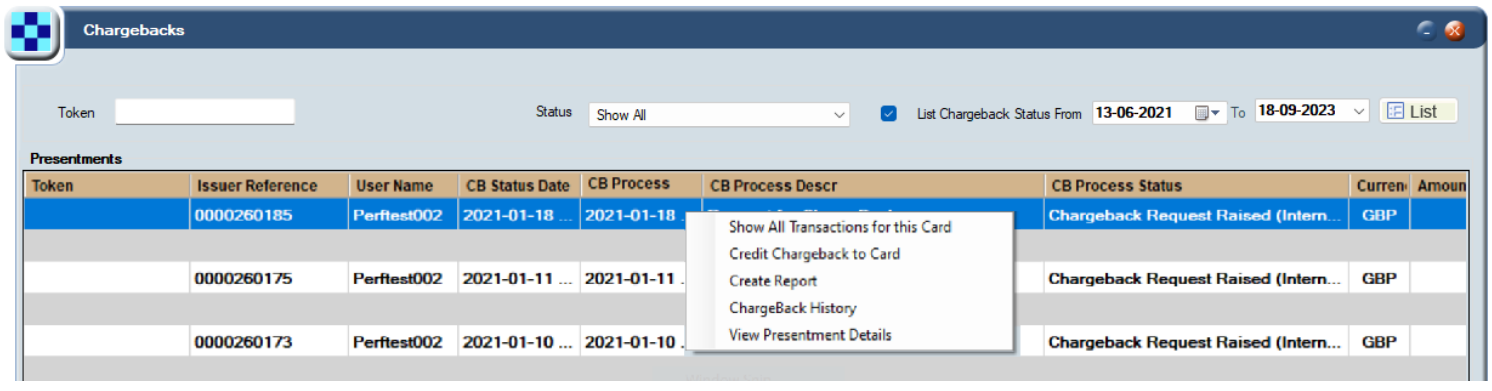


Figure 60: Show All Transactions for this Card option

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

10.3.2 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 (payment network) that the chargeback was successful. Note that this is done by clients; not Thredd.

To credit the chargeback amount back to the card:

1. From the Smart Client menu, select **Card Activity** > **Chargebacks** to view the **Chargebacks** screen.
2. From the **Chargebacks** screen, right-click the required transaction and select **Credit Chargeback to Card**.
3. A pop-up 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.

10.3.3 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:

1. From the Smart Client menu, select **Card Activity** > **Chargebacks** to view the **Chargebacks** screen.
2. From the **Chargebacks** screen, right-click the required transaction and select **Create Report**. The **Transaction Details** screen is displayed.

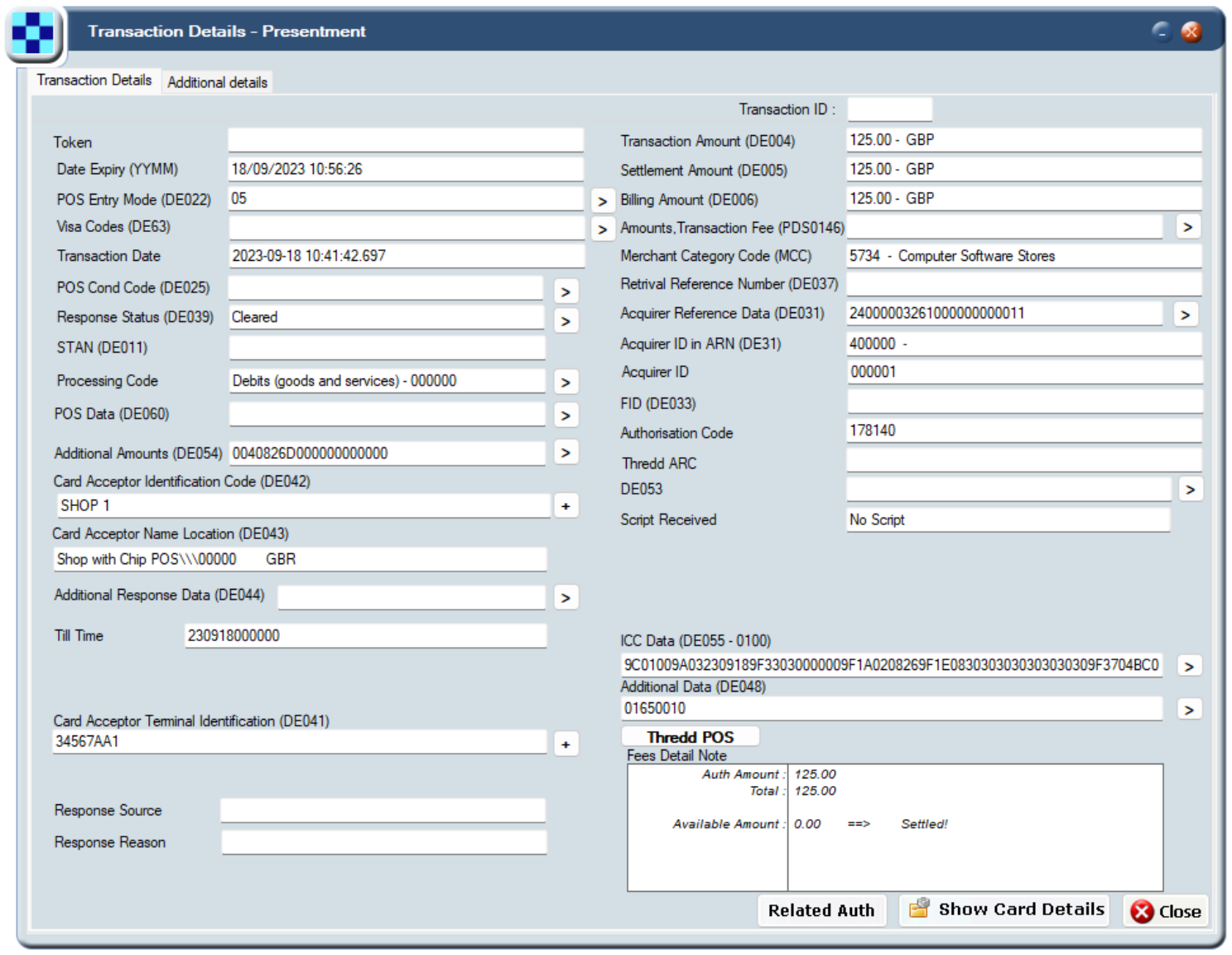


Figure 61: Transaction Details screen

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

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

10.3.4 Viewing Presentment Details

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

To view details of the presentment transaction linked to the chargeback:

1. From the Smart Client menu, select **Card Activity** > **Chargebacks** to view the **Chargebacks** screen.
2. In the **Chargebacks** screen, right-click the required transaction and select **View Presentment Details**. The **View Transactions - Presentments** screen is displayed, showing details of the linked presentment transaction.

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

10.3.5 Viewing Chargeback History

To view the Chargeback history of a chargeback transaction:

1. From the Smart Client menu, select **Card Activity** > **Chargebacks** to view the **Chargebacks** screen.
2. From the **Chargebacks** screen, right-click the required transaction and select **Chargeback History**. The **Chargeback History** screen is displayed.

Figure 62: Chargeback History screen

10.3.6 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. From the Smart Client menu, select **Card Activity** > **View Transactions** to view the **Transactions** screen.
2. In the **Transactions** screen, right-click the required transaction and select **Create Retrieval Request**. The **Create Retrieval Request** screen is displayed.

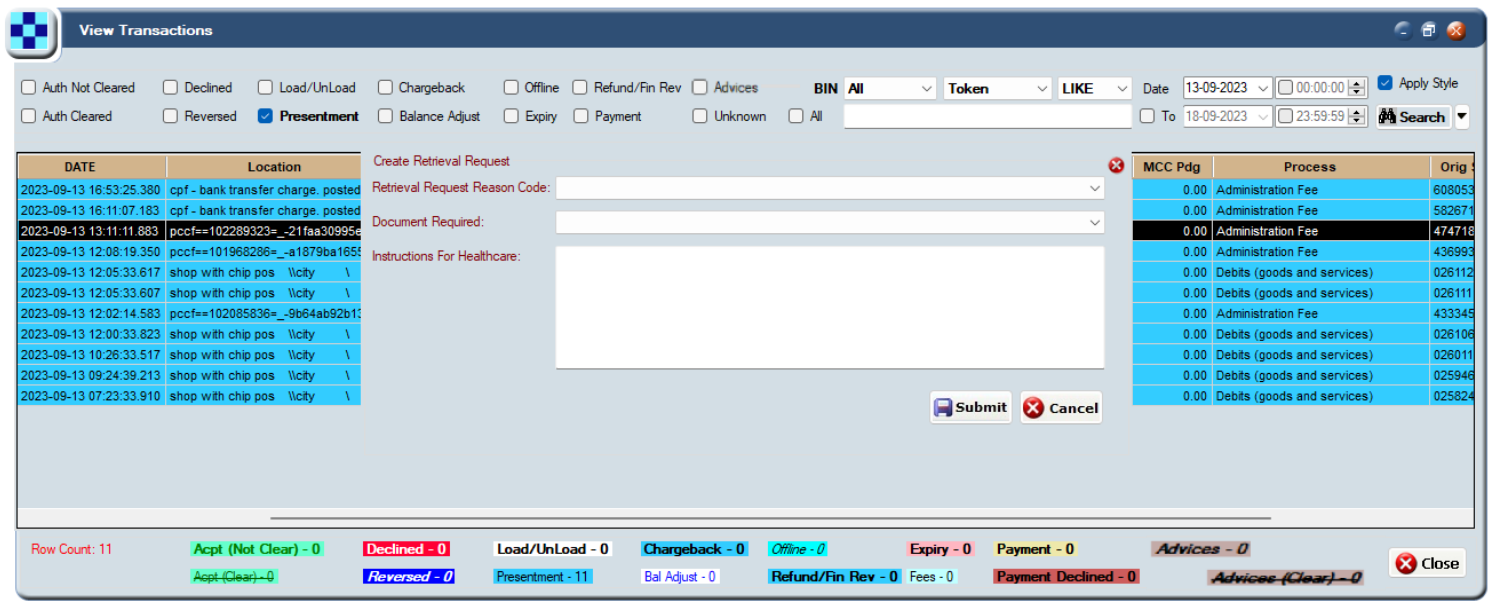


Figure 63: Create Retrieval Request screen

3. In **Retrieval Request Reason Code**, select an appropriate reason for the retrieval request. For details, see the table in the section Retrieval Request Reason Codes.
4. In **Document Required**, select the format required. The available options are:
    a. Hard copy of the original document
    b. Copy or image of the original document
    c. Substitute draft

5. Click **Submit**.

   Note: 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 Thredd support.

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

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.

Retrieval Request Reason Codes

The following table contains a list of the available Retrieval Request reason codes.

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.

10.3.7 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.

To reverse a chargeback:

1. From the Smart Client menu, select **Card Activity** > **Chargebacks** to view the **Chargebacks** screen.
2. From the **Chargebacks** screen, right-click the required transaction and select **Reverse Chargeback**.
3. A pop-up 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.
4. To close the message box, click **OK**. A chargeback reversal message is sent to Mastercom.

10.3.8 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.

To re-raise a chargeback:

1. From the Smart Client menu, select **Card Activity** > **Chargebacks** to view the **Chargebacks** screen.
2. From the **Chargebacks** screen, right-click the rejected chargeback transaction and select **Re-Raise Chargeback**. The following screen is displayed:

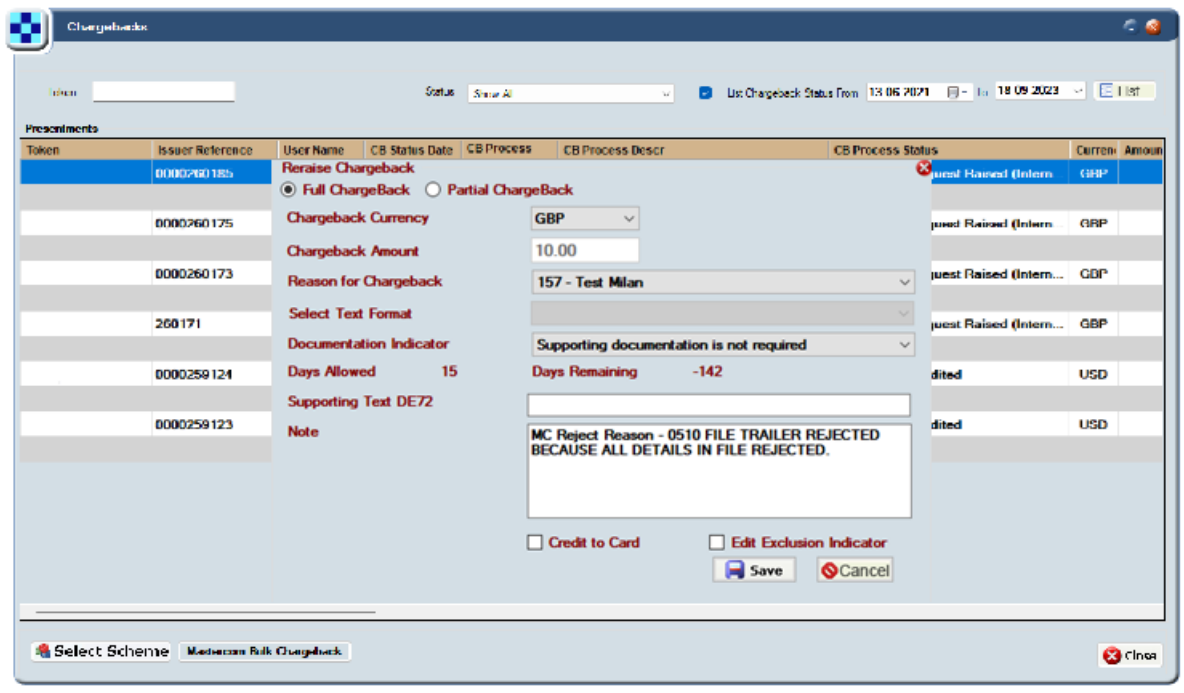


Figure 64: Reraise Chargeback screen

3. 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.

10.4 Uploading and Downloading Supporting Documents

10.4.1 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.

