Cross Border Services Guide

Version: 1.0

29 May 2025

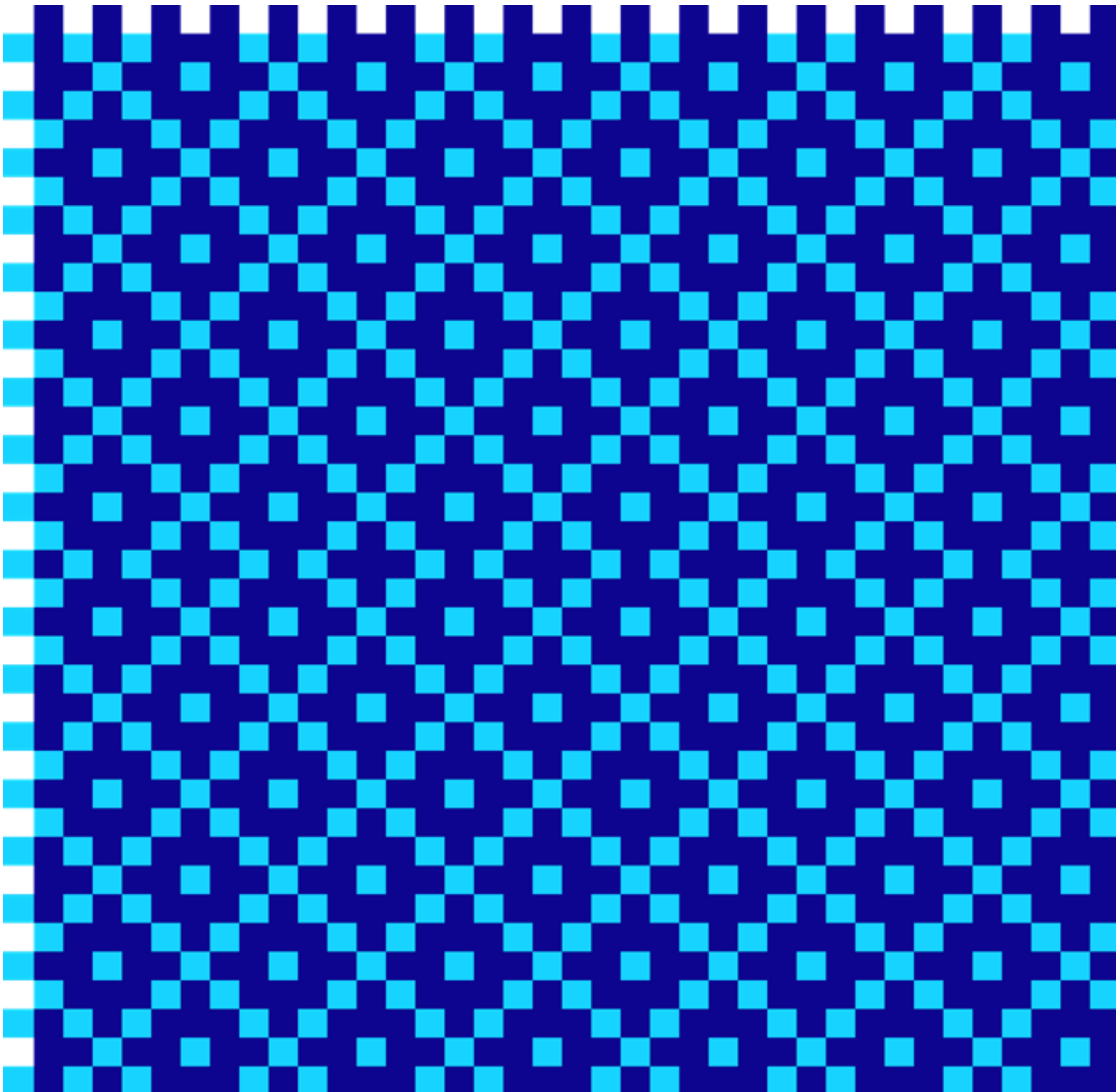
Publication number: CBS-1.0-5/29/2025

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 Guide

This guide is intended as a reference guide, to provide information on Cross Border Services.

What's changed?

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

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

Introduction

IMPORTANT: This document is intended for project sizing and client understanding of the intended development for the Thredd Cross Border pilot service. The pilot service is subject to contract between Thredd and the Client. You must sign a pilot addendum before Thredd can provide the service.

This is a draft implementation guide for Cross Border Services v0.1. It is intended for client's determination of the resource effort and is subject to change upon finalisation of the solution. This guide should be used for project sizing only. It must not be used for any service mapping or development as it is not the final launch implementation guide.

Note: Some links reference example “sandbox” sites that are not ready for developers to use or access.

Cross Border Payments (Also known as Push Transactions) enables you to complete a cross-border push transaction using the Mastercard Cross Border service, which is part of Mastercard Move service.

Most banks that provide cross-border payments currently rely on corresponding banks, which is unreliable, slow, and expensive, especially for niche markets and currencies. Most banks avoid providing this service to their customers due to the high cost. Using Thredd's Cross Border service, you can process the transfer through the Mastercard network, allowing cardholders or account holders to create cross-border payments and send to a “receiver” of the funds using a single connection. This is cost-effective and reliable, and dramatically reduces development costs as Thredd develops a majority of the connectors on behalf of our Originating Institutions.

Thredd has embedded the Mastercard Cross Border APIs into our platform, exposing a simpler set of APIs for you to use. This enables your cardholders to initiate a payment request or create a cross-border payment and send it to a “receiver” of the funds. The payments use cases include:

- Person-to-Person (P2P)
- Business-to-Business (B2B)
- Business-to-Consumer (B2C)
- Business-to-Person (B2P)
- Account-to-Account (A2A)
- Card- to-Card
- Mobile wallet open loop payments

