PSD2 SCA Guide

Version: 1.4

28 March 2024

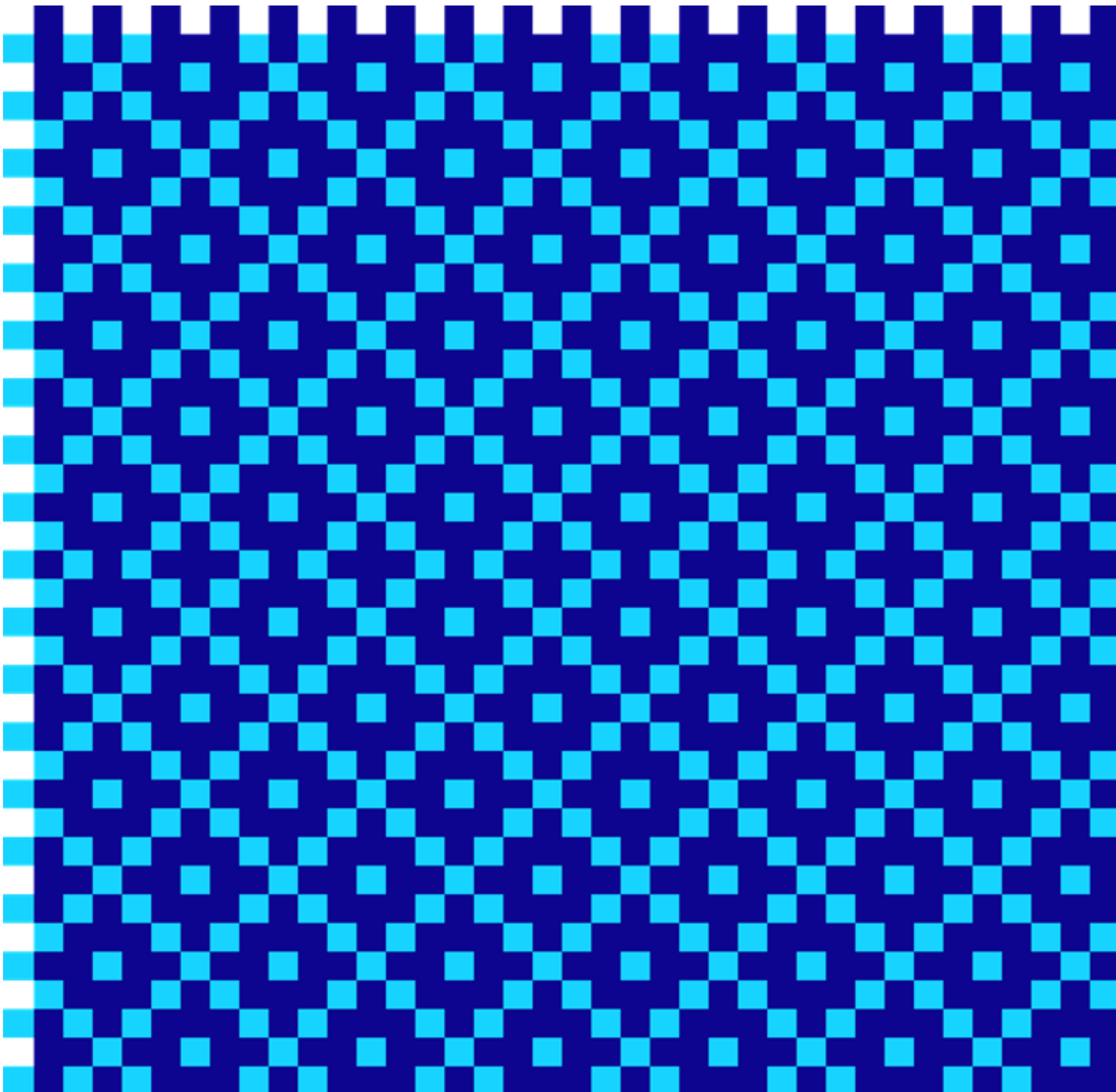
Publication number: PSD-SCA-1.4-3/28/2024

For the latest technical documentation, see the Documentation Portal.