To upload supporting documentation for the chargeback:

1. From the Smart Client menu, select **Card Activity** > **Chargebacks** to view the **Chargebacks** screen.
2. From the **Chargebacks** screen, right-click the required transaction and select **File Actions** > **Upload file to chargeback**. The following screen is displayed:

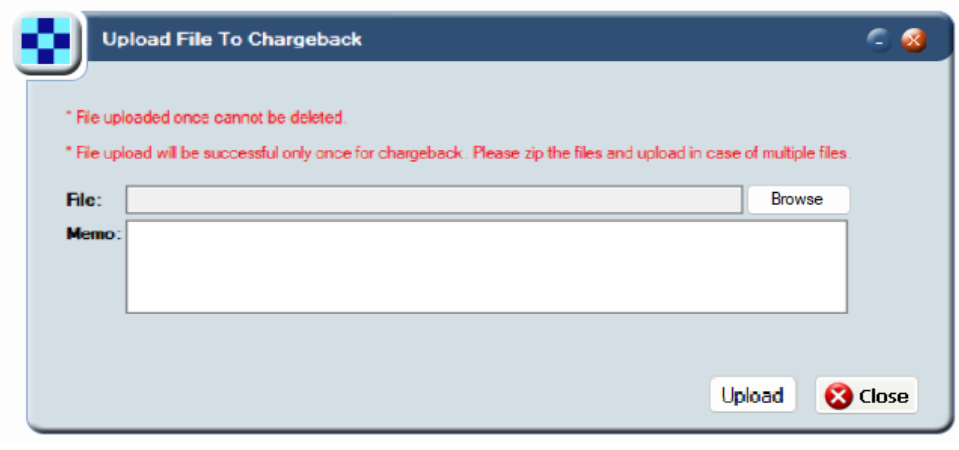


Figure 65: Upload File to Chargeback screen

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

3. To select a file to upload, click **Browse**.
4. In **Memo**, provide further details of the file being uploaded.
5. 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; Thredd does not have access to the details in the file.

10.4.2 Downloading Chargeback Documentation

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

To download documentation linked to the chargeback:

1. From the Smart Client menu, select **Card Activity** > **Chargebacks** to view the **Chargebacks** screen.
2. From the **Chargebacks** screen, right-click the required transaction and select **File Actions** > **Download file from chargeback**. The following screen is displayed:

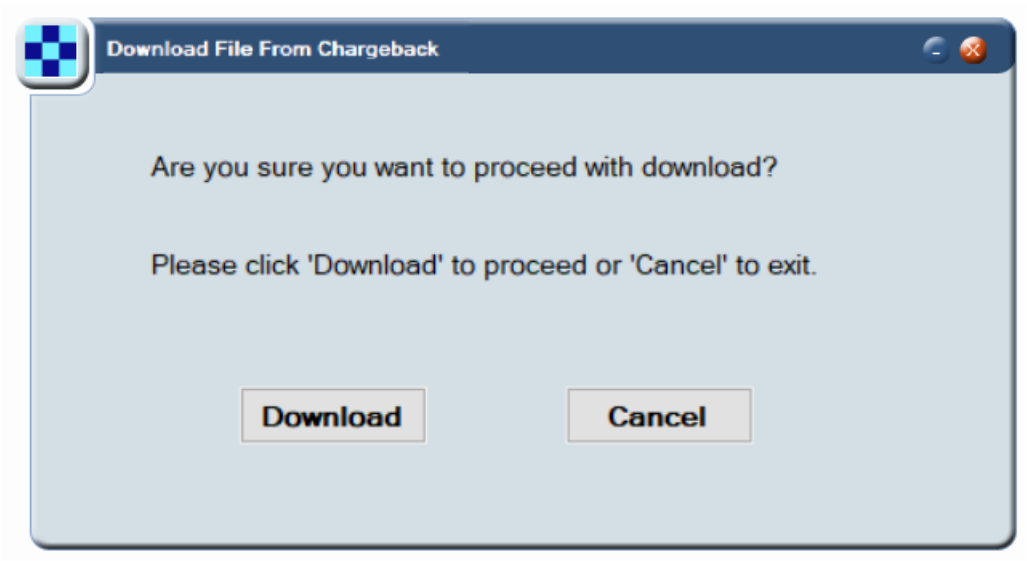


Figure 66: Download File From Chargeback screen

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

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

10.5 Viewing and Managing Fee Collections

10.5.1 Create a Fee Collection Message

Smart Client supports the sending and receiving of fee collections related to disputes.

1. From the Smart Client menu, select **Card Activity** > **View Transactions** to view the **Transactions** screen.
2. In the **Transactions** screen, right-click the required transaction and select **Create fee collection message**. The Mastercom Fee Collection screen is displayed.

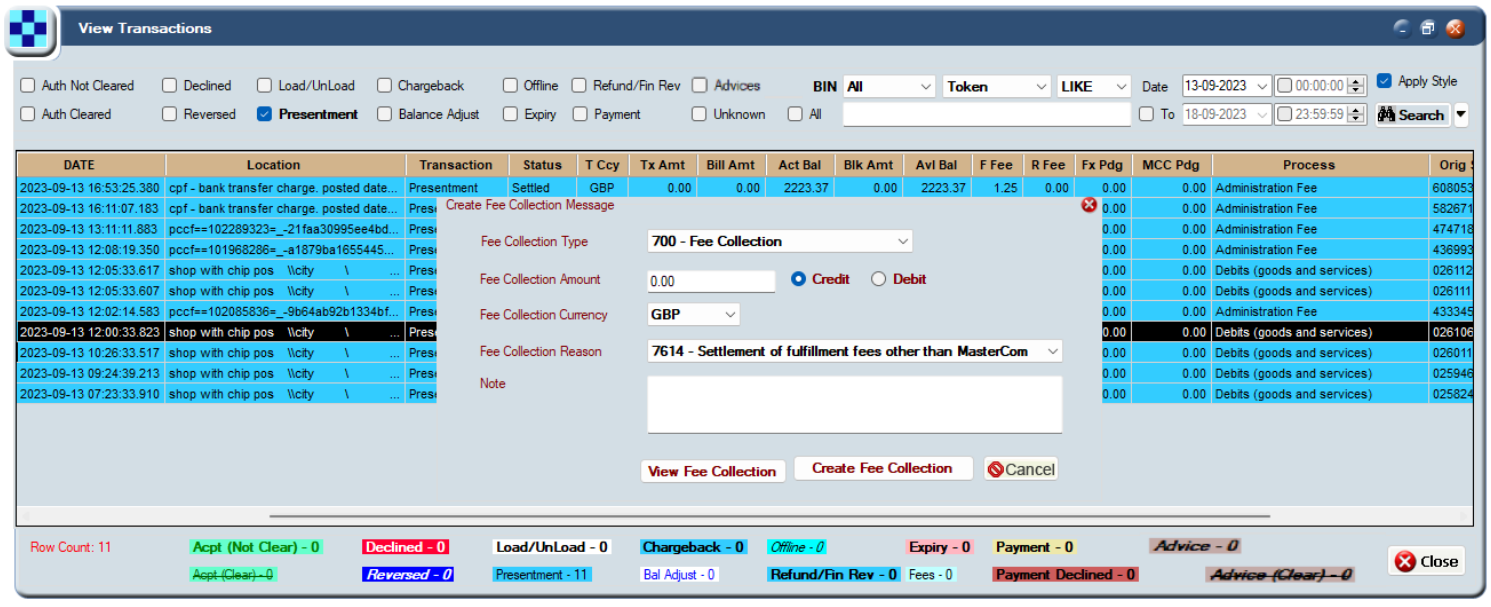


Figure 67: Mastercom Fee Collection screen

About Fee Collections fields

The following table contains information about each of the fee collection fields.

Fee Collection Information	Description
Fee Collection Type	Select the type of fee collection. Options include: • 700 - Fee Collection • 780 - Fee Collection Return • 781 - Fee Collection Return Resubmission • 782 - Fee Collection Arbitration Return
Fee Collection Amount	Enter the fee collection amount. Up to two decimal places are allowed. Tick one of the following options to indicate who to credit the fee to: • Credit sender – fee will be credited to your account • Credit receiver – fee will be credited to the receiver.
Fee Collection Currency	Select the currency of the fee.
Fee Collection Reason	Select the reason for the fee collection (DE 25 Message Reason Code values that apply to the fee collection).
Note	Free text field to enable you to add a short message about the fee.

10.5.2 Creating a Mastercom Fee Collection message

Mastercom supports the ability of issuers to send and receive fee collections related to disputes.

Note: 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. From the Smart Client menu, select **Card Activity** > **View Transactions** to view the **Transactions** screen.
2. In the **Transactions** screen, right-click the required transaction and select **Create Mastercom fee collection message**. The Mastercom Fee Collection screen is displayed.

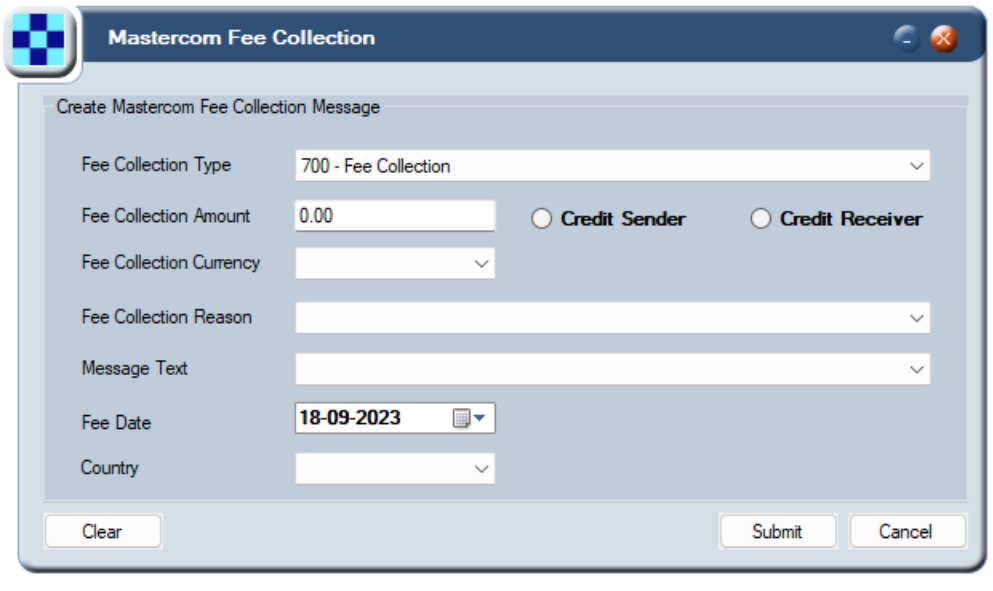
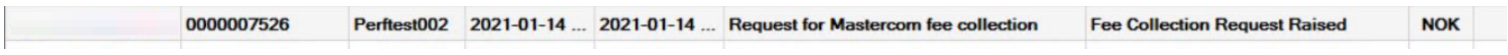


Figure 68: Mastercom Fee Collection screen

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

   Note: 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 Thredd support.

4. To close the message box, click **OK**.
5. The created fee collection message is displayed in the **Chargeback** screen.



Note: You can view details of any chargeback fees raised in the Fee Collection screen. See Viewing Fee Collections.

About Mastercom Fee Collection fields

The following table contains information about each of the fee collection fields.

Fee Collection Information	Description
Fee Collection Type	Select the type of fee collection. Options include: • 700 - Fee Collection • 780 - Fee Collection Return • 781 - Fee Collection Return Resubmission • 782 - Fee Collection Arbitration Return
Fee Collection Amount	Enter the fee collection amount. Up to two decimal places are allowed. Tick one of the following options to indicate who to credit the fee to: • Credit sender – fee will be credited to your account • Credit receiver – fee will be credited to the receiver.
Fee Collection Currency	Select the currency of the fee.
Fee Collection Reason	Select the reason for the fee collection (DE 25 Message Reason Code values that apply to the fee collection).
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.

Fee Collection Information	Description
Country	Select the country where the fee collection applies.

10.5.3 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** to display the **Fee Collection** screen.

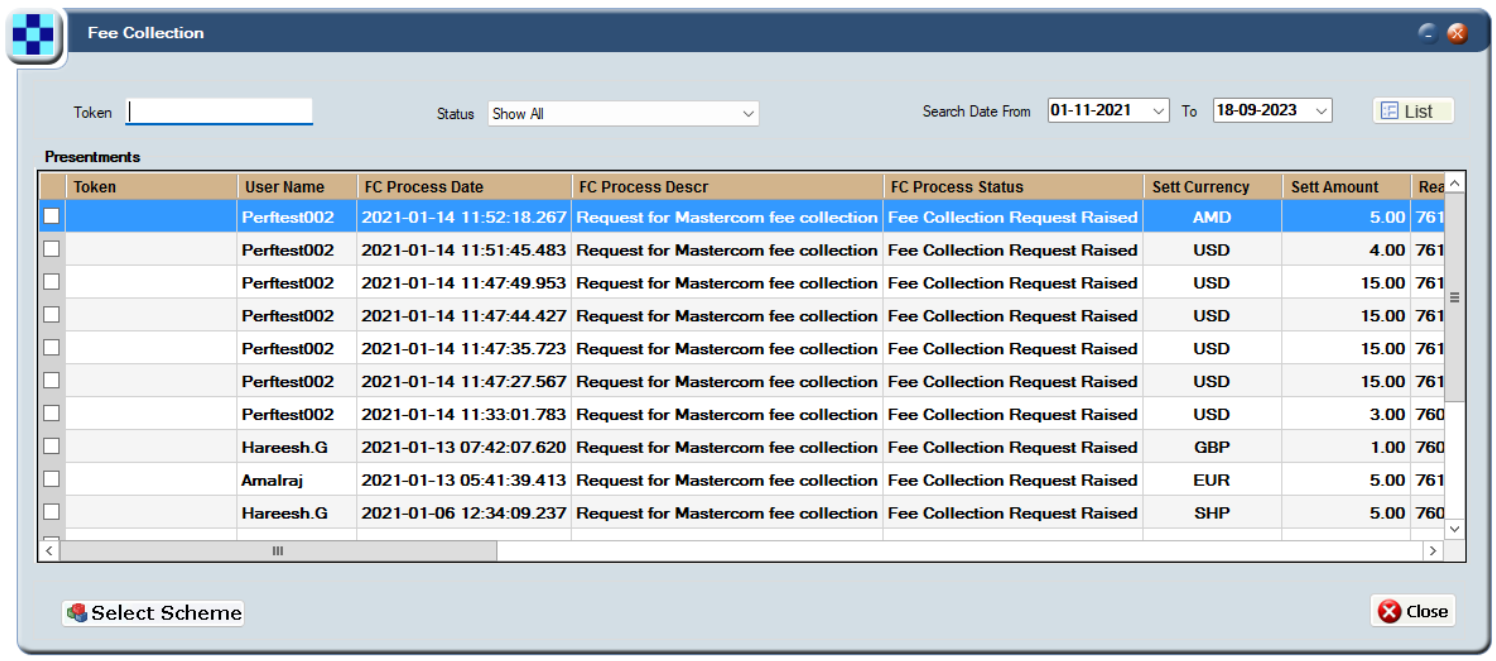


Figure 69: Fee Collection screen

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**.