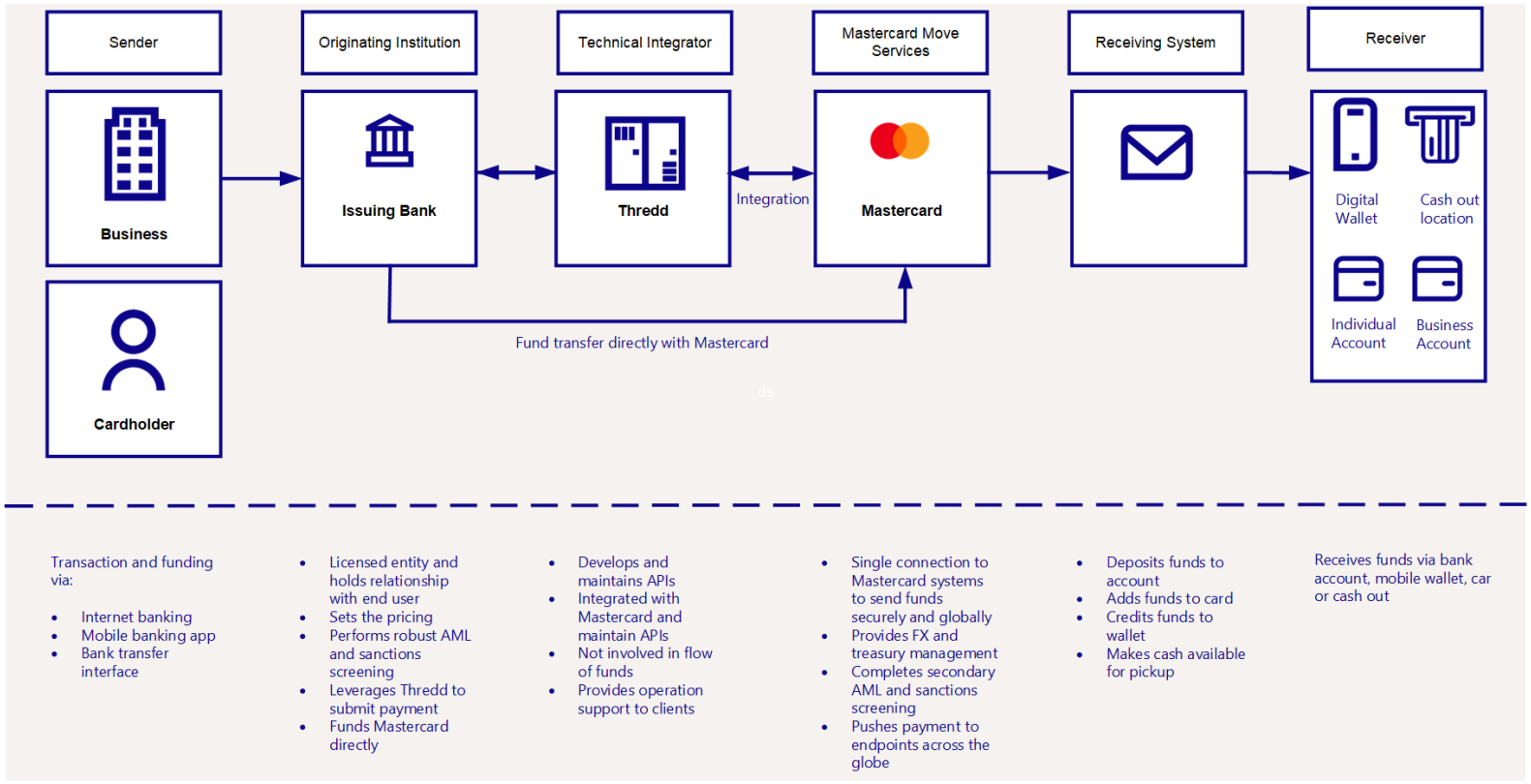
Benefits of using the Cross Border Service

- Reduce your development time by up to 12 months.
- Thredd will continue to add value by making sure the Thredd platform complies with the relevant mandates.

  Note: In some instances where there are regulated changes impacting the User Interface or a need to capture different information by region, there may still be changes required for clients and the relevant applications.
- When using money movement, each new connector will be easy to access when you have integrated to our orchestration layer. Once integrated using the new Thredd Portal, resellers will be able to manage their portfolio and risk settings in Thredd.

Basic Payment Flow

In Cross Border, the disburser (or sender) of the funds logs on, and from their bank or digital application or account, initiates a payment instruction to send a value to a "recipient". For example, a remittance payment request. This flows to the Originating Institution, to Thredd and then to Mastercard for initiation to the recipient bank network.



Use Cases

- **Urgent Bill Payments**: Ideal for both Business-to-Business (B2B) vendor and supplier payments, as well as account holder bill payments.
- **Deposits**: Merchant account transfer payment used to add money from services such as gig workers, content creators providers account or card.
- **Payroll**: Perfect for same-day payroll for hourly and temporary workers, or for make-up payments, error correction, and missed deadlines (emergency payroll).
- **Insurance Claims and Disaster Assistance**: Ensures timely disbursement of funds.
- **Refunds and Reimbursements**: Provides quick refunds and other reimbursements.
- **Account Transfers**: Facilitates same-day transfers between accounts (A2A).
- **Tax Payments**: Simplifies and speeds up tax payments.
- **Merchant Settlement**: Streamlines merchant settlements.
- **Cash Concentration**: Enhances cash management.
- **Pay another individual**: Paying someone back for money borrowed or to split bill.
- **Send money from one bank account to another (A2A or P2P)**: where both accounts belong to the same person. This is used frequently in smart budgeting and saving applications (Pooling accounts).
- **One-off bill payments**: Manual bank transfers to pay for one-off services, such as car repairs or for paying a trades-person.
- **Business payments**: Account-to-account payments for paying one off business invoices.
- **E-commerce payments**: While card payments are more commonly used for e-commerce payments, instant bank transfers (powered by open banking) are increasingly appearing as part of the online checkout process, as a lower-cost alternative.

