Thredd Portal PAN Finder Guide

Version: 1.0

26 June 2025

Publication number: TPPFG-1.0-5/6/2025

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 user guide provides information on how to install and use PAN Finder in Thredd Portal.

Target Audience

This guide is aimed at personnel who manage Primary Access Numbers (PANs), and are entrusted to handle card security in their corporation.

What's Changed?

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

Other Documentation

Refer to the table below for a list of other relevant guides that you can use in conjunction.

Document	Description
Thredd Portal Guide	Provides details of Thredd Portal for managing cards and transactions.

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

Introduction to PAN Finder in Thredd Portal

PAN Finder is a feature of the Thredd Portal application that enables you to find the 16-digit **PAN (Primary Account Number)**[1] from its associated 9-digit **Thredd token**[2]. It is a unique feature that is separate from the main card and transaction management functionality that exists within Thredd Portal. Possessing the cardholder's PAN can be useful for various card management and troubleshooting tasks, where it enables you to:

- contact the Card Scheme (Network) to query a transaction.
- initiate a chargeback process.
- check if the transaction is fraudulent with parties such as the Card Scheme or the police.

Organisations that are not compliant with **PCI-DSS**[3] do not store a customer's PAN in their database, and can therefore use this feature to find the PAN. However, an organisation compliant with PCI-DSS can also use this feature in the same way.

Accessing PAN Finder

For accessing PAN Finder, Thredd will need to approve your request, and your Organisation Administrator will set you up with the role of Sensitive Information Manager.

Requesting PAN Finder Access with Thredd

For requesting PAN Finder access, you will need to raise a JIRA ticket with customer support at Thredd using the following link: https://thredd.atlassian.net/jira/servicedesk/projects/CSTHREDD/

Access will require you to be on the Approval list. If you are unsure, check internally with your organisation. The Operations team will then inform you if your request is approved or declined.

Sensitive Information Manager Role

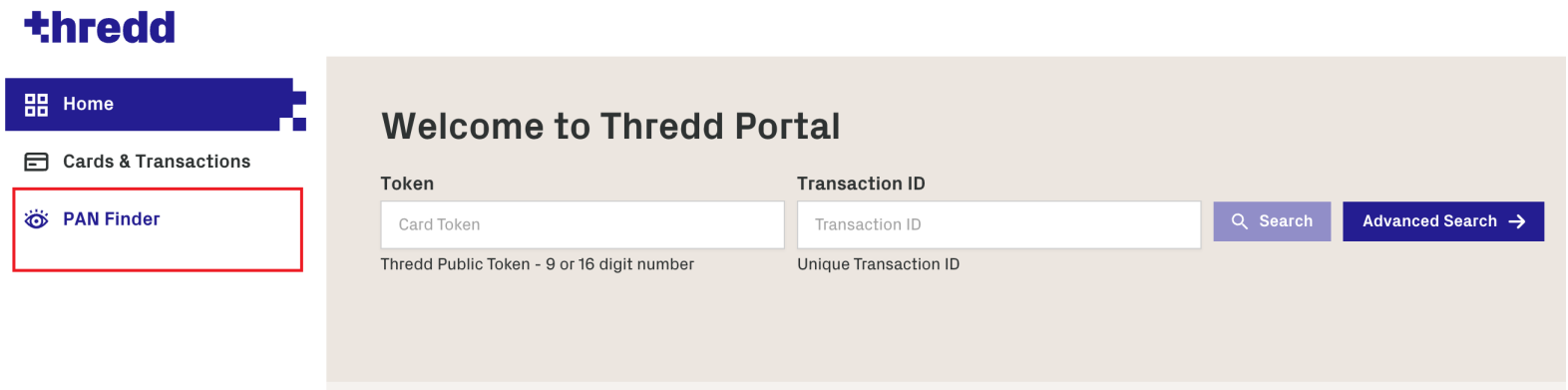
The Sensitive Information Manager is a role for finding the customer's PAN only, and does not allow you to perform the main card management functions in Thredd Portal. A single user in an organisation is assigned the Sensitive Information role by the Super Admin using a third party application called **CloudEntity**[4],

> **Note:** Because the 16-digit PAN is sensitive personal data, the user with the role of Sensitive Information Manager will bear the risk of managing this customer cardholder data. The role must only be granted to users that have strong knowledge of data security standards.

When you have received approval and have been set up with the role of Sensitive Information Manager, you will see the PAN Finder option when you sign in to Thredd Portal.