10.6 Mastercom SAFE Reporting

10.6.1 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. From the Smart Client menu, select **Card Activity** > **View Transactions** to view the **Transactions** screen.
2. From the **Transactions** screen, right-click the required transaction and select **Create Mastercom SAFE report**. The Create Mastercom SAFE report screen is displayed.

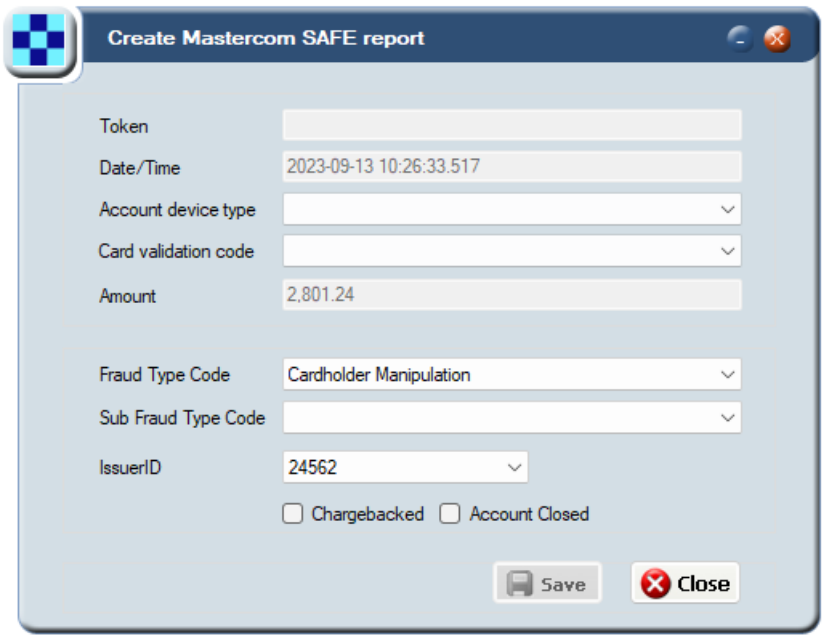


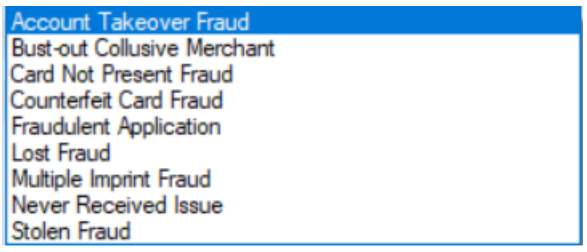
Figure 70: Create Mastercom SAFE report screen

3. Provide all the details as per the instructions in the table below and click **Save**.

   Note: 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 Thredd support.

4. To close the message box, click **OK**.
5. The created fee collection message is displayed in the **SAFE Report Details** Screen. See Viewing SAFE Report Details.

About Mastercom SAFE Report fields

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. 
Sub Fraud Type Code	Select a sub-fraud type code. Options include: • Convenience or Balance Transfer check transaction • PIN not used in transaction • PIN used in transaction • Unknown

SAFE Report Option	Description
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.

10.6.2 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, **Management Reports** > **Safe Report Details** to display the **Safe Report Details** screen.

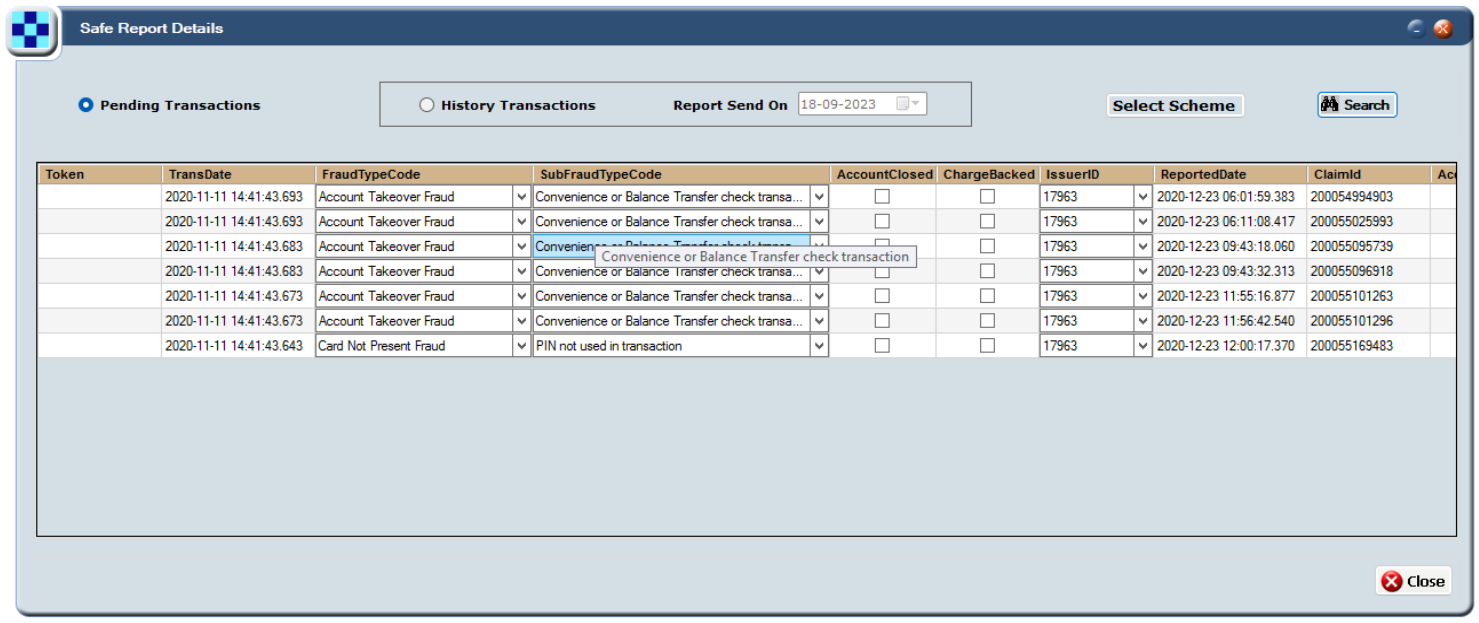


Figure 71: Safe Report Details screen

2. 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.
3. Click **Search**.

11 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.

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

11.1 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: Thredd do not currently support compliance case filings (pre-compliance and compliance). Thredd supports only pre-arbitration and arbitration case filings.

11.2 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 Thredd. 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.

11.2.1 Creating a Case in Smart Client

This section describes how to raise a case with Mastercard.

To create a Case in Smart Client:

1. From the Smart Client menu, select **Card Activity** > **View Transactions** to view the **Transactions** screen.
2. From the **View Transactions** screen, right click on the second presentment transaction.
3. Select **Actions** > **Create Case Filing**.