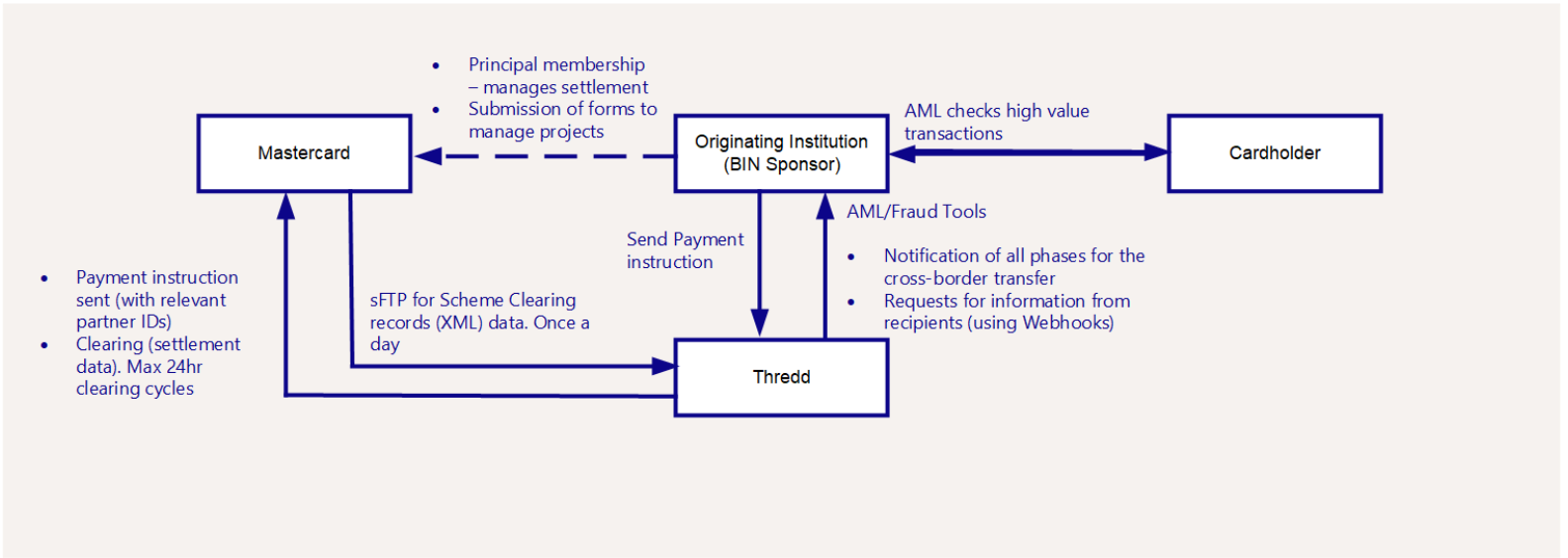
Supported Business Models

This section details the business models that are supported for the Cross Border service.

Standard Model

The standard model enables the Originating Institution to offer services directly to the end user (people or business).

The following diagram displays the roles and responsibilities of the standard model. In this model the client only provides cross border to their cardholders.



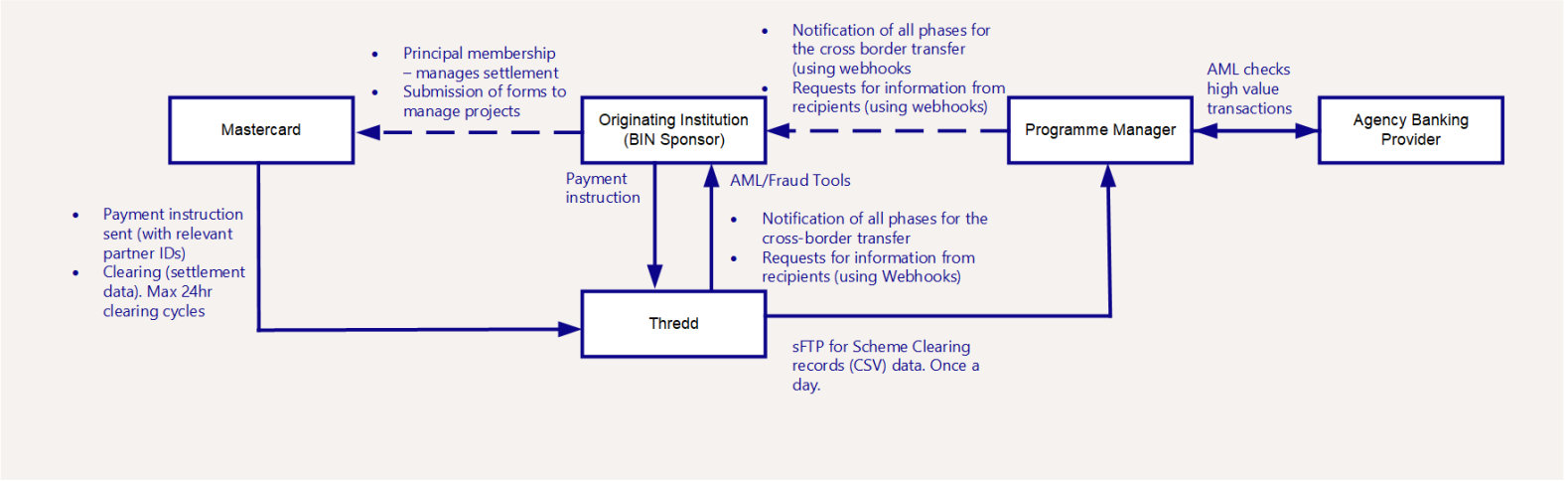
The following table describes the rules and responsibilities of the above.

Function	Roles and responsibilities
Mastercard	• Network between sending and receiving institutions • Clearing cycles (settlement data) in XML • Setting up sender configuration (per corridor) • Each originating institute must hold a participation agreement with Mastercard
BIN Sponsor	• Must have a regulated entity money transfer licence • Signs a Mastercard Participation Agreement, or has an ICA (for billing and settlement) assigned, before opening a Mastercard project • Signs Thredd addendum for Cross Border Services • Holds the risk when clients are onboarded • Must have a sufficiently funded account to manage settlement. Failure to have this will result in the transfer failing • Ensures compliance with Scheme mandates and regulator requirements for transfers • Runs Anti-Money Laundering (AML) checks for high value transfers threshold set by regulators • Holds unique the Client or Partner ID assigned by Mastercard, which is passed in the transfer message.
Thredd	• Amazon Web Services (AWS) cloud service using Thredd Portal for reporting if the originating institute decides they want reporting. • APIs consumed by the originating institute. • Thredd Portal interface for Customer Support and Operations. • Holds unique Client or Partner ID assigned by Mastercard, which is passed in the transfer message. • Provides connectivity, API development, data requirements per Mastercard specification, error code management, report and file transfer mechanisms
Cardholder	• Using either Thredd's new service or the bank's existing service, cardholder completes Know Your Customer (KYC) checks when opening the account with their bank • Holds an account with the originating institution • Has relevant funds to initiate the payment instruction

Reseller Model

The reseller model is for originating institutions that are authorised to include cross border services to their offerings of their own branded payment services to their program managers.

The following diagram displays the roles and responsibilities of the reseller model, where program managers or agencies resell services to their card or account holders.