Thredd 6th Floor, Victoria House, Bloomsbury Square, London, WC1B 4DA

Support Email: occ@thredd.com

Support Phone: +44 (0) 203 740 9682



Copyright

About this Guide

This guide provides information on the processing of transactions under the Second Payment Services Directive (PSD2) Strong Customer Authentication (SCA) regulations.

Target Audience

Technical team(s) responsible for implementing processing of cards within their card program.

What's Changed?

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

How to use this Guide

- To find out about the rules relating to PSD2 SCA, see PSD2 Strong Customer Authentication.
- To understand the end-to-end transaction flow and Thredd checks related to PSD2, see PSD2 Transaction Checks.
- For details of the PSD2 exemption checks run by Thredd, see PSD2 Rules and Exemption Checks.

Related Documents

Refer to the table below for a list of other relevant documents that should be used together with this guide.

Document	Description
External Host Interface (EHI) Guide	Describes the Thredd External Host Interface (EHI) and provides specifications on how to process and respond to messages received from EHI.
Transaction XML Reporting Guide	Describes the structure and contents of the Thredd Transaction XML reports.
3D Secure Guide (Apata)	Describes the Thredd 3D Secure Apata service and how to implement a 3D Secure project.
3D Secure Guide (Cardinal)	Describes the Thredd 3D Secure Cardinal service and how to implement a 3D Secure project.

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

External Documents

Document	Description
www.eba.europa.eu: Final Report on Draft RTS on SCA and CSC under PSD2	European Banking Authority (EBA) Final Report Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2). EBA/RTS/2017/02; 23 February 2017

PSD2 & Strong Customer Authentication

The Second Payment Services Directive (PSD2), is an European Union (EU) Directive which sets requirements for firms that provide payment services. It aims to improve consumer protection, make payments safer and more secure. PSD2 came into force on 13th January 2018, with some individual countries within the EU having extensions until 2022[1]. PSD2 introduced some new requirements for card issuers and processors, such as:

- The requirement for Strong Customer Authentication (SCA) on all e-commerce and contactless payments unless specific exemptions apply.
- The requirement for Dynamic SCA Linking - verifying that the details in an authentication session match the details in the subsequent payment authorisation

PSD2 rules are issued by the European Banking Authority (EBA).

Strong Customer Authentication (SCA)

The EBA states that for a transaction to be Strong Customer Authenticated (SCA), at least two of the following must be verified during the transaction:

- Cardholder must be identified by some characteristic unique to them (e.g. fingerprint, iris scans)
- Cardholder must know something only they should know (e.g. PIN, phone unlock code)
- Cardholder must possess something (e.g. chip card, mobile phone)[2]

Note: Thredd currently considers all 3D Secure transactions as SCA[3]. If the 3D Secure transaction is considered as SCA, Thredd automatically flags the possession and knowledge tests in the EHI `GPS_POS_Data` field. See PSD2 Transaction Status.

[1] According to the Financial Conduct Authority (FCA), the deadline for enforcing PSD2 SCA requirements in the UK was extended to March 14, 2022.

[2] The SCA possession test must be made with dynamic data, for example, using the EMV ARQC (Authorisation ReQuest Cryptogram), to prove the cardholder has the card. Using the magnetic stripe, for example, is not proof of possession.

[3] We can optionally set your programme so that Thredd only considers 3DS transactions as SCA if the cardholder was challenged.

PSD2 Dynamic Linking

PSD2 Dynamic SCA Linking requires that the details provided in a 3D Secure authentication session matches the details that were provided during the transaction authorisation. For example, matching of the authorised amount to the authenticated amount, and matching of the merchant name.

Thredd can do this matching. Alternatively, you can perform matching using details provided in transaction messages sent from the Thredd External Host Interface (EHI) to your systems. For more information, see the EHI Guide > Transaction Matching - Authentications and Authorisations.

SCA Exemptions

All transactions must have Strong Customer Authentication (SCA), unless they meet one of the following European Banking Authority (EBA) exemptions:

Article	Description of SCA Exemption
Article 11	Contactless transaction of up to EUR 50.00, and cumulatively not exceeding EUR 150.00 or 5 transactions.
Article 12	Paying a transport or parking fare at an unattended terminal.
Article 13	The receiver of funds is a trusted beneficiary, or this is a recurring payment transaction (but not the first instance of).
Article 14	The sender and receiver of funds are the same person.
Article 15	E-commerce transaction of up to EUR 30.00, and cumulatively not exceeding EUR 100.00 or 5 transactions.
Article 16	E-commerce transaction classified as low-risk (as defined in the Article).