---

[1]The Primary Account Number (PAN) is the card identifier found on credit and debit cards, as well as stored-value, gift and other similar cards. The 16-digit PAN is typically embossed on a physical card.
[2]A Thredd token refers to a digital representation of a payment card, created as part of the tokenisation process. Tokenisation is a security measure that replaces sensitive card information, such as the Primary Account Number (PAN), with a unique identifier or "token."
[3]The Payment Card Industry Data Security Standard (PCI DSS) is a comprehensive information security standard designed to protect credit card and payment card data.
[4]A service that provides identity, authorization, and open banking solutions to help organizations deliver secure digital transformation. Cloudentity is the Identity Provider (IdP) for Thredd Portal, and is also an OAuth OpenID Provider (OP) for the REST API.



Legal Disclaimer

When accessing the user interface for PAN Finder, you will need to agree to the following disclaimer.

By using PAN Finder to retrieve or view full Primary Account Numbers (PAN), Cardholder Data (CHD), or Sensitive Authentication Data (SAD), you acknowledge that your organization may fall within the scope of the Payment Card Industry Data Security Standard (PCI DSS). CHD includes the PAN, cardholder name, expiration date, and service code, while SAD comprises sensitive elements such as card verification codes (CVV/CVC), full magnetic stripe or chip data, and PINs used to authenticate cardholders and authorize transactions.Accessing or handling full PAN, CHD, or SAD imposes stringent security obligations, including strict controls on storage, transmission, and access, as mandated by PCI DSS. Failure to comply with these requirements may expose your organization to significant compliance risks, financial penalties, reputational damage, and increased vulnerability to data breaches.Please ensure you have the necessary authorizations, controls, and safeguards in place before accessing or processing this sensitive data.

Managing Access to PAN Finder

As an Organisation Administrator user in Thredd Portal, you can provide users with access to PAN Finder by assigning them the Sensitive Information Manager Role in CloudEntity. The user must have met the eligibility requirements for using the feature. Similarly, for any user that no longer needs access, you can assign them to a different Thredd Portal role, which allows them to use Thredd Portal without PAN Finder.

CloudEntity is the Identity Provider (IDP) that allows users in organisations that use the Thredd Platform to access Thredd Portal through SSO. When the role is assigned through CloudEntity, the user can access PAN Finder through SSO.

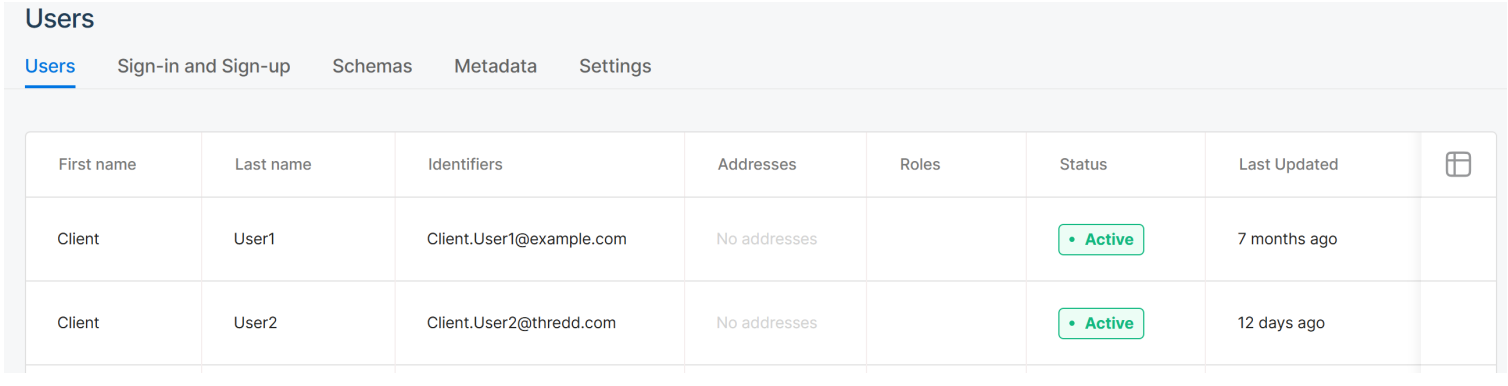
Program Manager Codes

Your organisation may use a dedicated Program Manager code for PAN Finder. If so, you will need to remove any other Program Manager codes when adding the Sensitive Information Manager role. You should therefore make sure that you know which codes to remove from the user profile.