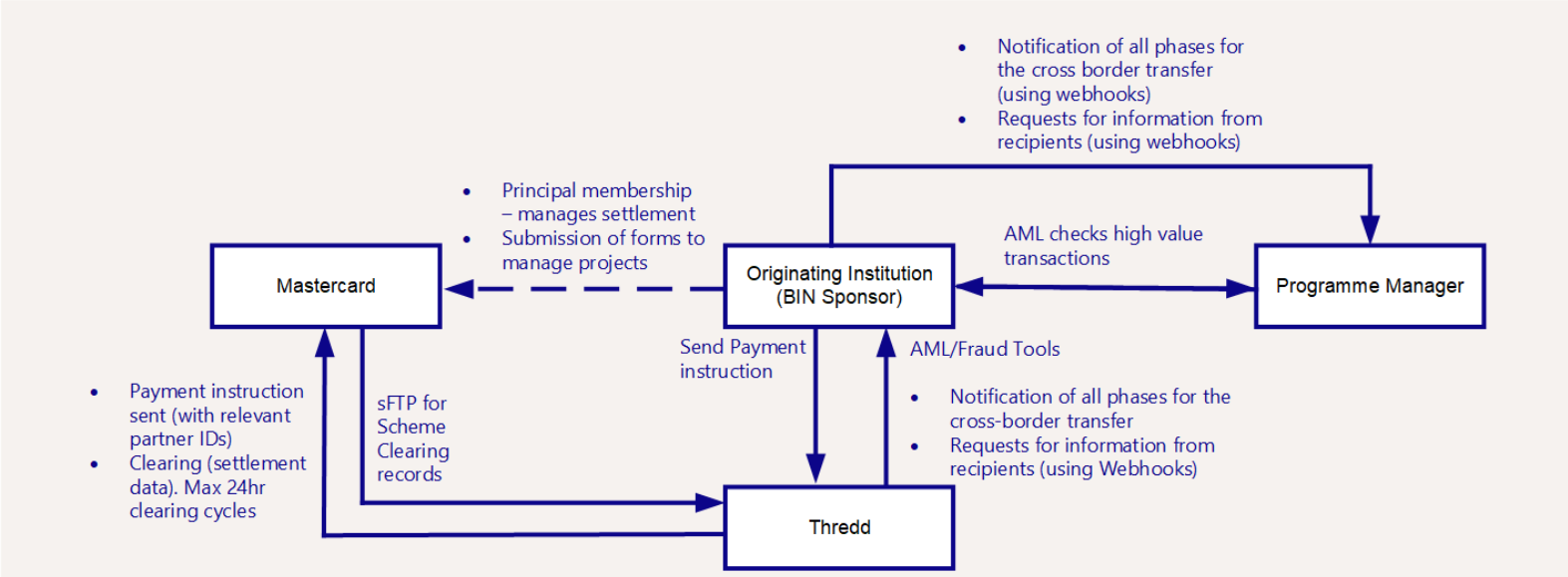
The following table describes the rules and responsibilities of the above.

Function	Roles and responsibilities
Mastercard	• Network between sending and receiving institutions • Clearing cycles (settlement data) in XML • Setting up sender configuration (per corridor) • Each originating institute must hold a participation agreement with Mastercard
BIN Sponsor	• Must have a Regulated entity money transfer licence • Signs a Mastercard Participation Agreement, or gets an ICA (for billing and settlement) assigned, before opening a Mastercard project • Signs Thredd addendum for Cross Border Services • Holds the risk when clients are onboarded • Must have a sufficiently funded account to manage a settlement. Failure to have this will result in the transfer failing • Ensures compliance with Scheme mandates and regulator requirements for transfers • Runs Anti-Money Laundering (AML) checks • Holds unique Client or Partner ID assigned by Mastercard passed in the transfer message.
Thredd	• Amazon Web Services (AWS) cloud service using Thredd Portal for reporting if the originating institute decides they want reporting. • APIs consumed by the originating institute. • Thredd Portal interface for Customer Support and Operations. • Holds unique Client or Partner ID assigned by Mastercard passed in the transfer message. • Provides connectivity, API development, data requirements per Mastercard specification, error code management, report and file transfer mechanisms
Programme Manager	• Using either Thredd's new service or the bank's existing service, the cardholder completes KYC checks when opening the account with their bank • Holds an account with the originating institution • Agency checked as having sufficient funds for transfer • Holds unique Client or Partner ID assigned by Mastercard passed in the transfer message • Credit facilities are only through a registered bank that does not hold a money transfer licence
Agency Banking Provider	• Using either Thredd's new service or the bank's existing service, the cardholder completes KYC checks when opening the account with their bank • Has relevant funds to initiate the payment instruction • Originating institute holds unique Client or Partner ID assigned by Mastercard passed in the transfer message • Credit facilities are only through a registered bank that does not hold a money transfer licence

Cross Border Model with BIN Sponsor to Programme Manager

The Cross Border model is for originating institutions that are authorised to include cross border services to a programme manager without a licence and without white label agreement.

The following diagram displays the roles and responsibilities of this model.



The following table describes the rules and responsibilities of the above.

Function	Roles and responsibilities
Mastercard	• Network between sending and receiving institutions • Clearing cycles (settlement data) in XML • Setting up sender configuration (per corridor) • Each originating institute must hold a participation agreement with Mastercard
BIN Sponsor	• Must have a Regulated entity money transfer licence • Signs a Mastercard Participation Agreement, or get an ICA (for billing and settlement) assigned, before opening a Mastercard project • Signs a Thredd addendum for Cross Border Services • Holds the risk as clients are onboarded • Must have a sufficiently funded account to manage a settlement. Failure to have this will result in the transfer failing • Ensures compliance with Scheme mandates and regulator requirements for transfers • Runs Anti-Money Laundering (AML) checks for high value transfers threshold set by regulators • Holds unique Client or Partner ID assigned by Mastercard passed in the transfer message.
Thredd	• APIs consumed by the originating institute. • Thredd Portal interface for Customer Support and Operations. • Holds unique Client or Partner ID assigned by Mastercard passed in the transfer message. • Provides connectivity, API development, data requirements per Mastercard specification, error code management, report and file transfer mechanisms
Programme Manager	• Using either Thredd's new service or the bank's existing service, the cardholder completes Know Your Business (KYB) checks when opening the account with their bank and ongoing KYB as needed by the Payment Card Industry (PCI) • Holds an account with the originating institution • Has relevant funds to initiate the payment instruction

Function	Roles and responsibilities
	• Originating institute holds unique Client or Partner ID assigned by Mastercard that is passed in the transfer message • Credit facilities are only through a registered bank that does not hold a money transfer licence

Client Configuration for Resellers

Configuring Cross Border Services for resellers requires the following:

From a process perspective:

- When an originating institute is onboarded, Compliance at Mastercard will onboard them with the reseller model in mind (it will be highlighted during the compliance review).
- When the originating institute identifies a new Transaction Originator, (any programme manager or aggregator under their programme). The process would be:
    - Fill out a separate form detailing the Transaction Originator name, address, corridors they want to send to and data points.
    - Complete a compliance review.
    - Network reviews to make sure the recipient bank in the corridors are comfortable with the nested flow challenge with the particular corridors of interest.