Note: The specific transaction limits (i.e., frequency and amount) may vary per country. Please check with your Issuer or country financial regulator for details. These limits can be set at your Thredd card Product level. See PSD2 Product Settings.

Transactions where the PSD2 rules do not apply

The PSD2 rules do not apply to the following types of transactions:

- The Issuer (BIN Sponsor) or Acquirer is outside the EBA's jurisdiction (i.e., outside the EEA or UK):
    - The Issuing BIN range is outside the EEAor UK (your BIN range will be exempt unless you specifically request including in SCA checks)
    - The Acquirer is outside the EEA or UK
- Credit transactions - where money is paid into the card
- Transactions to create a payment token[4]
- Mail Order or Telephone Order transactions[5]
- The message from Visa/Mastercard does not count as a transaction in EBA's definition. Examples:
    - Account Verification Requests / Account Status Enquiry requests
    - Merchant tokenisation (digital wallet) requests

Note: To understand the end-to-end transaction flow and Thredd checks related to PSD2, see PSD2 Transaction Checks.

Find out more about the PSD2 Regulations

Below are links to additional information about the PSD2 and SCA regulations.

- EBA website: Regulatory Technical Standards on strong customer authentication and secure communication under PSD2
- FCA website (UK only): Deadline extension for Strong Customer Authentication

[4] The payment token setup already has *approve-with-authentication*, which meets the EBA's requirement.

[5] The EBA is of the view that anything initiated via paper or telephone is out of the scope of SCA under PSD2.

PSD2 Transaction Checks

The figure below provides a summary of the checks that Thredd runs on an incoming payment authorisation transaction to determine whether the PSD2 rules apply and to approve or decline the transaction, based on whether Strong Customer Authentication (SCA) has been correctly applied.