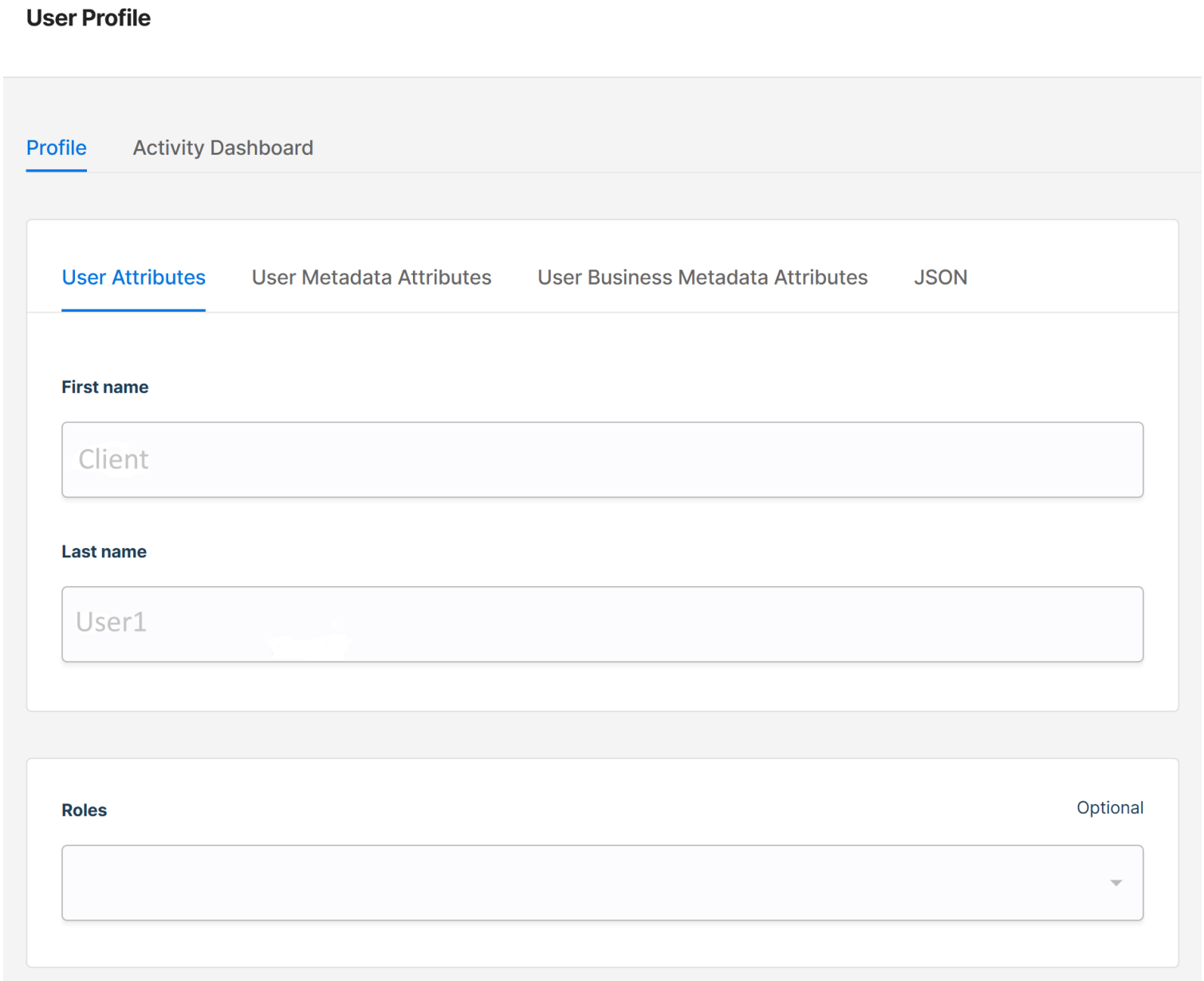
Adding the Sensitive Information Manager Role to a User

You add the Sensitive Information Manager role to a user through the CloudEntity application.

1. Log in to CloudEntity at https://auth.uat.threddid.com. CloudEntity application displays the homepage for your organisation, which includes the details of the users.
2. Select **Users** from the left-hand menu. The Users page appears.



3. Double-click an entry for a user that you want to set the role for. The profile for the user appears.



4. Click the **User Business Metadata Attributes** tab.
5. If your organisation has more than one Program Manager Code (pmcode), you can remove the other codes and keep the one for PAN Finder access by clicking the minus button next to the Restricted codes list.
6. Select Sensitive Information Manager under **Thredd roles**.