From an integration perspective:

- Assuming Thredd are integrating with originating institutes that are acting as resellers, then the mapping with the Technical Endpoint Guide should be the same (there are certain mandated requirements for resellers which would be applicable).

Anti-Money Laundering (AML) and Know Your Customer (KYC)

The originating institute is responsible for setting up controls with their programme managers who might run their own AML and KYC checks, as they would for other projects. Specifically, Mastercard and Thredd set up the originating institute as a reseller and from a compliance perspective before Mastercard stress check the controls in place for the specific originating institute, ensuring they have met the regulatory obligations before contracting with Mastercard. The originating institute would be managing their own customers and on-boarding downstream.

Payment Card Industry (PCI) Requirements

Each originating institute or their sub-clients will need to adhere to PCI requirements for the data they handle. There is no additional requirements specific for the Cross Border Service, however all potential originating institute should note that in cash out scenarios where there is a card number involved, this use case increases originating institutes PCI overhead if they don't already handle or store card numbers.

Settlement Accounts and Billing

For this service, there is no requirement for an originating institute to have an existing Mastercard BIN already set up.

This service requires the originating institute to have a settlement "Float" account, set up for the funds to be taken from. The account can be with any bank the originating institute chooses. The specific ICA assigned to your portfolio or Client ID will be billed for the relevant end-of-day settlement amount. The originating institute will need to choose their bank and settlement currency of the account.

The settlement currency is the currency in which a business receives its payments. It is the currency that funds are transferred to the business bank account. This currency is used to finalise and transfer funds from the originating institute to the recipient's bank, ensuring they receive their earnings in the desired currency.

Accessing the API Hub

The Thredd API Hub provides clients with a route to access the Thredd test environment, where clients can test prior to launch.

You can access our test environment using the following url:

- UAT: https://uat-api.thredd.com/api/v1/
- Sandbox: https://sandbox.globalprocessing.com/sandbox/
- Production: https://api.thredd.com/api/v1/

Note: There is a Postman Collection available that you can use to access our test environment. For more information on how to set up the Postman Collection, see Cards API Website: Accessing API Hub.

Note that the service leverages OAuth, a standard security protocol which provides applications with secure delegated access. OAuth works over HTTP and authorises our APIs with signatures generated from private cryptographic keys installed on a Cross Border Services customer's system, rather than less secure user credentials.

The API Hub enables a single, global entry point into Thredd Platform. This includes:

- A unique URL
- A central authentication and authorisation component acting as Policy Enforcement Point (PEP)
- Central logging for all incoming requests

Prerequisites

Before you can use the API Hub, you must be set up on Thredd's Trust Framework. This is a combination of several components which enable secure access to Thredd's resources, using a common identity store. The main components related to the API Hub are:

- CloudEntity
- Radiam Connect

CloudEntity

A Software as a Service (SaaS) capability which acts as the Identity Provider (IDP) for Thredd's interfaces (including Raidiam Connect and Thredd Portal) and as an OAuth OpenID Provider (OP) for the registration and management of customer applications, generation and validation of access tokens, and for the enforcement of access control policies.

Set Up CloudEntity

Thredd sets up CloudEntity for you to enable a Single Sign On journey by linking your IdP with CloudEntity. If you do not use an IdP, CloudEntity can act as the IdP.

A Single Sign On journey is used to access Raidiam Connect for the creation of certificates, as well when connecting to the Thredd Portal card management application. In both cases, there is at least one additional Admin user, who manages users. Once set up, your organisation is unlikely to need to engage with Thredd for integrating CloudEntity.

CloudEntity is also used behind-the-scenes for managing access to the REST API as an Authorisation Server.

Raidiam Connect

Raidiam Connect is Thredd's Certificate Authority for setting up and managing certificates to connect to various services. The certificates include:

- Transport Certificates – for establishing secure connections between resources.
- Signing Certificates – for the creation of signed messages, used for authentication of clients, and non-repudiation and authentication of notifications.
- Encryption Certificates – for the encryption of payloads using an asymmetric encryption approach.

Set Up Radium Connect

Thredd will provide access to Raidiam Connect. Thredd adopts a self-service approach, which allows you to independently manage your certificates.

To request access to Raidiam Connect, please raise a support ticket.

Note: For more information on connecting to Thredd, see the Connecting to Thredd Guide.

Base URLs

There are two base URLs available for the API Hub, depending on the environment you're using.

- For the production environment, use the https://api.thredd.com/ base URL
- For the UAT environment, use the https://uat-api.thredd.com/ base URL

See the Create a Card API for an example of the Create Card endpoint using the production base URL (https://api.thredd.com/api/v1/cards)

Accessing API Hub as a New Client

The following section describes the steps you need to follow to access the API Hub as a new client.

Step One - Request an Access Token

Request an access token by making a call to the Get Access Token endpoint.

See the below example of a successful Get Access Token response. Access tokens are valid for 10 minutes and include the scopes that are associated with your application.