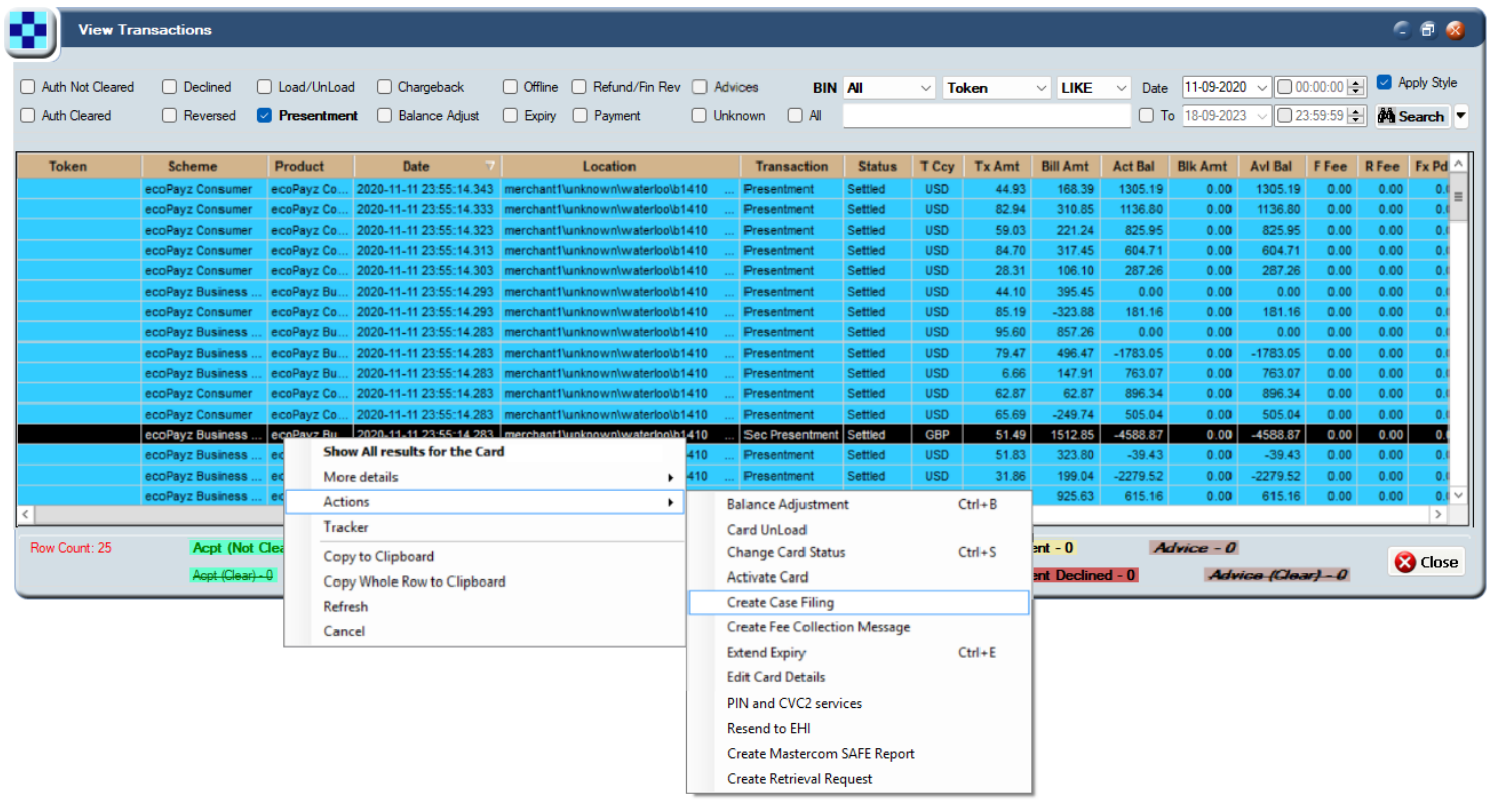


Figure 72: Create Case Filing menu option

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

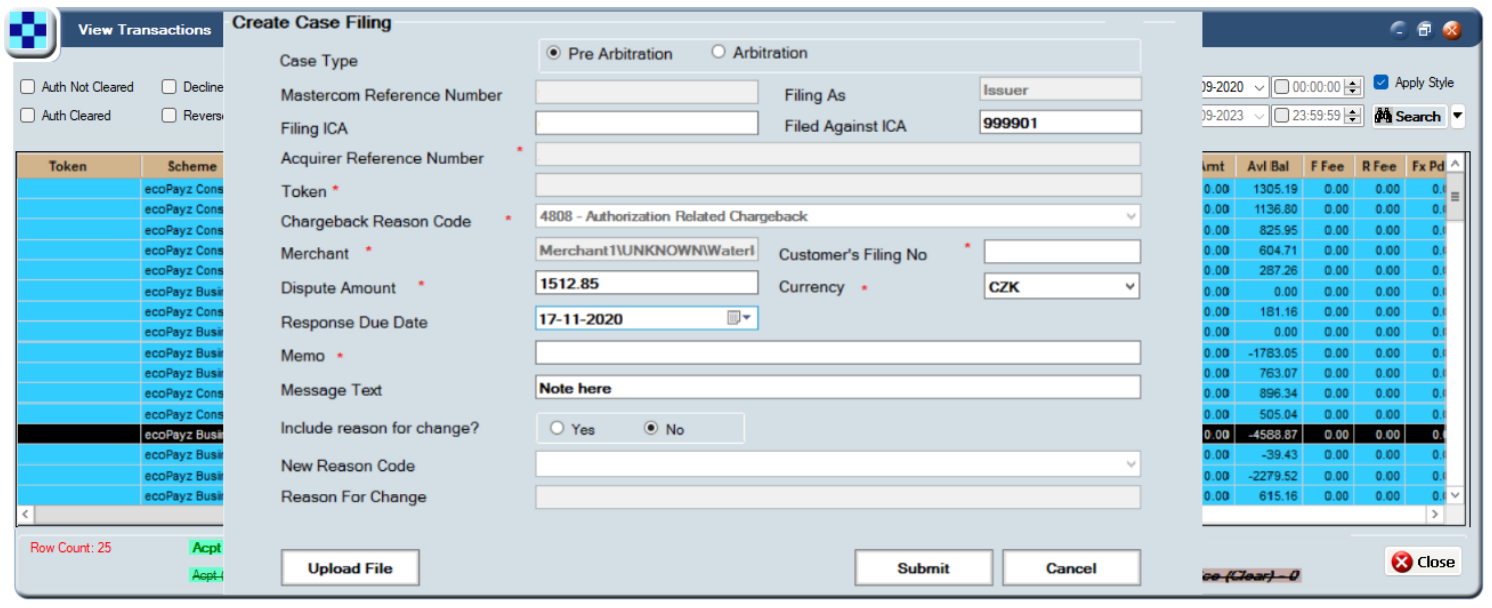


Figure 73: Create Case Filing Screen

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

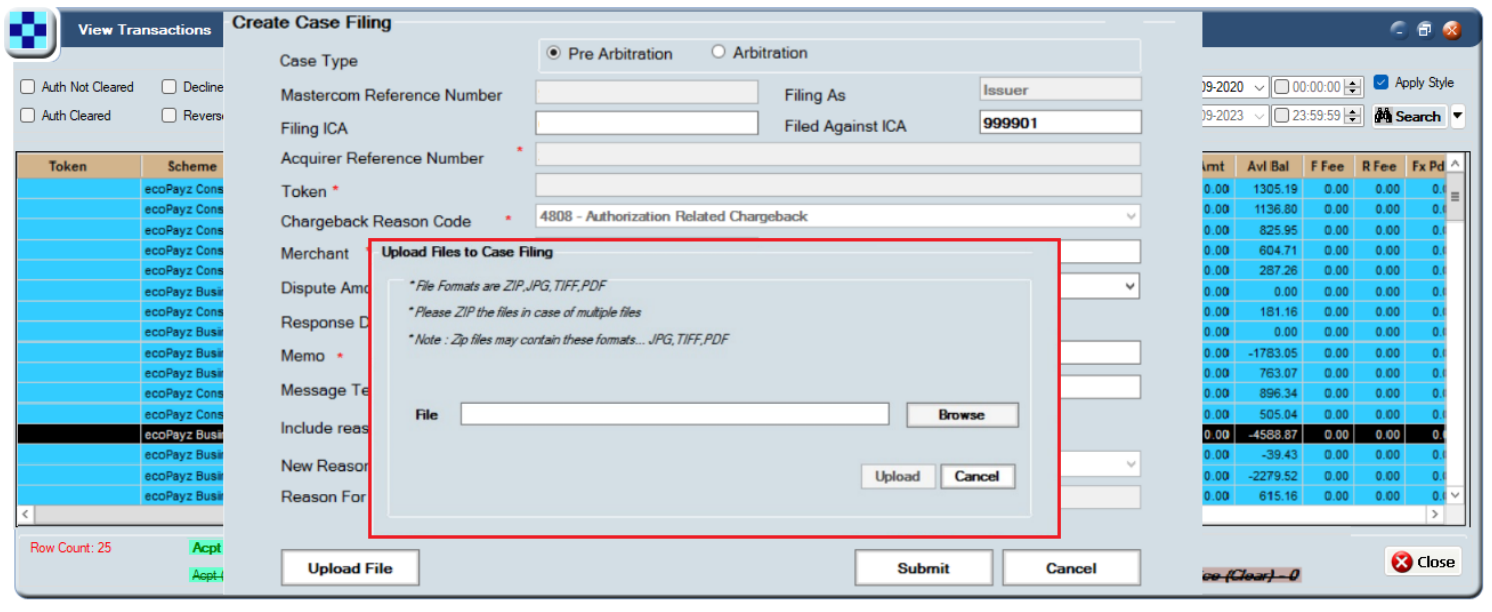


Figure 74: Upload Files to Case Filing Screen

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

11.2.2 Viewing Cases

To view cases using Smart Client:

1. Select **Card activity** > **Case Filing** to display the **Case Filing** screen.

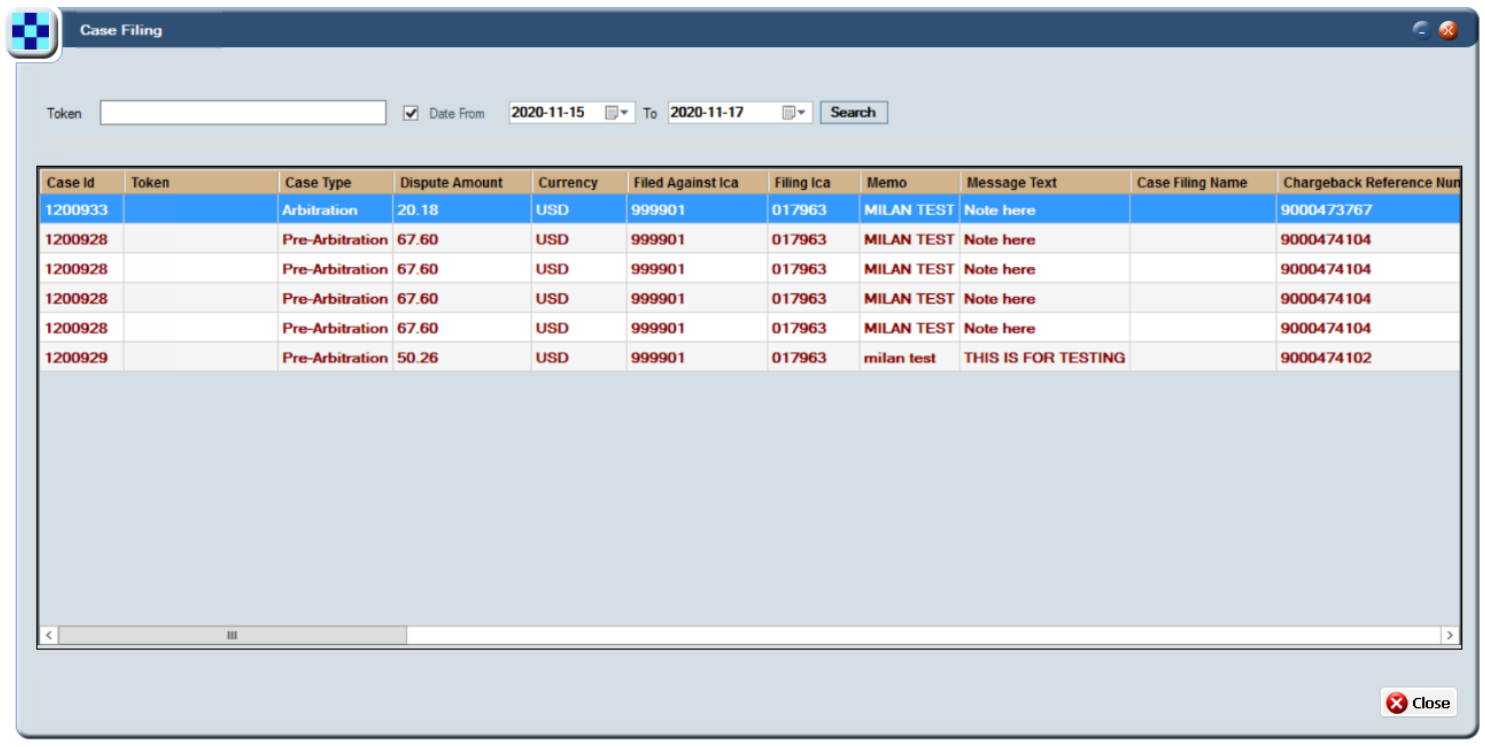


Figure 75: Case Filing Screen

11.2.3 Updating a Case

To update a case:

1. Select **Card activity** > **Case Filing** to display the **Case Filing** screen.
2. Right click a file and choose **Update Case Filing**. The following screen appears:

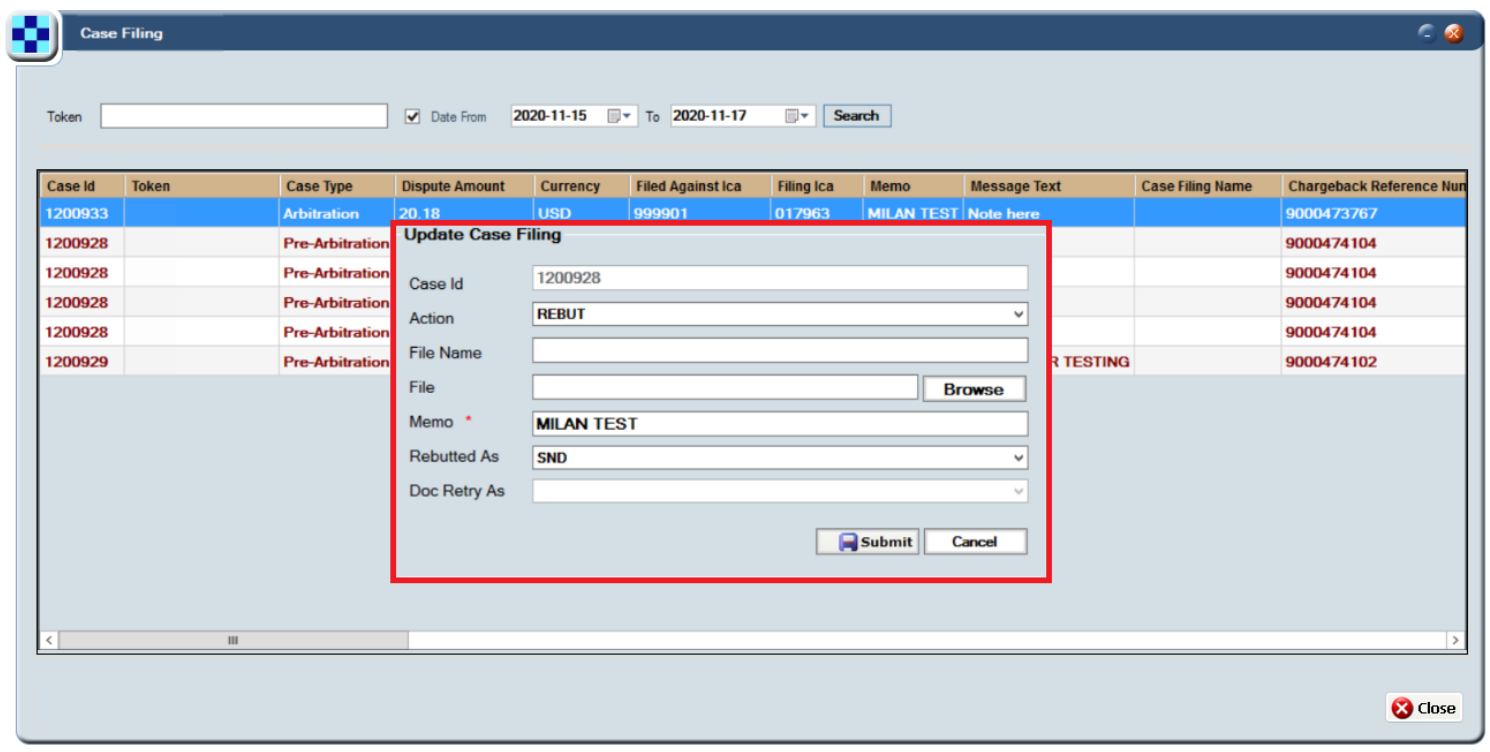


Figure 76: Update Case Filing Screen

3. Choose **Escalate**, **Withdraw**, **Rebut**, or **Doc_Retry**.
4. Select **Submit**.

11.2.4 Viewing the Status of a Case

To retrieve the status of a case:

1. Select **Card activity** > **Case Filing** to display the **Case Filing** screen.

   Right click a file and choose **Retrieve Case File Status**. A screen appears showing the status of the case:

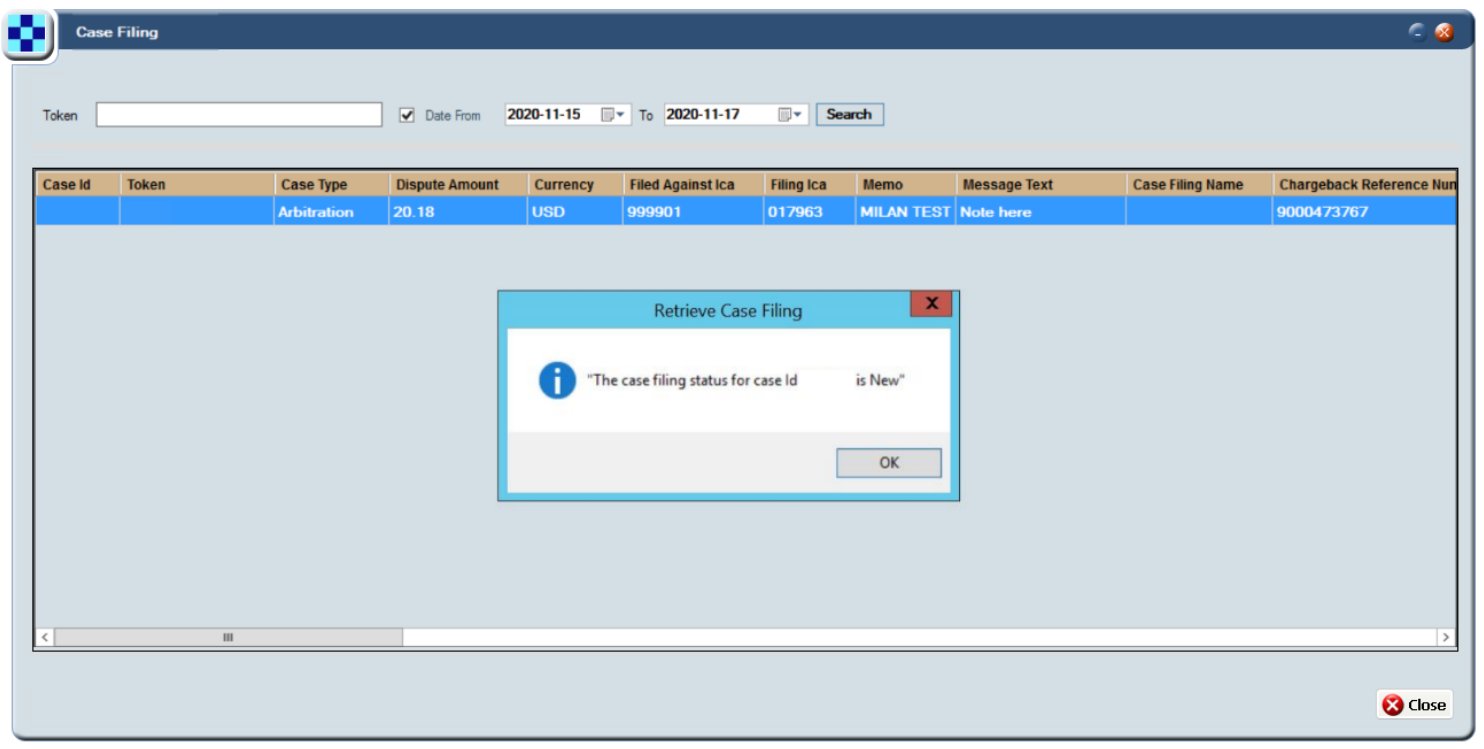


Figure 77: Retrieve Case Filing Screen

11.2.5 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 to display the Case Filing screen**.
2. Right click a file and choose **Download Case Filing file**.