7. When you are ready to release to production, perform steps 1 to 5 after logging in to https://auth.prod.threddid.com.

Removing PAN Finder Access for a User

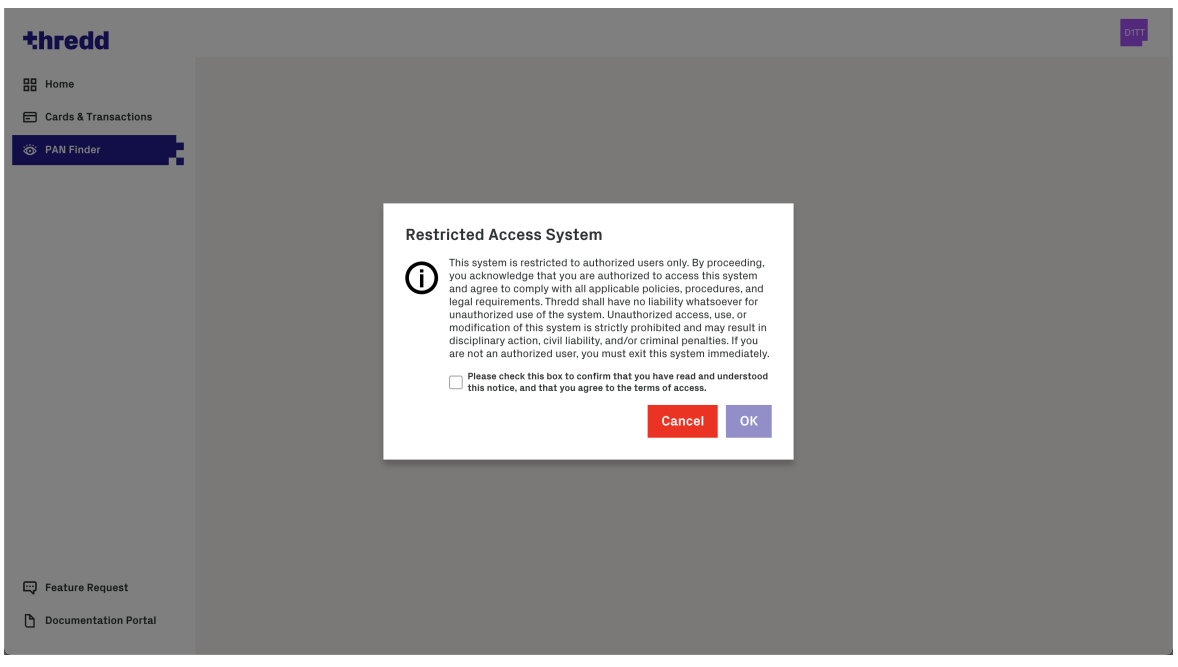
You remove access to PAN Finder to a user through CloudEntity.

1. Access details of the user with the role of Sensitive Information Manager by double-clicking a user entry from the **Users** page.
2. Click on **User Business Metadata Attributes**.
3. Select any role other than Sensitive Information Manager from the **Thredd Roles** drop-down list.
4. Click **Save**.
5. When you are ready to release to production, perform steps 1 to 4 after logging in to https://auth.prod.threddid.com.

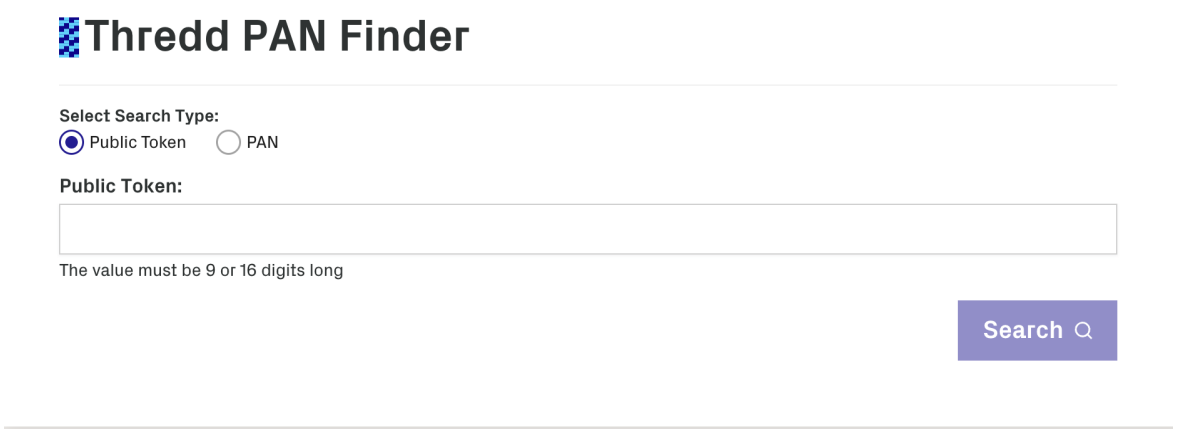
Using PAN Finder in the Thredd Portal Interface

When set up with the Sensitive Information Manager role, you can log in to **Thredd Portal**[1] via SSO and start using the PAN Finder functionality from the interface.