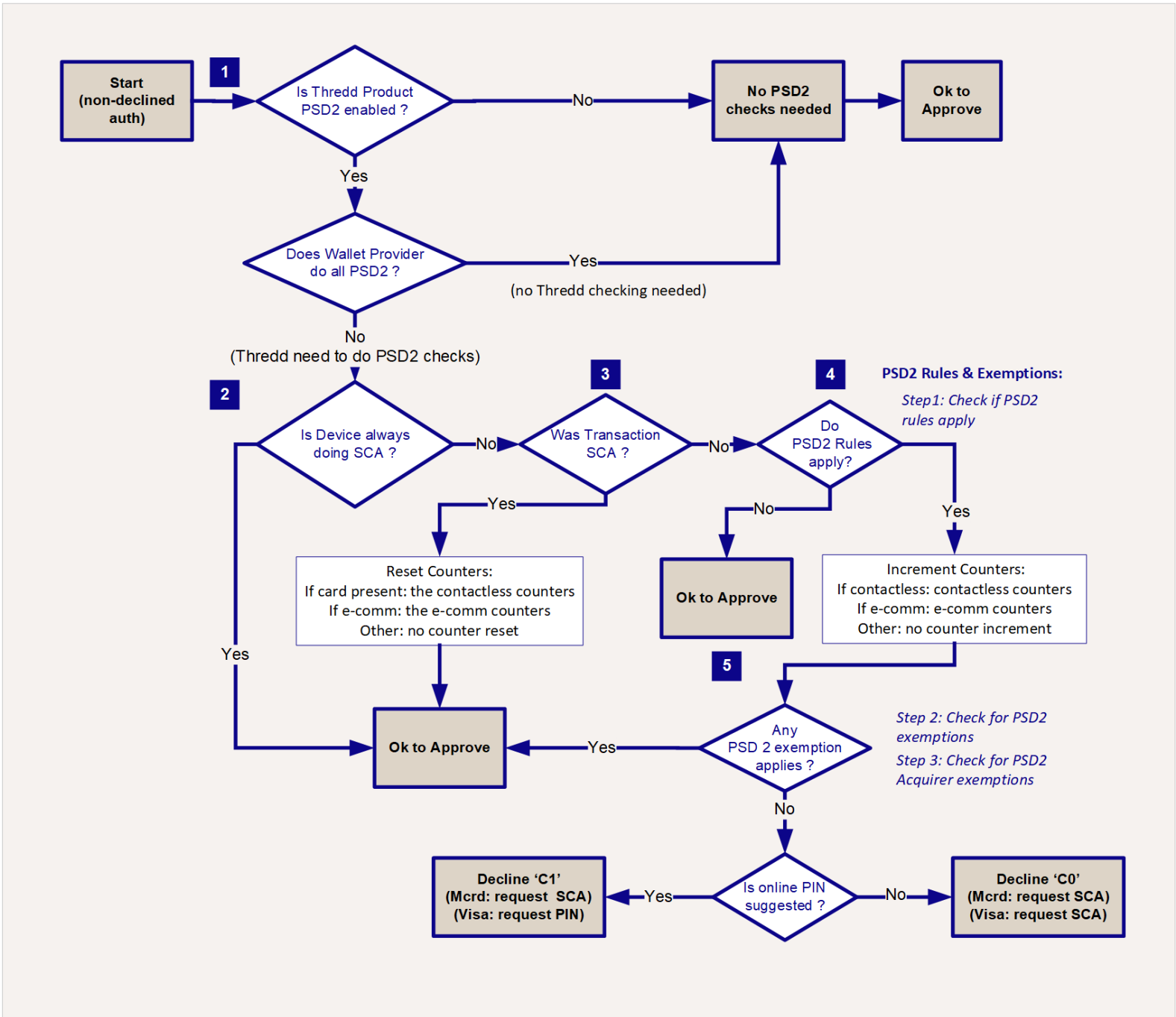


Figure 1: Transaction Checks under PSD2 (for Payment Authorisation)

The numbers in orange in the figure above correspond to the steps described below:

1. Assuming the payment authorisation transaction has passed all other Thredd checks and has not been declined, then Thredd checks for the following conditions:
    - The Thredd Product is not enabled for PSD2.
    - The Wallet Provider (e.g., Apple Pay) manages the PSD2 checks (i.e., does SCA on their end).

    If either condition applies, then Thredd does not need to do PSD2 checks. Thredd can approve the transaction (provided that there is no other reason to decline).

    If none of above conditions apply, Thredd continues with the PSD2 SCA checks.
2. If the cardholder's device does the SCA checks, then the transaction can be approved.
3. If the cardholder's device does not do the SCA checks, then Thredd checks whether SCA has been done (see SCA Checks):
    - For e-commerce 3D-secure transactions, we can optionally configure your programme so that Thredd only considers the transaction as SCA if the cardholder is challenged (asked to verify their identity via 3D secure) during an online (e-commerce) transaction.
    - If SCA has been done, then Thredd resets the SCA counters (either e-commerce or contactless) and can approve the transaction.

      Note: If required, you can also manually reset the SCA counters using the Thredd API. For details see Reset Counters.

4. If SCA has not been done, then Thredd continues with some additional checks (as described in PSD2 Rules and Exemption Checks; a summary is provided below):
    a. Thredd checks whether the PSD2 rules apply (see Step 1: Check if PSD2 Rules Apply)
        - If PSD2 rules do not apply, then the transaction can be approved (provided that there is no other reason to decline).
        - If PSD2 rules apply, then increment the SCA counters.
          Thredd continues with the next check.
    b. Thredd checks whether any PSD2 exemptions apply (see Step 2: PSD2 Exemption Checks and Step 3: PSD2 Acquirer Exemption Checks).
    c. If an exemption applies, the transaction can be approved (provided that there is no other reason to decline).
    d. If no exemption applies, the transaction is soft declined. See Soft Declines.

SCA Checks

This section provides further details of Strong Customer Authentication (SCA) checks which can be carried out as part of the PSD2 Transaction Checking process. See the figure below.