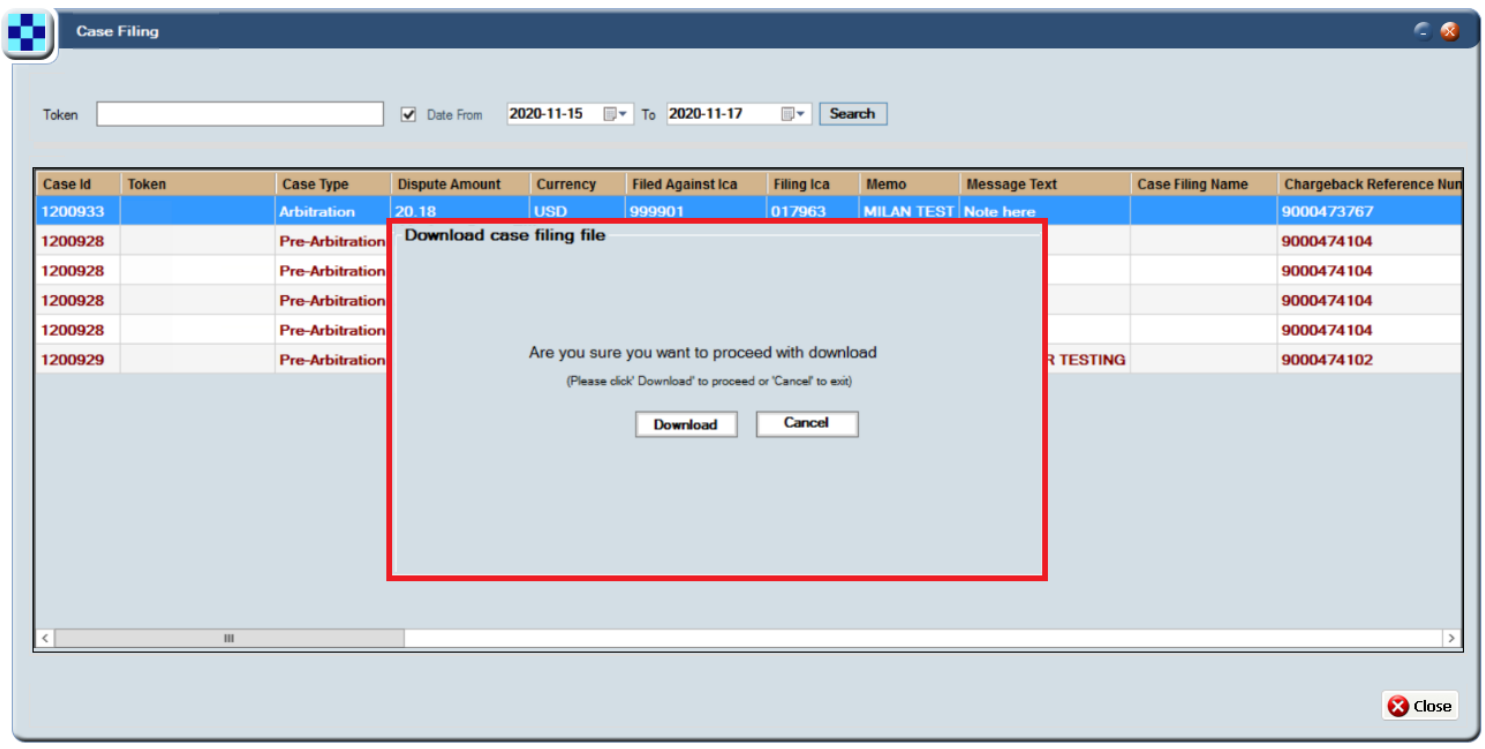


Figure 78: Download Case Filing File Screen

3. When prompted, confirm that you want to proceed with the download.

11.3 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.

11.4 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 Mastercard Fee section of the Transaction XML reports. For more information, see the Transaction XML Reporting Guide.

11.5 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 period as chargeback rules specify. Mastercom 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 period, 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, acts on the case or before Mastercom 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.

12 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 Thredd 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 Thredd 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.

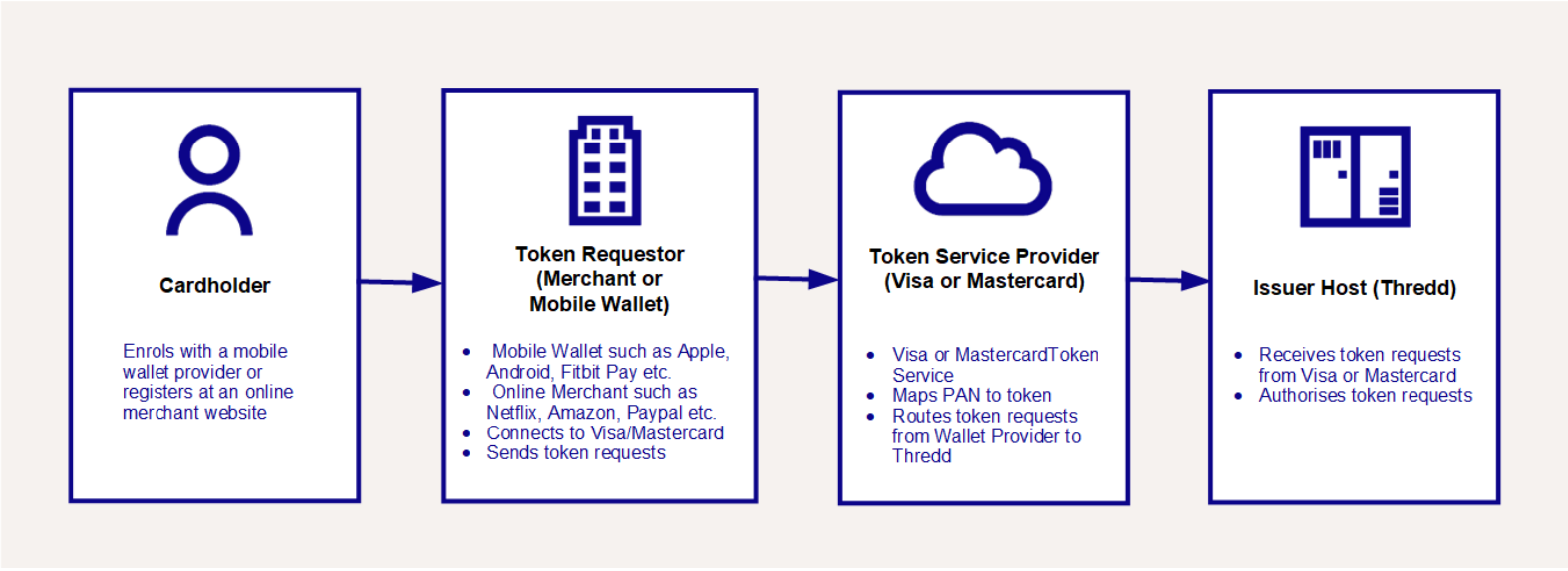


Figure 79: Parties involved in the MDES/VDEP tokenisation flow

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 (digital wallets), token provisioning and use cases, see the *Thredd Tokenisation Service Guide*.

12.1 Identifying MDES and VDEP-enabled Cards

To identify whether a card has any MDES/VDEP payment-tokens on it, see Viewing Payment Tokens.

To identify whether a transaction is on an MDES/VDEP payment token, see the device information in the bottom left of the **View Transaction Details** screen. See Locating Device Token Data

To identify a transaction from Visa/Mastercard used to create a new payment-token, see About the processing codes, and look for processing codes: “330000” (Tokenisation Authorisation Request), “340000” (Activation Code (to activate a new payment-token) Notification), and “350000” (Tokenisation Complete Notification).

12.2 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 *Thredd Tokenisation Service Guide*.

12.2.1 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*	*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*	*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**

Figure 80: Tokenisation Complete Notification ,Token Event Notification, and Token Authentication in the View Transactions screen

12.2.2 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	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

Figure 81: Debit (goods and services), Tokenisation Complete Notification , and Token Authentication in the View Transactions screen

12.2.3 About the processing codes

Token Authentication Request (TAR) – 330000

The Tokenisation Authentication Request (TAR) allows Thredd to provide a realtime decision as to whether the token service provider (MDES/VDEP) can digitize a card and designate a token on their behalf.

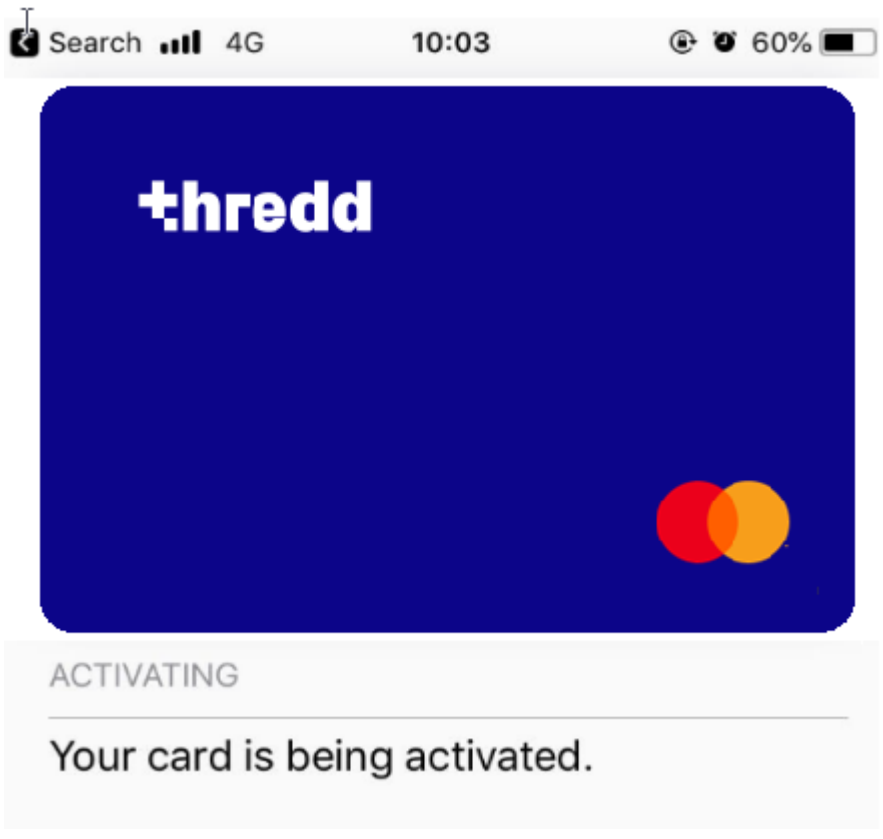


Figure 82: Card activation notification in realtime on a mobile device.

Authorisation	**Accepted**	**USD**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**Token Authentication**

Figure 83: Token Authentication in the View Transactions screen

Activation Code Notification (ACN) – 340000

This is received by Thredd from Mastercard and contains the Activation Code Notification (ACN) message. This signals Thredd 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 Thredd, 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	Activation Code Notification

Figure 84: Activation Code Notification in the View Transactions screen

Tokenisation Complete Notification (TCN) – 350000

This the final step in the digitisation process to confirm the setup of the token was successful.

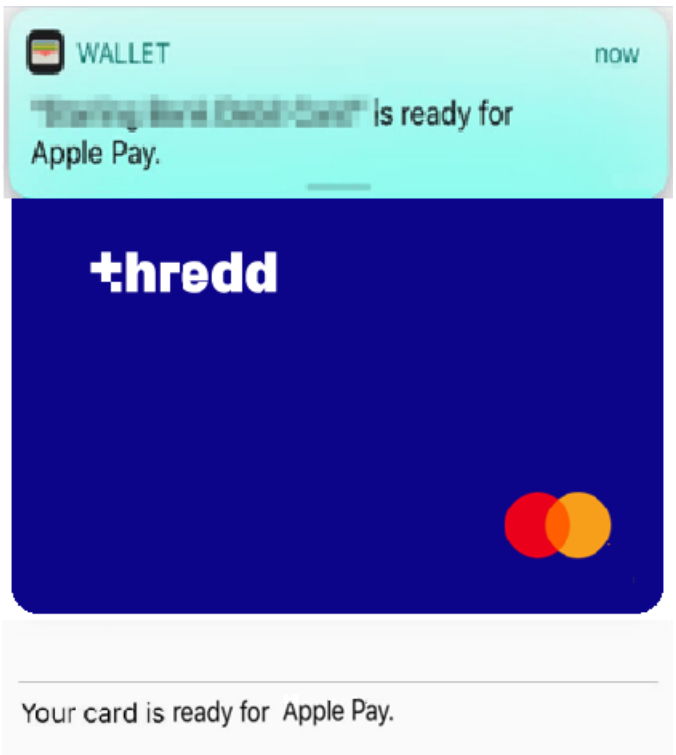


Figure 85: Card ready for use notification on a mobile device.

This message, constructed in a similar format to the previous MDES/VDEP messages, contains all the details of the tokenisation (digital wallets) 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

Figure 86: Tokenisation Complete Notification in the View Transactions screen

Token Event Notification (TEN) – 360000

This notification is 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 deactivated.

12.3 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 Thredd references as the `<Payment_Token>`.