Example Get Access Token response


```
{
    "access_token": "eyJh-
bGciOiJFUzI1NiIsImt-
pZCI6IjI4MjE0MTkzNzIxODQ1ODQ2MTM4MDA3OTA2MDQwMzExOTc1ODE0NCIsInR5cCI6Ik-
pXVCJ9.eyJhaWQiOiJjb25maWRlb-
nRpYWwtY2x-
pZW50cyIsImFt-
ciI6W10sImF1ZCI6WyJodHRw-
czovL3JwLmRp-
cmVjdG9yeS5zYW5kYm94LnRocmVkZGlkLmNvbS9vcGVuaWRfcmVseWluZ19wYXJ0eS8xMzNkMTI2OS01NWVlLTQyYjctYmE3My0wNjA4MzhjMDc0YWUiLCJzcGlmZmU6Ly-
91YXQt-
dGhyZWRkLmV1LmF1dGh6LmNs-
b3VkZW50aXR5Lm-
lvL3Vh-
dC10aHJlZGQvY29uZm-
lkZW50aWFsLWNsaWVudHMvY29uZm-
lkZW50aWFsLWNsaWVudHMt-
b2F1dGgyIl0sImNuZiI6eyJ4NXQjUzI1NiI6IkkzZ0QyZVFydlhl-
cTBsMWNyR2pqS1A1VjVWX0REc1U1MURXQjRPcFZ2M00i-
fSwiZXh-
wIjoxNzQzMDgyOTk4LCJpYXQiOjE3NDMwODIzOTg-
sIm-
lkcCI6IiIsIm-
lzcyI6Im-
h0dHBzOi8vdWF0LXRocmVkZC5ldS5h-
dXRoei5jbG91ZGVudGl0eS5pby91YXQt-
dGhyZWRkL2Nvb-
mZpZGVudGl-
hbC1jbGllb-
nRzIi-
wianRpI-
joiZWMzNTY5MGItMmNkZC00YzJlLTk0ZjItODA1NWE0NGMwZTVkIi-
wib-
mJmI-
joxNzQzMDgyMzk4LCJw-
bWlkI-
```

```
joxNi-
wic2NwIjp-
bIjNkcy5yZWFkIi-
wiYXBh-
dGEucmVhZCIsImFwYXRhLndy-
aXRlIi-
wiYnVsa2Nh-
cmQucmVhZCIsImJ1bGtjYXJkLndy-
aXRlIi-
wiY2FyZHMucmVhZCIsImNh-
cmRzLndy-
aXRlIi-
wiY3Z2LnJlYWQiLCJjd-
nYud3Jp-
dGUiLCJkaWd-
pdGFsY2h-
hbm5l-
bCIsInBpbi5yZWFkIi-
wicGluLndy-
aXRlIi-
wic2Nh-
bWRldGVjdCIsIndzIl0sInN0I-
joicHVibGljIi-
wic3ViI-
joi-
aHR0cHM6Ly9ycC5kaXJlY3Rvcnkuc2FuZGJveC50aHJlZGRpZC5jb20vb3Bl-
bmlkX3Jl-
bHlpbmdfcGFydHkvMTMzZDEyNjktNTVlZS00MmI3LWJhNzMtMDYwODM4YzA3NGFlIiwidGlkIjoidWF0LXRocmVkZCJ9.jdRwIDZzv5tXuR6mPpFJ0JbqiCUCZ-
ToDrluW7AxjEwu78krMYEkDawjhmIfmv8gKTb2qERmMEXxZnOBYuAZ8w",
    "expires_in": 599,
    "scope": "3ds.read apata.read apata.write bulkcard.read bulkcard.write cards.read cards.write cvv.read cvv.write digit-
alchannel pin.read pin.write scamdetect ws",
    "token_type": "bearer"
}
```


Step Two - Include the Access Token in the Authorisation Header

When using the endpoints in the API Hub, you must include Access Token in the header.

Step Three - Add X-Region Header

The X-Region header is mandatory in a header and determines the region or environment you are trying to connect to. Select from:

- Use 0 for the Default environment
- Use 1 for the EMEA environment
- Use 2 for the APAC environment

Note: If you're not sure of the environment you should use, speak to your Account Manager or Implementations.

Webhooks

Webhooks is a comprehensive service designed to facilitate real-time event subscription and notification delivery.

You can use the Thredd REST API to create and update webhook endpoints, and specifying desired events for notification for the endpoints. Additionally, clients can retrieve historical or missed events on demand, update their details, and manage event subscriptions. Webhooks provide a robust platform for efficient event-driven interactions, retrieving notification details, subscribing to events, and re-sending notifications.

The advantage of webhooks is that there is no persistent open connection to the system where you need to keep filtering for events that you are interested in. It is an asynchronous mechanism where you wait for the system to notify you. The HTTP payload will contain the details of the event. Before using webhooks, you will need to setup a URL that can listen for any alerts. Contact the Thredd Application Support Team for help with this as your IP address must be whitelisted first. When the URL has been set up correctly, it must be registered using the Create Webhook endpoint.

About Events

When a webhook has been created, events can be created for them. An event is an activity that happens outside of your system, such as a change in transaction status or request for information. For example, a fraud event is triggered which causes the card to be suspended. The webhook is then sent the details of the attempted transaction, allowing you to proactively contact your cardholder.

The Thredd cross border service there will be three key webhook notifications:

- General Status of the Transaction:
    - Quote status
    - Transaction status change
    - Cancellation of the quote or transaction
    - Retrieval of quote or transaction
- Additional services:
    - Request for information (RFI) from the receiver
    - Document request
    - Return information via above API
    - Information supplied incorrect, check

How it Works

1. Program managers create a webhook using the Create Webhook endpoint.
2. The program manager creates a subscription for the webhook to subscribe to specific events using the Add Event Subscriptions endpoint. This allows the webhook to receive notifications for those events.
3. When the setup is complete, whenever the event triggers, the webhook sends notifications to the program managers, ensuring they receive updates on relevant events and changes on their systems or applications.

Responding to Webhooks

Webhook endpoints should return a 2XX HTTP status code. Any other information you return in the request headers or request body will be ignored. If Thredd does not receive a 2XX response to our POST request, we will retry the request to a maximum of 3 times.

Retry	Time after first failure
1st Retry	1 second.
2nd Retry	1 second.
3rd Retry	1 second.

Thredd will not process the event further after 3 retries. We recommend utilising notificationId as your main duplicate check. This is important if a webhook has failed and needs to be resent.

Example of Webhook Endpoints

The following table describes each of the available endpoints you can use for creating and maintaining webhooks and events.

Name	Verb	Endpoint	Description
Register New Webhook	POST	eds/api/v1/Webhooks	Enables you to create a webhook service. It returns a Webhook identifier that should be saved if the notification needs to be amended in the future.
List Webhooks for Program Manager	GET	eds/api/v1/Webhooks	Enables you to view all webhooks associated with a specific program manager.
Update Webhook Details	PUT	eds/api/v1/Webhooks/{webhook_id}	Enables you to update webhook details by specifying the webhookId in the endpoint URL.
Get Webhook Details	GET	eds/api/v1/Webhooks/{webhook_id}	Enables you to retrieve webhook details by using the webhookId in the endpoint URL.
Update Webhook Details	PUT	eds/api/v1/Webhooks/{webhook_id}/status	Enables you to update the webhook status, such as activation and unregistration, by specifying the webhookId in the endpoint URL.

Manage Event Transactions

This page details how to retrieve the status of the cross border service transaction status from a webhook.

Events send a notification to your webhook endpoint when something happens on your programme. Events occur when an API resource changes state, and their data field shows the resource's state at that moment. You can retrieve events through API endpoints or set up webhooks to get Event objects sent to your server.