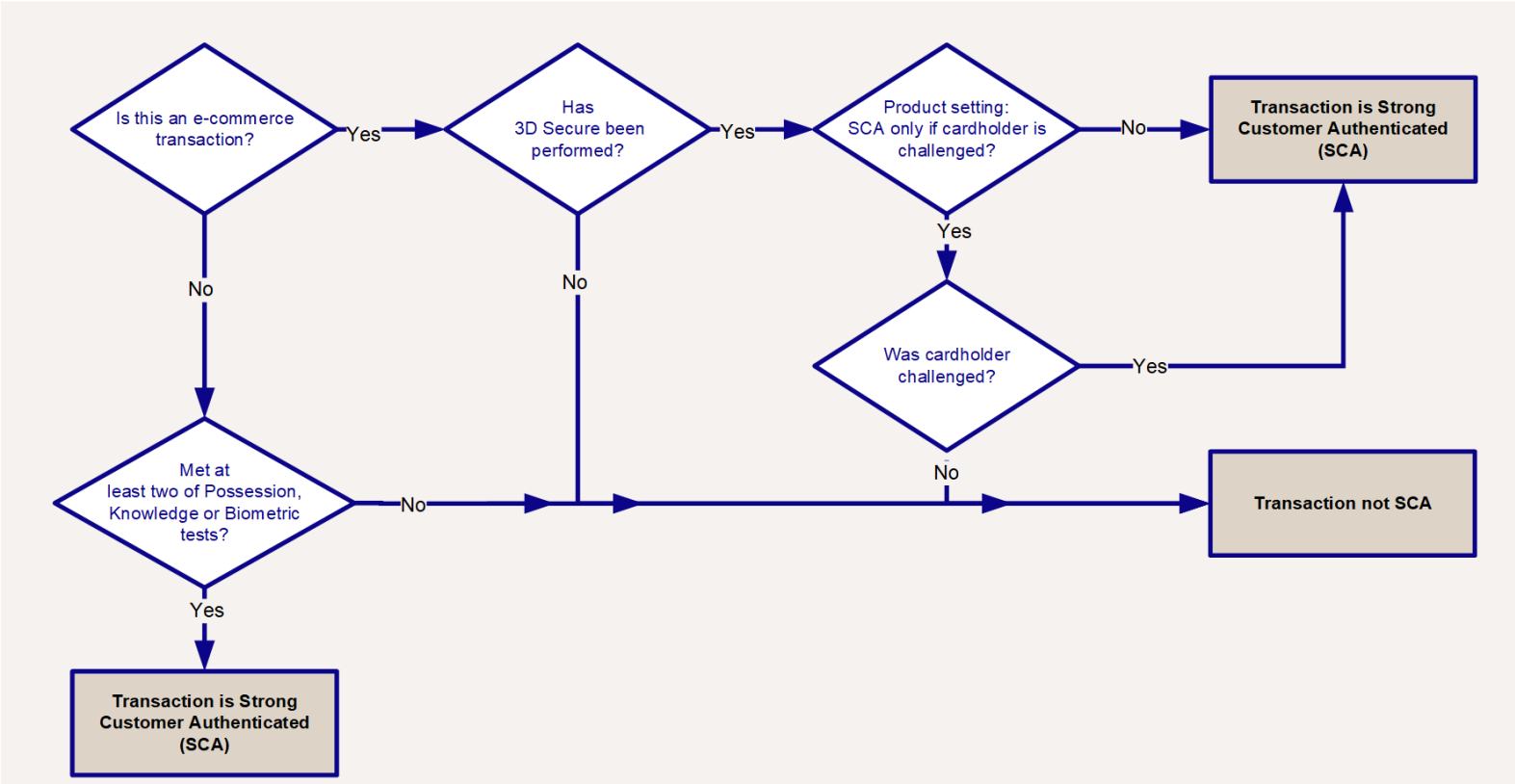


Figure 2: Strong Customer Authentication (SCA) Checks

For details of where SCA checks fit into the overall PSD2 checking process, see PSD2 Transaction Checks.

The SCA checks are run as follows:

1. Check whether this an e-commerce transaction.
2. If this is not an e-commerce transaction, then check that at least two of Possession, Knowledge or Biometric tests are met.

   If at least two tests are met then the transaction is considered as strong customer authenticated (SCA), otherwise it is considered as not SCA.
3. If this an e-commerce transaction then check whether the transaction has gone through 3D Secure checks.
   - If no 3D Secure checks were performed, then the transaction is considered as not SCA.
   - If 3D Secure checks were performed, then check whether the PSD2 product setting *3DS is SCA only if cardholder is challenged* is enabled.