12.3.1 Locating Device Token Data

To find information about the device token in Smart Client:

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

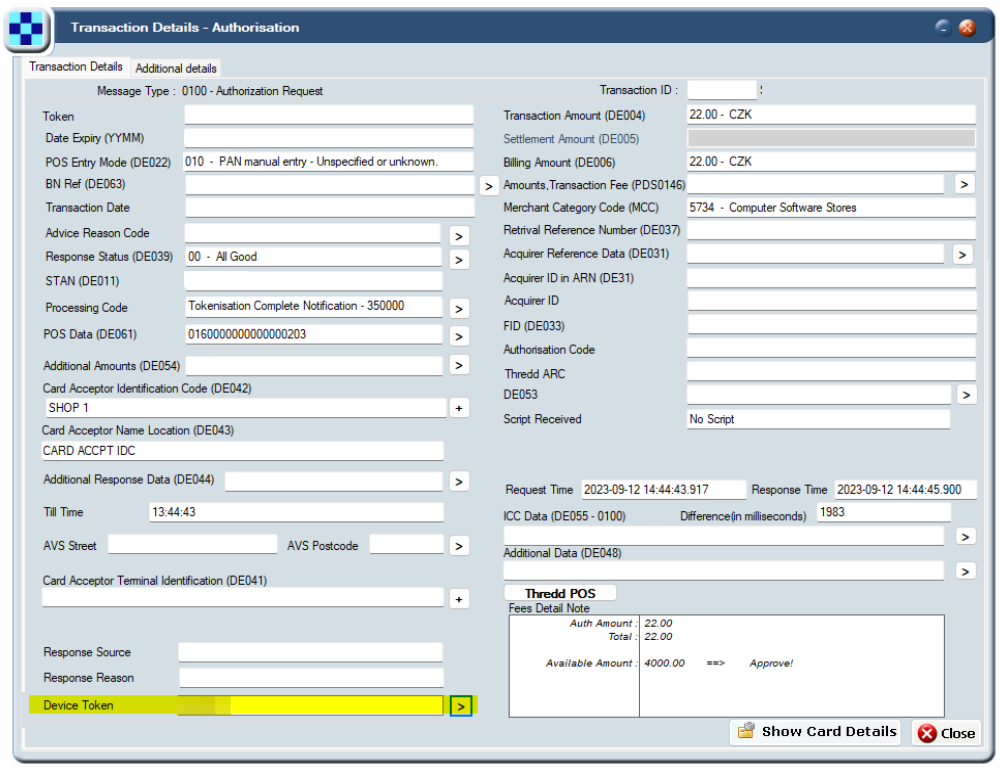


Figure 87: Device Token field on the View Transactions screen

3. 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 than 00 (All Good), the authorisation is declined.

12.3.2 Locating MDES/VDEP Device Status

Using Smart Client, 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**.
2. **Form Factor** shows the type of device being used for the wallet (for example, a mobile phone, tablet, or watch).
3. 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.

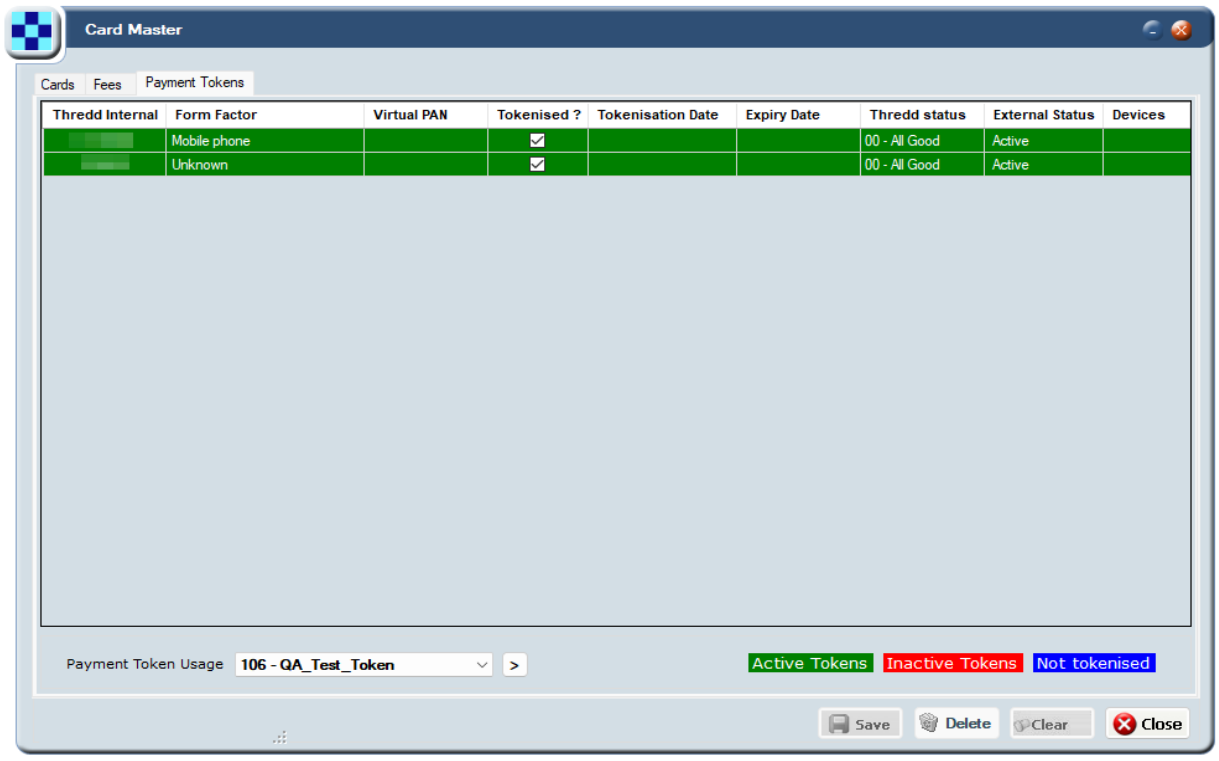


Figure 88: Device Tokens in the Card Master screen

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

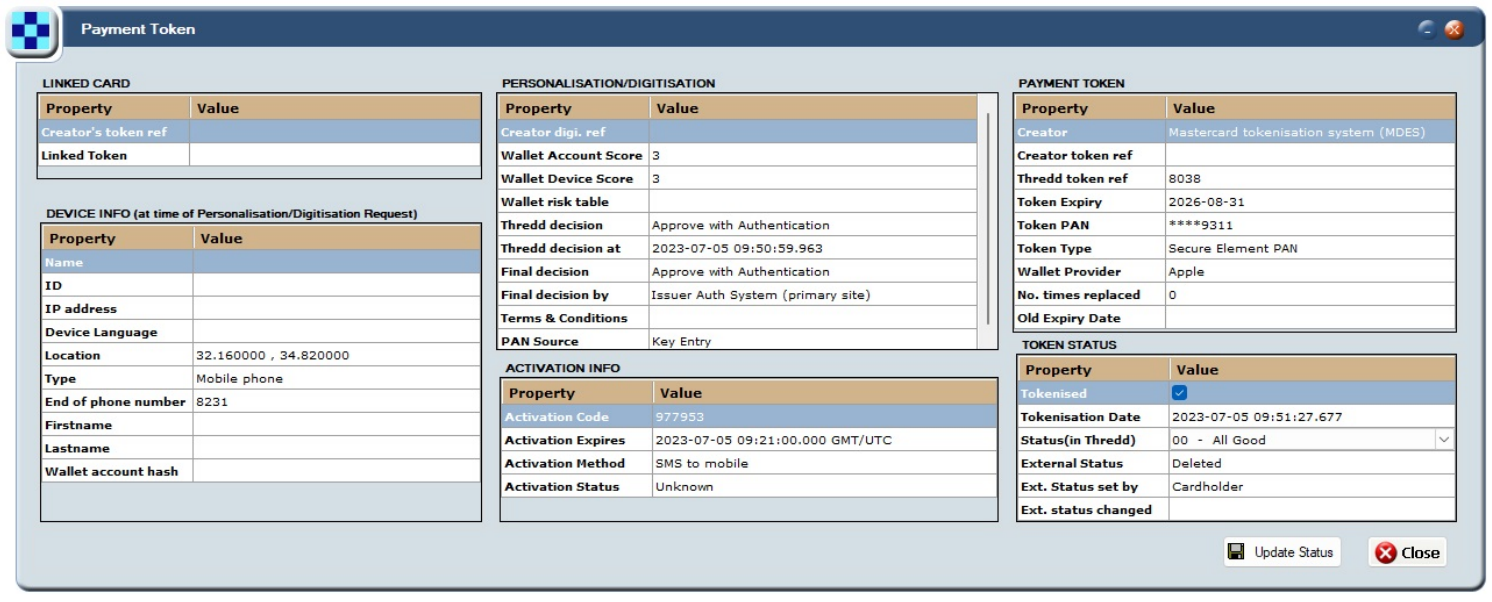


Figure 89: Payment Token screen

5. Update the token status if necessary.

12.4 MDES/VDEP EHI Considerations

MDES messages are also sent through the Thredd 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

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

12.5 Using MDES/VDEP API

Thredd offers a number of APIs relating to MDES/VDEP:

Using SOAP Web Services API	Using the REST-based Cards API
• Payment Token Status Change – use this to change the status of an MDES and VDEP Payment Token Card. • Payment Token Get – use this to get the details for MDES Payment Token Cards. **Note:** For more information, see the Web Services Guide.	• Update Payment Token Status – use this to change the status of an MDES and VDEP Payment Token Card. • Get Card Payment Token – use this to get the details for MDES Payment Token Cards. **Note:** For more information, see the Cards API Website.

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 Thredd system, the transaction will not show up in Smart Client. For example, if a cardholder is authenticated through 3D Secure checks 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 Thredd.

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 (payment network). 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 Thredd client portfolio, Thredd 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

- Thredd will not block merchant locations where there is a mix of fraudulent and valid transactions as this would impact legitimate cardholder transactions.
- Thredd 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.
- Thredd pro-actively completes an additional step 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 Thredd for fraud prevention outside of the normal processor remit.
- This block will apply across all Thredd client programmes.

Thredd recommends the use of Thredd's real-time Fraud Transaction Monitoring to help guard against fraud. Thredd can also offer 3D Secure using Adaptive Authentication which reduces friction in the transaction process versus traditional 3D Secure. For information about these products, contact your Thredd 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 the Thredd API: SOAP Web Services Card Change Status or Cards API Update Card Status. 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 Thredd 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 Thredd Smart Client and your Thredd 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 Thredd 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, email the Thredd Operations Command Centre at occ@thredd.com (operational 24 hours a day, 7 days a week).

Cannot log into Smart Client

- Solution 1: Check that your credentials are correct. Please raise a JIRA ticket or email the Thredd Operations Command Centre at occ@thredd.com.
- Solution 2: 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.
- Solution 1: Check that your credentials are correct. Please raise a JIRA ticket or email the Thredd Operations Command Centre at occ@thredd.com.
- Solution 2: Check that the application is connected securely to Thredd. See the Connecting to Thredd Guide.
- 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 will spot this in the View Cards screen where the address is blank, and the post code is 0 (zero). This indicates Thredd 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 the Thredd Web Services API 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 Thredd 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 Thredd 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 ecommerce 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	Thredd 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 [1]	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	YES

Status Code	Description	Who can set?	Functions permitted for the card	Functions blocked for the card	Example of use	Reversible
					card voided	
G1	Short-term debit block	PM	Credits	Auths (except credits)[2]	PM chooses this card status	YES
G2	Short-term full block	PM		Auths[2]	PM chooses this card status	YES
G3	Long-term debit block	PM	Credits	Auths (except credits)[3]	PM chooses this card status	YES
G4	Long-term full block	PM		Auths[3]	PM chooses this card status	YES
G5	Thredd Protect short-term debit block	Thredd Only	Credits	Auths (except credits)[2]	Thredd Protect sets this status based on various criteria	YES
G6	Thredd Protect short-term full block	Thredd Only		Auths[2]	Thredd Protect sets this status based on various criteria	YES
G7	Thredd Protect long-term debit block	Thredd Only	Credits	Auths (except credits)[3]	Thredd Protect sets this status based on various criteria	YES
G8	Thredd Protect long-term full block	Thredd Only		Auths[3]	Thredd Protect sets this status based on various criteria	YES
G9	Interactive Voice Response (IVR) Lost/Stolen Block (like 41 Lost)	IVR		Auths, Activation	Cardholder phoned the IVR automated phone line to block their card	YES

3.6

Note:

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. **Note:** For details, see: • Cards API Website (REST) • Web Services Guide (SOAP).
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. **Note:** For details, see: • Cards API Website (REST) • Web Services Guide (SOAP).
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 presentments.
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. 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	You can apply the specific “Card Usage Rules” which dictate card behaviour such as PAN entry method rules, cardholder verification, regional based rules, and transaction types. **Tip:** 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.
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	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: 1. DE42 – Merchant ID 2. DE43 – Address, text field for the merchant ID 3. DE61 – Postcode

Group Type	Purpose
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 Thredd.

Appendix D: Common Notes Field Values

Refer to the table below for details of common values in the **Notes** fields on the **View Transactions** screen. You can use this information to help you understand and troubleshoot.

Note	Description	Likely outcome of transaction	Action/ Troubleshooting
Accepted by EHI	Authorisation accepted by the external host.	Accepted	No action required.
Accepted by EHI Gen: Pre-Authorization Request	Pre-authorisation request accepted by the external host.	Accepted	No action required.
Accepted by EHI ASI card	ASI (Account Status Enquiry) authorisation accepted by the external host.	Accepted	No action required.
Accepted with load via EHI	Authorisation accepted by the external host with load.	Accepted	No action required.
ASI.... AVS check ASI card	Account Status Enquiry - Address verification system.	Usually accepted	No action required.
ASI.... CVC check ASI card	Account Status Enquiry - CVC (Card verification Code) check.	Usually accepted	No action required.
Auth Reversed on [Transaction Date]	The authorisation was reversed on a particular date.	Nothing changes on this transaction line.	Find reversal on the mentioned date and see notes field.
AUTOMATIC AUTHORISATION REMOVAL BillAmt - [Billed amount] Location - [transaction Location]	Authorisation has been reversed. Usually this note refers to the hanging authorisation filter.	Credits bill amount to available balance.	No action required.
BLACKLIST	This merchant (card acceptor id) is not allowed as per the card acceptor blacklist assigned to the card.	Always declined	Remove Card acceptor id from the blacklist via Smart Client or web services.
C01 - Person-to-Person	Type of credit authorisation that is person to person. These values are received in DE48 subelement 77 known as Transaction Type Identifier. Note that the values are discontinued.	Accepted or declined based on usage group rules.	Check usage group Rules.
C04 - Gaming Re-pay	Type of credit authorisation for gaming and gambling. These values are received in DE48 subelement 77	Accepted or declined based on usage group rules.	Check usage group Rules.