1. Log in to Thredd Portal and observe the following message in the window.



2. When you have read and understood the notice, select the check box.
3. Click **OK**. The Thredd PAN Finder screen appears. The Search Type is the option you use for finding the token or PAN.



4. To find the PAN, do the following:
    1. Ensure that the **Public Token** option is selected.
    2. Enter the 9-digit Thredd token in the **Public Token** field.
    3. Click **Search**. The relevant token appears in the search results.
5. To find the Public Token from the PAN, do the following:
    1. Select the **PAN** option.
    2. Enter the 16-digit PAN in the **PAN** field.
    3. Click **Search**.

The PAN and Thredd token details that appear as search results are obscured after 30 seconds to prevent the data from being exposed.

[1] Thredd Portal is Thredd's new web application for managing your cards and transactions on the Thredd Platform. For more information, see the Thredd Portal Guide.

General FAQs

This section provides answers to frequently asked questions.

Q. How do the PAN Finder appear in the Thredd Portal user interface?

PAN Finder consists of a field in which you enter the 9-digit Thredd token to retrieve its PAN. This field appears after you acknowledge the notice.

Q. What is the Sensitive Information Manager role?

The Sensitive Information Manager is a role in Thredd Portal that allows a user to operate PAN Finder. The role is set in CloudEntity.

Q. Does the Sensitive Information Manager allow me to use other functions in Thredd Portal?

No, the Sensitive Information Manager role only allows a user to use PAN Finder.

Q. Does an organisation need to be PCI-Compliant to use PAN Finder?

An organisation is not required to be PCI-compliant in order to use PAN Finder. However, they need to understand the security implications of handling sensitive cardholder data.

Glossary

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

#

3D Secure

3D Secure (3-domain structure), also known as a payer authentication, is a security protocol that helps to prevent fraud in online credit and debit card transactions. This security feature is supported by Visa and Mastercard and is branded as ‘Verified by Visa’ and ‘Master-card SecureCode’ respectively.

A

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.

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.

C

Card Scheme (Network)

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

Chargeback

Where a cardholder disputes a transaction on their account and is unable to resolve directly with the merchant, they can raise a chargeback with their card issuer. The chargeback must be for a legitimate reason, such as goods and services not received, faulty goods, or a fraudulent transaction.

Clearing File/Clearing Transaction

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.

CloudEntity

A service that provides identity, authorization, and open banking solutions to help organizations deliver secure digital transformation. Cloudentity is the Identity Provider (IdP) for Thredd Portal, and is also an OAuth OpenID Provider (OP) for the REST API.

E

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 mag-netic stripes for backward compatibility.

External Host

The external system to which sends real-time transaction-related data. The URL to this system is configured within 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 per-form transaction-related services, such as payment authorisation, transaction matching and reconciliation.

F

Fee Groups

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

H

Hanging Filter

The period of time during which waits for an approved authorisation amount to be settled. This is defined at a product level. A typical default is 7 days for an auth and 10 days for a pre-auth.

I

Incremental Authorisation

A request for an additional amount on a prior authorisation. An incremental authorisation is used when the final amount for a transaction is greater than the amount of the original authorisation. For example, a hotel guest might register for one night, but then decide to extend the reservation for additional night. In that case, an incremental authorisation might be performed in order to get approval for additional charges pertaining to the second night.

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

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.

MIP

Mastercard Interface Processor (MIP) The processing hardware and software system that interfaces with Mastercard's Global Payment System communications network.

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.

P

PAN (Primary Account Number)

The Primary Account Number (PAN) is the card identifier found on credit and debit cards, as well as stored-value, gift and other similar cards. The 16-digit PAN is typically embossed on a physical card.

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.

PCI-DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a comprehensive information security standard designed to protect credit card and payment card data.

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

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

Thredd Portal

Thredd Portal is Thredd's new web application for managing your cards and transactions on the Thredd Platform. For more information, see the Thredd Portal Guide.

Thredd token

A Thredd token refers to a digital representation of a payment card, created as part of the tokenisation process. Tokenisation is a security measure that replaces sensitive card information, such as the Primary Account Number (PAN), with a unique identifier or "token."

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.

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.

V

Validation

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

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	Reason	Revised by
1.0	26-06-2025	First version	KD

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.