     If enabled, and the cardholder was challenged, the transaction is treated as SCA.

     If enabled, but the cardholder was not challenged, then the transaction is considered as not SCA.

Note: We recommend that your 3D secure cardholder challenge meets the PSD2 requirements (where the cardholder must complete at least two of the Possession, Knowledge or Biometric tests). For more information, see the 3D Secure Guide.

PSD2 Rules and Exemption Checks

The figure below provides a summary of the key checks that Thredd performs on an incoming payment authorisation transaction, to determine whether the PSD2 rules apply and if there are any exemptions from the PSD2 rules.

Note: These checks are done as part of the full PSD2 Transaction Checks.

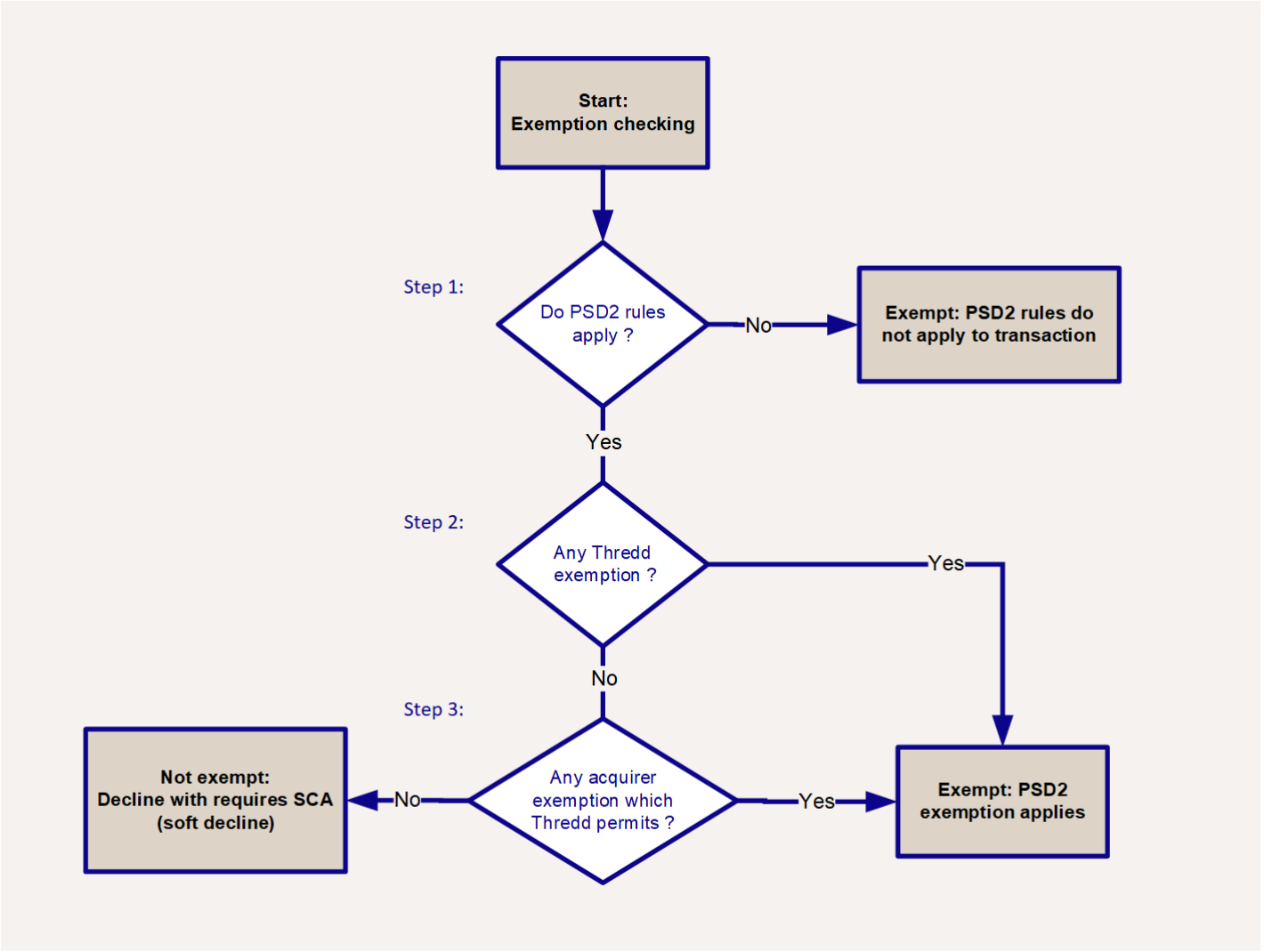


Figure 3: PSD 2 Checks Performed by Thredd - Summary View

Note: For a more detailed process flow which breaks down steps 1-3 above, see Detailed Thredd PSD2 Exemption Checks Workflow.

There are three main exemption checks which are applied to the transaction:

- Step 1: Check if PSD2 Rules Apply
- Step 2: Check for PSD2 Exemptions
- Step 3: Check for PSD2 Acquirer Exemptions

Step 1: Check if PSD2 Rules Apply

PSD2 checks are required for this transaction if all the following are true:

- This an authorisation request (MTID 0100)