Note	Description	Likely outcome of transaction	Action/ Troubleshooting
	known as Transaction Type Identifier. For more details, refer to Mastercard's Customer Interface Specification.		
CardRequest.XML load by	Card Load performed by CRI file.	Accepted Load	No action required.
CB:Charged Back on CBC: Chargeback Credit confirmed on	This shows when a presentment is charged back.	Either an accepted Chargeback or rejection.	Check the Chargeback screen to show all Chargeback information.
Declined by Ext Auth	The authorisation was declined by the external host operating external authorisation.	Always declined	Check external host for decline reason.
Declined by EHI	The external host has declined the authorisation.	Always declined	Check decline reason on External Host.
DR: AF:Mag ATM attempt	Magnetic stripe used at an ATM. The hard-coded block is still applied to this product.	Always declined	To remove block, gain issuer sign off and raise a change request with Thredd via Jira.
DR: ARQC not matching	The ARQC (Authorization ReQuest Cryptogram) generated by the card does not equal the ARQC generated by Thredd.	Always declined	This can be due to issue with the Card manufacturer, network, Thredd, Terminal etc. If this is a recurring issue, please raise to Thredd.
DR: Auth Amount	The card does not have enough available funds for the authorisation.	Usually declined, unless the external Host overwrites and accepts the authorisation.	Load the card with the required amount. If enough Available funds please check the value of fees applied etc.
DR: Auth Amount Total : Available Amount : ==> Decline! Declined by Thredd Accepted with load by EHI	Authorisation declined by Thredd but accepted with load by EHI.	Accepted	No action required.
DR: AVS Failed because of: Address not Matching	Address verification system failure. The address sent to Thredd in the authorisation message does not match the address details held.	Usually declined. Thredd can configure to accept if AVS is wrong.	Ensure the cardholder is using the address registered in the 'Cardholder details' held under the card details on Smart Client.
DR: AVS Failed because of: House No not Matching	Address verification system failure. The house number of the address sent to Thredd in the authorisation	Usually declined. Thredd can configure to accept if AVS is wrong.	Ensure the cardholder is using the address registered in the 'Cardholder details' held under the card

Note	Description	Likely outcome of transaction	Action/ Troubleshooting
	message does not match the details held by Thredd.		details on Smart Client.
DR: Bad Retailer	This retailer has been blocked via the merchant blacklist.	Always declined	Merchant has been blocked for fraudulent behaviour. Contact Thredd for details.
DR: Card expiry check failed with Emboss Expiry date (DE014)	The expiry date sent to Thredd in the authorisation message does not match the expiry date held by Thredd (This is the embossed expiry of the card),	Always declined	Advise the cardholder to use embossed Expiry. If issue persists there could be an expiry misalignment, if so raise a Jira for Thredd Operations.
DR: Card Service Code check failed, Txn MSR Track 2 service code=xxx but Thredd service code=xxx Declined by Thredd	The service code in the track 2 data of the authorisation message does not match the service code held by Thredd.	Always declined	Validate transaction with cardholder as this can indicate a fraudulent card transaction attempt involving card skimming. If persists and is a valid transaction contact Thredd/merchant.
DR: Card usage group check…. Card Acceptance Method (A) - (Rule causing decline specified)	The POS (Point of Sale) entry mode used (DE22) is not allowed as per the card usage group assigned to the card.	Always declined	Change the usage group assigned to the card, gain issuer sign off and raise a change request to allow this Entry mode or tell the cardholder to use a different POS Entry mode.
DR: Card usage group check…. Transaction type (T)	The transaction type (processing code) is not allowed as per the card usage group assigned to the card.	Always declined	Change the usage group assigned to the card, gain issuer sign off and raise a change request to allow this transaction type.
DR: CAVV incorrect (checked by	The cardholder Authentication Verification Value was incorrect.	Always declined	Potential attempted Fraud as incorrect authentication value has been passed.
DR: CVC1 does not match	The CVC1 sent to Thredd Does not match what we hold.	Always declined	Potential fraud due to card skimming. Contact cardholder to confirm.
DR: Declined due to Expired card	The card is expired.	Always declined	Check if the card expired correctly as per the configuration detailed on the Product Set up Form.
DR: Declined due to Card Destroyed	Card status is set to 83 - destroyed.	Always declined	Order new card Via WS_Regenerate.

Note	Description	Likely outcome of transaction	Action/ Troubleshooting
(Original status 83, changed to 05)			
DR: Declined due to Do not honour	Card Status is set to 05 - to do not honour.	Always declined	Change status to 00 – All good or order new card.
DR: Declined due to Do not honour Declined by Thredd (EHI sent decline notification)	Card Status is set to 05 - to do not honour.	Always declined	Change status to 00 – All good or order new card.
DR: Declined due to GroupMCCCheck	The MCC (Merchant Category Code) passed in this authorisation is not allowed as per the MCC group assigned to the card.	Always declined	Remove this MCC from the MCC group or advise the cardholder to use a merchant with a different MCC.
DR: Declined due to Invalid card number (no such number) card not found	The Card number (PAN) passed in DE 2 is not recognized by Thredd.	Always declined	Either an accidental entry by the cardholder or attempted Fraud. No action required.
DR: Declined due to Limited network Check	This merchant is not included in the limited network assigned to the card.	Always declined	Advise the the cardholder to use the card within the allowed limited network.
DR: Declined due to Lost Card (Capture) (Original auth resp status 41, changed to 05)	Card Status is set to 41 – Lost card.	Always declined	Order new card via Webservices. (WS_ regenerate)
DR: Declined due to Restricted card (Card is not active)	This card has not been activated.	Always declined	Activate card via Smart Client, Webservices or phone/IVR line, (Activation methods available depend on the product set up).
DR: Declined due to technical fallback transactions	The transaction declines due to the phasing out of the magstripes.	Always declined	Advise the cardholder to use the chip/contactless.
DR: Declined due to voided card (Original auth resp status 99, changed to 05)	Card Status is set to 99 – Voided card.	Always declined	Change status to 00 – All good or order a new card.
DR: Emboss CVC2 not matching with CVC2 on PDS92	The CVC2 sent to Thredd in the authorisation message does not match the CVC2 held by Thredd.	Usually declined. Can be configured to accept for VISA if no CVC2 is provided.	Advise the cardholder to use embossed Expiry. If issue persists there could be an expiry misalignment, if so raise a Jira for Thredd Operations.
DR: Exceeds Max Per Transaction limit	The authorisation value (bill amount) is higher	Always Decline	Upgrade Card to a different Limit group, or

Note	Description	Likely outcome of transaction	Action/ Troubleshooting
	than the maximum per transaction limit in the Limit group assigned to the card.		wait until the limit group allows this to be completed (time dependent on the configuration.)
DR: Exceeds withdrawal amount limit	This authorisation would exceed the daily withdrawal limit as per the Limit group assigned to the card.	Always declined	Upgrade Card to a different Limit group or wait until the limit group allows this to be completed (time dependent on the configuration.)
DR: Exceeds withdrawal amount limit for the Accum period 1	This authorisation would exceed the accumulated period 1 withdrawal limit as per the Limit group assigned to the card.	Always declined	Upgrade Card to a different Limit group or wait until the limit group allows this to be completed (time dependent on the configuration.)
DR: Exceeds withdrawal amount limit for the Accum period 2	This authorisation would exceed the accumulated period 2 withdrawal limit as per the Limit group assigned to the card.	Always declined	Upgrade Card to a different Limit group or wait until the limit group allows this to be completed (time dependent on the configuration.)
DR: Exceeds withdrawal frequency limit	This authorisation would exceed the frequency limit as per the Limit group assigned to the card, , only 10 withdrawals are allowed per day.	Always declined	Upgrade Card to a different Limit group or wait until the limit group allows this to be completed (time dependent on the configuration.)
DR: Exceeds withdrawal frequency limit for the Accum period 1	This authorisation would exceed the accumulated period 1 frequency limit as per the Limit group assigned to the card, e.g. Only 10 withdrawals are allowed per week.	Always declined	Upgrade Card to a different Limit group or wait until the limit group allows this to be completed (time dependent on the configuration.)
DR: Incorrect Pin	PIN used by the cardholder does not match the PIN held by Thredd.	Always declined	Send PIN reminder to the cardholder. If the PIN is blocked, send a PIN block script and advise to use EMV capable Chip and ATM.
DR: Invalid Merchant	This merchant is not allowed as per the settings of the card. e.g., hard-coded AFD block or calendar group.	Always declined	Request Thredd to remove hardcoded AFD block – Issuer approval required via a change request/Jira. Advise the cardholder to use within the allowed time/date (calendar group.)
DR: ICVV does not match	The ICVV value sent to Thredd is Incorrect.	Always declined	This can be due to issue with the Card

Note	Description	Likely outcome of transaction	Action/ Troubleshooting
	ICVV is a card verification value stored/composed on the chip in EMV scenarios.		manufacturer, network, Thredd, terminal etc. If this is a recurring issue, please raise to Thredd.
DR: Invalid Use of Chip card in POS terminal, with no chip data	POS entry mode is Chip, but the card is not chip-capable.	Always declined	Potential Fraud - Contact cardholder to ensure that they still have the card, block and re-order card. Confirm in the transaction details that Entry mode is incorrect.
DR: Online Pin try limit exceeded	Online PIN is blocked due to too many incorrect entries. (3)	Always declined	Send a PIN unblock script to card. The Product Manager may decide to carry out cardholder verification and send a PIN reminder to the cardholder. Advise cardholder to use EMV capable chip and PIN for ATMs.
DR: Offline PIN try limit exceeded	Offline PIN is blocked due to too many incorrect entries. (3)	Always declined	Send a PIN unblock to the card. PM may decide to carry out cardholder verification and send PIN reminder to the cardholder. Advise cardholder to use EMV capable chip and PIN POS, or advise them to go to an ATM and unblock the PIN.
DR: Declined due to Security Violation	Card Status is set to 63 because of security violation.	Always declined	Change card status to 00 - All good.
DR: Decline due to Whitelist	This merchant (card acceptor id) is not allowed as per the card acceptor whitelist assigned to the card.	Always declined	Add card acceptor id to the whitelist via Smart Client or web services.
DR: Magstripe txn but no Track1 or Track2 data	An authorisation was received with magnetic strip as the Pan Entry mode but no Track 1 or 2 data was provided.	Always declined	Potential fraud due to card skimming. Contact cardholder to confirm and block card ASAP.
DR: Transaction not permitted to cardholder	The transaction is not permitted to the cardholder for a reason, e.g. calendar group.	Always declined	Check the groups assigned for the exact decline reason.
EH remote server unavailable	The remote server for the EH (External Host) returned an error: (503) Server unavailable.	If stand in ticked, Thredd approves/declines based on product config. If not ticked, it is declined (almost always declined).	Check the External Host for any issues. Contact Thredd.

Note	Description	Likely outcome of transaction	Action/ Troubleshooting
EH Timeout	EH (External Host) didn't responded in the agreed time (timeout happened).	If stand in ticked, Thredd approves/declines based on product config. If not ticked, it is declined (almost always declined).	Investigate why the External Host did not respond in time. Contact Thredd.
EHI DNS Error	The remote name could not be resolved.	If stand in ticked, Thredd approves/declines based on the product configuration. If not ticked, it is declined (almost always declined).	Investigate why the DNS name could not be resolved. Contact Thredd.
Empty/Invalid response code received from EH	The respond code received by Thredd from the External Host is invalid or absent.	If stand in ticked, Thredd approves/declines based on product config. If not ticked, it is declined (almost always declined).	Investigate why the response code was absent or invalid. Contact Thredd for assistance.
EMV ATC (0x0002) is not higher than last EMV transaction ATC (0x00C4) value	The application transaction counter is lower in this authorisation than it was in the previous.	Always declined	May indicate fraud. Confirm if the cardholder attempted the transaction. If not, block and reorder the card.
Fees	Fees applied to a card.	Shows as presentment line in Smart Client/sent to EHI.	Not applicable
FX Rate Applied : Client FX of [applied FX rate] dated, YY MMM YYYY HH:MM	An FX rate has been applied to this authorisation as provided to Thredd.	FX rate applied on amounts sent by MC. Usually accepted unless there is another reason for decline.	No action required.
GEN: Balance Transfer - Overnight Sweep of funds from Primary Card (123456789) to Secondary (987654321)	Funds transferred automatically overnight from secondary card to primary card.	Funds transferred to primary card.	No action required.
GEN: Multi Wallet Auto Transfer	Funds transferred to a multi-FX wallet automatically.	Transfer to fund wallet during authorisation.	No action required.
Gen: Pre-Authorization Request	A merchant has requested a ‘preauthorisation’. An authorisation for an estimated value.	Depends on other criteria, e.g. limits, EHI etc. Usually Accept.	No action required.
GEN: Secondary Card Balance Transfer	Funds transferred to a secondary card automatically.	Transfer to fund secondary card during authorisation.	No action required.
incorrect track 1 data (wrong cvv1)	The CVV1 in the track 1 data was incorrect.	Always declined	Potential fraud due to card skimming. Contact cardholder to confirm and block card ASAP.
incorrect track 1 data (wrong exp date)	The Expiry Date in the track 1 data was incorrect.	Always declined	Potential fraud due to card skimming. Contact cardholder to confirm and block card ASAP.