Thredd's page for managing webhooks is here for reference: Manage Event Subscriptions

Get Event Notifications

The Get Event Notifications "TransactionReference" endpoint enables you to retrieve the events to a webhook, with the webhook ID specified in the URL. You can retrieve a webhook's event TransactionReference by making a GET request to the Get Event TransactionReference endpoint, including the webhookId in the URL. For example:

```
https://api.thredd.com/eds/api/v1/Webhooks/{webhook_id}/TransactionReference
```

If successful, a 200 response is returned and the response will list all event subscriptions associated with the webhook. For example:

Example Get Event Subscriptions response

```
{
"status": "success",
"response" : {
  "webhookId":"12345666",
   content: [
   {
      "eventCode" : 200,
      "description" :"transactionReference"
   }
 }
```

Error Codes and Network Codes

Successfully processed API requests will result in response messages with HTTP code 200 (SUCCESS). A transaction response with an 'APPROVED' status ("status": "APPROVED") indicates that the transaction was successful. In some situations, a transaction response can have an 'UNKNOWN' status, see Transaction Responses with an 'UNKNOWN' Status.

Cross border services uses HTTP reason codes to communicate the status of the transaction, for a full list please refer to this page: Appendix 1: Response Codes and Error Handling.

Transaction Responses with an UNKNOWN Status

A timeout can occur when the “payment brand a.k.a. scheme” does not receive a response from the Receive Network within the expected timeframe (40 seconds). In rare cases, such as timeouts or network communication issues, a transaction response can have an ‘UNKNOWN’ status. The “scheme” will continue to retrieve the status from the Receive Network. If the transaction was approved or declined, the status will be changed accordingly and will be reflected in GET response.

Do not resubmit a transaction that has an ‘UNKNOWN’ status, because the original transaction may have been processed successfully.

In rare situations, an API lookup call or Webhook call that results in an ‘UNKNOWN’ status response, the final status will be reflected in the appropriate system within 24 hours, i.e. the result could take up to 24 hours to successfully reflect the outcome.

Cross Border APIs

The following APIs are available to support Cross Border services. These are split into two areas:

- Validation and Quote APIs
- Payment APIs

Quotes

The Quotes endpoint enables you to calculate for configured service corridors, the amount senders should fund or recipients will receive for a payment, depending on the Transaction Instruction.

Example Quotes endpoint:

```
{{base-url}}/send/v1/partners/{partner-id}/crossborder/quotes
```

Quote Confirmation

The Quote Confirmation endpoint enables you to confirm the FX rate quote that you received in the Quotes endpoint. This confirmation is mandatory prior to submitting a payment transaction. The Quote Confirmation endpoint needs to be run before the 'confirmationExpiryTime' received in the Quotes endpoint response.

Example Quote Confirmation endpoint:

```
{{base-url}}/send/partners/{partner_id}/crossborder/quotes/confirmations
```

Cancel Confirmed Quote

The Cancel Confirmed Quote endpoint enables you to cancel a quote that has been confirmed using the Quote Confirmation endpoint.

Example Cancel Confirmed Quote endpoint:

```
{{base-url}}/send/partners/{partner_id}/crossborder/quotes/cancellations
```

Retrieve Confirmed Quote

The Retrieve Confirmed Quote endpoint enables you to retrieve quote details requested for payment utilisation.

Example Retrieve Confirmed Quote endpoint:

```
{{base-url}}/send/partners/{partner_id}/crossborder/quotes/{transaction_reference}/proposals/{proposal_id}
```

Payment APIs

The following section describes the endpoints used during payment transactions.

Submit Payment

The Submit Payment endpoint enables you to submit a transaction instruction to send transaction funds to a recipient.

Example Submit Payment endpoint:

```
{{base-url}}/send/v1/partners/{partner-id}/crossborder/payment
```

Clearing

Thredd currently offers the settlement services for transactions and the flow is as follows:

1. Thredd receives the Clearing message.
2. The message is processed and the data extracted.
3. Thredd checks the validity of the Account, PAN or DPAN.
4. Thredd matches the clearing message to the corresponding original payment instruction.
5. Thredd updates the balance accordingly:
    a. Removes pending status or amounts
    b. Debits amount from actual balance
    c. Reflects the updated available balance
6. If there is no matching payment instruction identified, the balance updates must still be applied.
7. If no clearing message has been received within the time frames configured on the client product (usually 24 hours from payment instruction) then the pending amount is automatically returned to the card's available balance.

Note: Clearance process for Cross Border transactions: Thredd is not involved in the transfer of funds and the client must hold the balance directly with the Scheme.

Settlement Configuration

The client will set up the following with the Scheme, Mastercard:

- Settlement models, (pre-funded or not)
- Settlement Currencies,
- Payment details,
- Holidays,
- Time zone impacts to funding a Settlement Bank Account or Collateral Account, details pertinent to the settlement model
- Processing Cutoff time.

Clearing Files

The following files are used for the clearance purpose.

Pre-funding Settlement Model and Collateral Settlement Model

The Collateral settlement model is a terminology only used in the UK that refers to pre-funding.This model requires a customer to hold funds into an account in advance of transactions being processed

Report Name	Description File	File Transfer Bulk Type	Occurrence/Timing/Format
Daily Transaction Reports (DTR)	Provides detailed Transaction Instructions for new Transactions for the 24-hour Processing Day.	Standard: Test: T6J6 Production: T6J4 Encrypted: Test: T1Q2 Production: T1Q0	Daily at the start of the 24-hour processing window defined by the Cross-Border Services Customer.
Balance Activity Report	Provides all Processing Day Transactions that impacted an applicable balance, along with the amount. Transactions are grouped by currency.	Standard: Test: TC7K Production: TC7J Encrypted: Test: T1D4 Production: T1Q8	Daily at the start of the 24-hour processing window defined by the Cross-Border Services Customer.
Status Change Report (SCR)	Provides detailed Transaction Instructions for Transactions where a status has changed since the previous Transaction status was reported.	Standard: Test: T6J2 Production: T6J0 Encrypted: Test: T1Q6 Production: T1Q4	Daily, at 4 intervals, including weekends and holidays 5 am, 11 am, 5 pm and 11 pm (CT)

Next Day Settlement Model

Next Day Settlement Model refers to a customer paying a balance of all different transactions carried by Mastercard the day before.