Note	Description	Likely outcome of transaction	Action/ Troubleshooting
incorrect track 1 data (wrong service code)	The Service Code in the track 1 data was incorrect.	Always declined	Potential fraud due to card skimming. Contact cardholder to confirm and block card ASAP.
LSR: Balance transferred from TOKEN 1 To TOKEN 2	Automatic transfer when replacement card ordered. (Only if new card Is regenerated with new PAN etc).	Balance transferred to new card.	No action required.
Neg Reversal due to AFD Advice with different amount. (AFD Amount=)	Reversal received from merchant with negative amount Increasing the blocked amount.	Accepted, increases blocked amount.	No Action required.
No response from EH Authorised by Thredd-Accepted	No response received from the External Host in authorisation process. Thredd STIP (Stand In Processing) has accepted this transaction.	Accepted	Check if the External Host is available, if this issue is affecting a high volume of transactions, raise with Thredd operations with the appropriate priority.
No Response from EH	The External Host did not respond within the configured limit. (May be unavailable).	Always declined. (If stand in is enabled, a different note will appear. (As in row above).	Check if the External Host is available, if this issue is affecting a high volume of transactions, raise with Thredd operations with the appropriate priority.
Recalculated-BillAmount=	Presentment received for authorisation where FX rate is applied. Billing amount is recalculated based on the FX rate.	Accepted(Presentment)	No action required.
Refund	Shows on a credit for refund financial message.	Accepted as it is a financial message.	No action required.
Reverse Authorisation for Auth on [Transaction date]	Reversal for an authorisation on a specified date.	Reverse authorisation, credit bill amount back to available balance.	No action required.
Reverse Authorisation for Auth on [Transaction date]Partial dispense by ATM (Misdispense) or POS partial reversal	Reversal for an authorisation on a specified date. This is due to an ATM error.	Reverse authorisation, credit bill amount back to available balance.	No action required.
Reverse Authorisation for Auth on [Transaction date] Issuer timeout Auth Reversed	Reversal for an authorisation on a specified date. This is due to an issue timeout.	Authorisation reversed	If volumes are high, contact Thredd.
Reverse Authorisation for Auth on 2017-07-28 13:22:35.703 No	Reversal for an authorisation on a specified date.	Authorisation reversed	No action required.

Note	Description	Likely outcome of transaction	Action/ Troubleshooting
confirmation from point of service			
Reverse Authorisation for Auth on [Transaction date] Transaction not completed	Reversal for an authorisation on a specified date.	Authorisation reversed	No action required.
Reverse Authorisation for Auth on [Transaction date] No confirmation from point of service	Reversal for an authorisation on a specified date.	Authorisation reversed	No action required.
Reverse Authorisation for Auth on [Transaction date] Banknet advice: APS error; unable to deliver response	Reversal for an authorisation on a specified date. This is due to a Banknet error preventing the response from reaching the merchant/acquirer.	Authorisation reversed.	If volumes are high, contact Thredd.
Root element is missing.	Incorrect response from the External Host.	Decline unless stand -in is enabled.	Investigate the EHI response for incorrect/missing tags.
System error	An error occurred while processing. Generic error code.	Always decline	If persistent, contact Thredd via Jira.
Visa repeat Message	Thredd has received a Visa Repeat 0101 message.	Authorisation accepted, declined, reversed. (Similar to 0100 message).	If persistent, contact Thredd, however, note this is not a Thredd issue.
DR: cannot find matching Base1 0100 TAR X-REQUEST-ID	The received tokenisation-related message, like TEN (Token Event Notification), is not linked to any TAR (Token Authorisation Request) in our system/TAR, which might have got archived.	Advice message only	No action required.
DR:MDES Thredd Status check failed Gen: Pre-Authorization Request	The underlying DPAN (Device Primary Account Number) status in our system is blocked.	Authorisation is declined	Change the status to All Good to further approve the DPAN transactions.
DR: Decline existing tokens(24) Min_ Tokens_To_Decline (15) DR: MDES/VDEP validation failed MDES check failed from Tokenisation Processing	The TAR (Token Authorisation Request) is declined whenever the permitted number of DPAN's (Device Primary Account Numbers) on a card would exceed if the TAR is approved or the number of assigned DPAN's on a card is already greater than the	TAR is declined	Delete one or more DPAN's to permit further tokenization on the card. Or increase the number of permitted DPAN's in Payment token group via change request.

Note	Description	Likely outcome of transaction	Action/ Troubleshooting
	permitted values.		
DR: Expiry Date missing	Blank expiry is not permitted in the authorisation as per the usage group config.	Auth is declined	Enable ‘Allow blank expiry date..” flag in the usage group.
DR: MDES Digitisation reference already exists Tokenization request associated with Orange Flow indicator is not permitted	When Thredd receive a TAR (Token Authorisation Request) with a Digitization reference (Correlation ID) which already exist in our database, our system will decline the TAR with reason stating "MDES Digitisation reference already exists MDES check failed from Tokenisation Processing". This is an expected behaviour.	TAR is declined	No action required.
Tokenization request associated with Orange Flow indicator is not permitted	TAR (Token Authorisation Request) was declined by Thredd because of the Orange flow indicator in the request based on the configuration.	TAR is declined	If the TAR needs to be challenged instead of decline, raise a change request to change this config in the Payment Token Usage Wallet.
DR: Decline due to missing CVV2DR: MDES/VDEP validation failed MDES check failed from Tokenisation Processing	TAR (Token Authorisation Request) was declined due to CVV missing in the request. The decline was as per the Card usage group.	TAR is declined	No action required.
DR: Wallet Provider Not Configured: ANDROID not in PAYMENT_TOKEN_ USAGE_WALLET for payment_token_ usage_id=119 MDES check failed from Tokenisation Processing	TAR (Token Authorisation Request) was declined because GooglePay/Android is not added to the Payment Token usage wallet group.	TAR is declined	Can add GooglePay/Android to the payment token usage group wallet via a change request. Similar declines could arise for Apple wallet as well if the respective wallet is not added to it.
DR: Decline as wallet recommended decline	In the TAR (Token Authorisation Request), the wallet recommendation was to decline the request. As per the Payment token config decision, Thredd declined TAR.	TAR is declined	No action required.
DR:MDES Decline - Wallet disabled for tokenisation MDES check failed from Tokenisation	If the Default Decision when a TAR (Token Authorisation Request) is received from a particular wallet is set to	TAR is declined	No action required.

Note	Description	Likely outcome of transaction	Action/ Troubleshooting
Processing	“Decline”, this is when this error is returned.		
DR: Invalid Wallet Provider: token_ requestor_ id=40010071298 not in Payment_token_ requestor_map	if the Token RequestorID is not added to the Payment_ token_requestor_map table at Thredd’s end, the TAR (Token Authorisation Request) will be declined.	TAR is declined	No action required.
DR:VDEP new DPAN received on unknown payment-token (no TAR)	This error is returned in the Notes field when we receive an Auth advice TEN (Token Event Notification) or Authorisation in which the DPAN (Device Primary Account Number) received is not found anywhere in the Thredd Database.		No action required.
DR: Decline as wallet_ account_score (1) = wallet_account_max_ score_decline(1) DR: MDES/VDEP validation failed MDES check failed from Tokenisation Processing	If the Device score or wallet score received in the TAR (Token Authorisation Request) is equal to or less than the value configured in that field, then TAR would be declined.	TAR is declined	No action required.
DR: IAV:V (checked by MC-PREVAL) Declined by Thredd	Authorisation was declined based on the On-behalf service result (DE48.71.05). An on-behalf service is one offered by the scheme where the issuer can optionally participate, e.g., Cryptogram validation service, Mastercard AAV Checks etc. For more details, refer to Mastercard's Customer Interface Specification.	Authorisation is declined	No action required.
DR: Requires SCA	Based on the Product’s SCA configuration, the authorisation was declined due to additional authentication required/No SCA exemption is applicable/ transaction performed against SCA guidelines like PAN manual entry where the cardholder is present etc.	Authorisation is declined	No action required.
PSD2 Counter Reset ...	Either the transaction went was authenticated	This is just an informational message and is not a reason of decline.	No action required.

Note	Description	Likely outcome of transaction	Action/ Troubleshooting
	using PIN or 3DS which reset the SCA counters.		
Unable to locate bound device 0 ...	The device ID in the transaction is not found anywhere in the DB.	This is just an informational message and is not a reason of decline.	No action required.
Refund matching credit auth	When a refund presentment is matched to its respective Refund Auth.	Informational message	No action required.
Declined by Fraud Advantage Gen: Pre-Authorization Request Declined by Thredd	When the Authorisation is declined by the Featurespace/Fraud Advantage service.	Authorisation is declined	No action required.
DR: MDES Invalid Card Number - payment_token not found Declined by Thredd	When we receive a payment token transaction from a DPAN (Device Primary Account Number) which is not assigned on that card, the above error is returned.	Authorisation is declined	No action required.
DR: Invalid Country Declined by Thredd	The country from which the authorisation originated is blocked by Thredd on that product/scheme.	Authorisation is declined	No action required.
DR: Japan-Restricted Payment mode	When F118 is received, Thredd will only approve transactions with F118.8 = 10 (one-time payment) and decline everything with note: 'DR: Japan-Restricted Payment mode' that has a value different to 10. The F118 field is used in Japan (as well as other specific countries) by acquirers to share payment modes.	Authorisation is declined	No action required.

Glossary

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

#

3D Secure (3DS)

: 3D Secure is a technical standard adding an extra layer of security to payment 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 cardholders.

Act Bal

: Actual Balance

AFD

: Automated Fuel Dispenser

AID

: Acquiring Institution Identification Code

API

: Application Programming Interface

APW

: Mastercard Automated Parameter Worksheet

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, Visa or Discover, 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.

CIQ

Visa Client Implementation Questionnaire

Clearing File/Clearing Transaction

Thredd 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

DGN

Discover Global Network, which consists of Discover, Diners Club International, and Pulse.

Discover (DGN)

Discover Global Network, which consists of Discover, Diners Club International, and Pulse.

DPAN

Device Primary Account Number

E

EHI

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 Thredd sends real-time transaction-related data. The URL to this system is configured within Thredd 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 Thredd 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

H

Hanging authorisation filter

The period of time during which Thredd waits for an approved authorisation amount to be settled. This is defined at a Thredd product level. A typical default is 7 days for an auth and 10 days for a pre-auth. For more information, see the External Host Interface Guide.

I

Issuer (BIN Sponsor)

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

M

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 identity the type of account provided to them by their acquirer.

MFX

Multi-Currency Card

MultiFX

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

MVC

Master Virtual Card

O

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

P

PAN

Primary Account Number

PM

Program Manager

POS

Point of Sale

POSFX

A Thredd 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 Thredd 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)

Secure Connectivity Framework

Thredd's Secure Connectivity Framework is the combination of several components which enable secure access to Thredd's resources, using a common identity store.

Smart Client

Smart Client is Thredd's user interface for managing your account on the Thredd Platform. Smart Client is installed as a desktop application and requires a secure connection to Thredd systems in order to be able to access your account.

STAN

System Trace Audit Number

Stand In Processing (STIP)

The card network may perform approve or decline a transaction authorisation request on behalf of the card issuer. Depending on your Thredd mode, Thredd 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

VROL System

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

Document History

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

Version	Date	Description	Revised by
3.6	28/01/2026	Added non-mTLS URL for Smart Client under System Requirements. See Installing Smart Client.	KD
	10/07/2025	Added mTLS environment links to System Requirements. See Installing Smart Client.	JB
	22/05/2025	Added a note to indicate that card status changes prior to 2022 are no longer retrievable. See Searching for a Card.	KD
	15/05/2025	Added Appendix on Notes field values. See Appendix D: Common Notes Field Values.	KD
	27/03/2025	Added reference to Connecting to Thredd guide for the Secure Connectivity Framework.	KD
	27/02/2025	Added section on entering OTP codes for Multi-Factor Authentication when logging in to Smart Client. See Getting Started with Smart Client.	JB
	27/01/2025	Clarified which fields are used in the Thredd API to populate the *Card Purchaser* field details in Smart Client. See Viewing Card Details.	WS
	13/09/2024	Removed references to VPN.	WS
	29/07/2024	Added references to Cards API Website (REST). See Viewing Card Details and Appendix C: Usage Groups.	PC
	02/07/2024	Updated the company address.	PC
3.5	18/04/2024	Updates to content to align with taxonomy updates on our Documentation Portal.	WS
	26/02/2024	Added Network field to Transaction Details page and added reference to new transaction types. See Viewing Transaction Details and Searching for a Transaction.	JB
	31/01/2024	Updated the list of prerequisite software required before installing Smart Client. See Installing Smart Client.	WS
	03/01/2024	Added Smart Client download links to PRD1 and PRD2 environments. See Installing Smart Client.	JB
	31/10/2023	Editorial review of content including the re-branding of all screen shots.	JB
3.4	13/10/2023	Removed references to creating multiple chargebacks from Managing Chargebacks.	JB
	11/09/2023	Added details of the new **Fetch 3DS Credentials** button, available on the Card Master screen. See Viewing Card Details.	WS
3.3	13/06/2023	Removed Viewing Foreign Exchange (FX) Transactions topic; the CurrrencyCloud solution has been withdrawn.	MW
	08/06/2023	Updated Operations email address to be occ@thredd.com	MW

Version	Date	Description	Revised by
	27/04/2023	Rebranded PDF and HTML versions now available	MW
3.2	18/04/2023	Added a new table describing permissions to the section About Roles and Permissions.	WS
	23/12/2022	Replaced the screenshot in Editing Card Details to show additional fields like 'Country' 'City' and 'DOB'. Replaced the screenshot in Locating MDES/VDEP Device Status to show additional 'PAN Source' field.	MW
	01/12/2022	Updated Copyright Statement.	
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 Finding MDES/VDEP Data on Smart Client. Added additional Card Status Codes to the appendix. Added Case Filing 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: • Removed 'Unload' from Status Code 63 • 3D Secure CAVV result • MDES/VDEP updates • Chargeback Updates	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.

Thredd UK Ltd.

Company registration number 09926803

Support Email: occ@thredd.com

Telephone: +44 (0) 203 740 9682

Our Head Office

Kingsbourne House

229-231 High Holborn

London

WC1V 7DA

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@thredd.com.