Report Name	Description File	File Transfer Bulk Type	Occurrence/Timing/Format
Daily Transaction Reports (DTR)	Provides detailed Transaction Instructions for new Transactions aligning to the Processing Cutoff for the current Processing Day	Standard: Test: T6J6 Production: T6J4 Encrypted: Test: T1Q2 Production: T1Q0	Daily around 9:30 pm (CT), including weekends and holidays. CSV format.
Settlement Reconciliation file (SRF)	Provides the amount to be settled and the details associated with each Transaction that is part of the settlement for that Processing Day. Transactions are grouped by currency.	Standard: Test: TX39 Production: TX37 Encrypted: Test: T1D4 Production: T1Q8	Daily around 1:30 am (CT)
Status Change Reports (SCR)	Provides detailed Transaction Instructions for Transactions where a status has changed since the previous Transaction status was reported.	Standard: Test: T6J2 Production: T6J0 Encrypted: Test: T1Q6 Production: T1Q4	Daily, at 4 intervals, including weekends and holidays at 5 am, 11 am, 5 pm and 11 pm (CT)
Net Settlement Advisement (optional)	Provides Net Settlement Positions by Cross-Border Services Customer ICA, and not CrossBorder Services specific. See line 10 of the report.	Made available via Mastercard Connect, email, or fax.	

Appendix 1: Response Codes and Error Handling

For more information on all HTTP status codes, refer to the Mastercard developer site: Mastercard Developers.

Request Method	Common Response Codes
POST	200 (OK) = Request completed successfully 400 (BAD REQUEST) = General errors with request message 402 (REQUEST FAILED) = Transfer declined 409 (CONFLICT) = Errors with transaction reference ID 500 (INTERNAL SERVER ERROR) = System error
GET	200 (OK) = Request completed successfully 400 (BAD REQUEST) = General errors with request message 404 (NOT FOUND) = Supplied ID not found or invalid

The following table includes more response codes that may be returned for requests. In the event of network or infrastructure issues, other response codes may be returned by the infrastructure, per Mastercard developer guide, please refer to the Mastercard developer guide and error handling scenarios (On Thredd Confluence).

HTTP Response Codes	Description
200 (OK)	The GET request to retrieve details for a disbursement was successful.
201 (CREATED)	The POST request to create a disbursement (Payment Transaction) was processed successfully. A response status value of 'APPROVED' indicates the transaction was successful. If the status is 'UNKNOWN', see Transaction Responses with an 'UNKNOWN' Status.
202 (ACCEPTED)	Can occur for some timeouts. The POST request was accepted but did not complete during the allotted timeframe, so the response status value is 'UNKNOWN'. Processing of the request will continue asynchronously. You can use a GET request to retrieve the latest status, see Transaction Responses with an 'UNKNOWN' Status.
400 (BAD REQUEST)	The request could not be fulfilled due to general errors such as validation errors or missing required data.
401 (UNAUTHORIZED)	Error code response for missing or invalid authentication token.
402 (REQUEST FAILED)	The POST request to create a disbursement (Payment Transaction) was processed successfully but the transaction was declined. You can use a GET request to see the Network Response Code, which indicates the issuer's reason for declining the transaction, see Network Response Codes.
403 (FORBIDDEN)	You are not authorized to perform the operation, or the resource is unavailable for some reason.
404 (NOT FOUND)	The GET request to retrieve details for a disbursement was unsuccessful because the disbursement was not found.
405 (METHOD NOT ALLOWED)	The requested URL exists, but the requested HTTP method is not applicable. For the permitted methods, see API Reference.
409 (CONFLICT)	The POST request does not have a unique Disbursement Reference ID. You must use a unique ID for each new disbursement.
429 (TOO MANY REQUESTS)	You have sent too many requests in a given amount of time ("rate limiting"). The response will include a Retry-After header indicating how long to wait before making a new request. This is a courtesy response. When the service is receiving a very large number of requests from a single party the system may just drop connections to

HTTP Response Codes	Description
	minimize resource monopolization.
500 (INTERNAL SERVER ERROR)	The server encountered an unexpected condition which prevented it from fulfilling the request. It indicates an error that the caller cannot address from their end. Requests resulting in a 500 response code will generally include the Mastercard Send API error structure in the response.
5XX (SERVER ERROR)	Typically indicates an error in the network infrastructure between the client and Mastercard Send API server. Such errors will never contain the Mastercard Send API error structure in the response.

Contact Us

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

Thredd Ltd.

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.

Document History

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

Version	Date	Reason	Revised by
1.0	28/05/2025	First version	JB

1 Glossary

A

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.

C

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.

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

Mastercard Interface Processor (MIP)

The processing hardware and software system that interfaces with Mastercard's Global Payment System communications network.

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.

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.

Originating Institution (OI)

The entity with a money transfer licence that has an agreement with Mastercard and Thredd to offer the service to their cardholders. They can also be an OI if they have the appropriate agreement to offer services to their programme managers and/or agencies. For example, an Originating Institution offers services to its customers that are the Senders of a Transaction.

P

Partial Amount Approval

Some acquirers support a partial amount approval for Debit or Prepaid payment authorisation requests. The issuer can respond with an approval amount less than the requested amount. The cardholder then needs to pay the remainder using another form of tender.

Program Manager

A 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.

S

Scheme (Network)

Card network responsible for managing transactions over the network and for arbitration of any disputes. For Cross Border Services the network is Mastercard and is the regulated entity that will be the owner of the Originating Institute.agreement. Thredd is authorised to offer the issuer processing service to the Originating Institute.

sFTP

Secure File Transfer Protocol. File Transfer Protocol FTP) is a popular unencrypted method of transferring files between two remote systems. SFTP (SSH File Transfer Protocol, or Secure File Transfer Protocol) is a separate protocol packaged with SSH that works in a similar way but over a secure connection.

Smart Client

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

SSL Certification

An SSL certificate displays important information for verifying the owner of a website and encrypting web traffic with SSL/TLS, including the public key, the issuer of the certificate, and the associated subdomains.

Stand In Processing (STIP)

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

T

Technical Integrator (TI)

Thredd is the Technical Integrator of record which integrates the Cross Border Service for their Platform. Clients need the appropriate “Thredd addendum” agreement to offer services to their cardholders, programme managers and/or agencies.

Thredd Portal

Thredd Portal is Thredd's new web application for managing your cards and transactions on the Thredd Platform.

TLS

Transport Layer Security (TLS) is a security protocol that provides privacy and data integrity for Internet communications. Implementing TLS is a standard practice for building secure web apps.

Transaction Originator

The programme manager or agency that is nested under the parent OI portfolio. A financial institution holding all required licenses is needed to offer services to its direct customers and participates in Cross-Border Services indirectly using an Originating Institution under the Reseller Model.

V

Validation

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