- PSD2 compliance is enabled for the Thredd Card product
- The transaction is not set up as an MDES/VDEP payment token or
  the transaction is set up as an MDES/VDEP payment token, but checks are done by Thredd
- The transaction has not already been declined

If all the above are true, then Thredd tests whether the PSD2 rules apply as shown in the figure below:

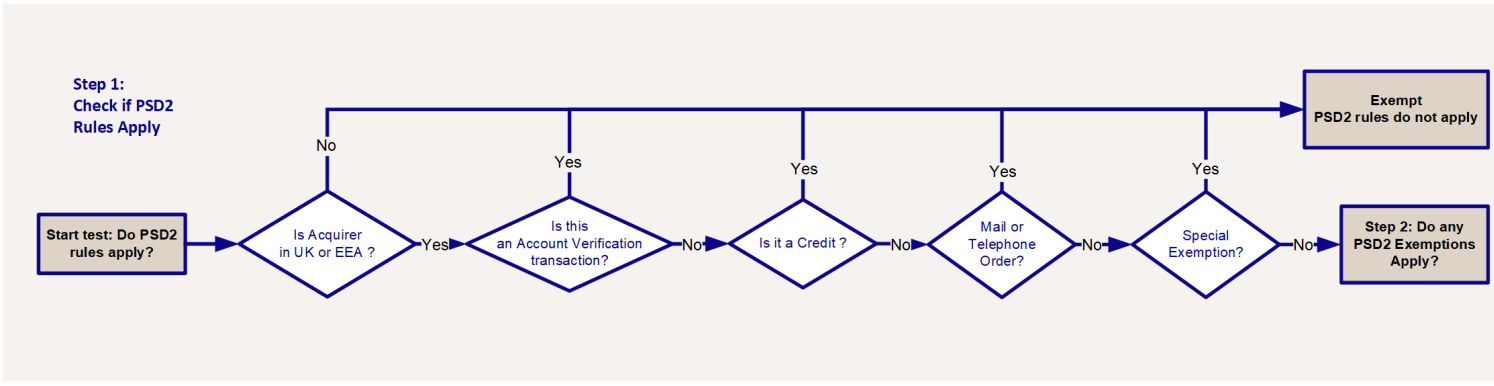


Figure 4: PSD2 Check Step 1: Exempt from PSD2 Rules

The PSD2 rules do not apply to the following types of transactions:

- The Acquirer is outside of the UK or EEA[1]
- Account Verification transactions
- Credit transactions
- Mail and Telephone Order (MOTO) transactions
- Special exemptions for cardholder present transactions on specific Merchant Category Codes (MCCs) such as hotel and car rental merchants. (Exemption flags must first be set in the Thredd system.)

If any of these conditions apply to the transaction, then it is treated as out of scope of the PSD2 regulations.

If none apply, then Thredd performs Step 2: Check for PSD2 Exemptions.

[1] If the card issuer/BIN is outside of the UK/EEA they would typically disable their Thredd card product for PSD2 checks.

Step 2: Check for PSD2 Exemptions

In this step Thredd checks for the following PSD2 transaction exemptions:

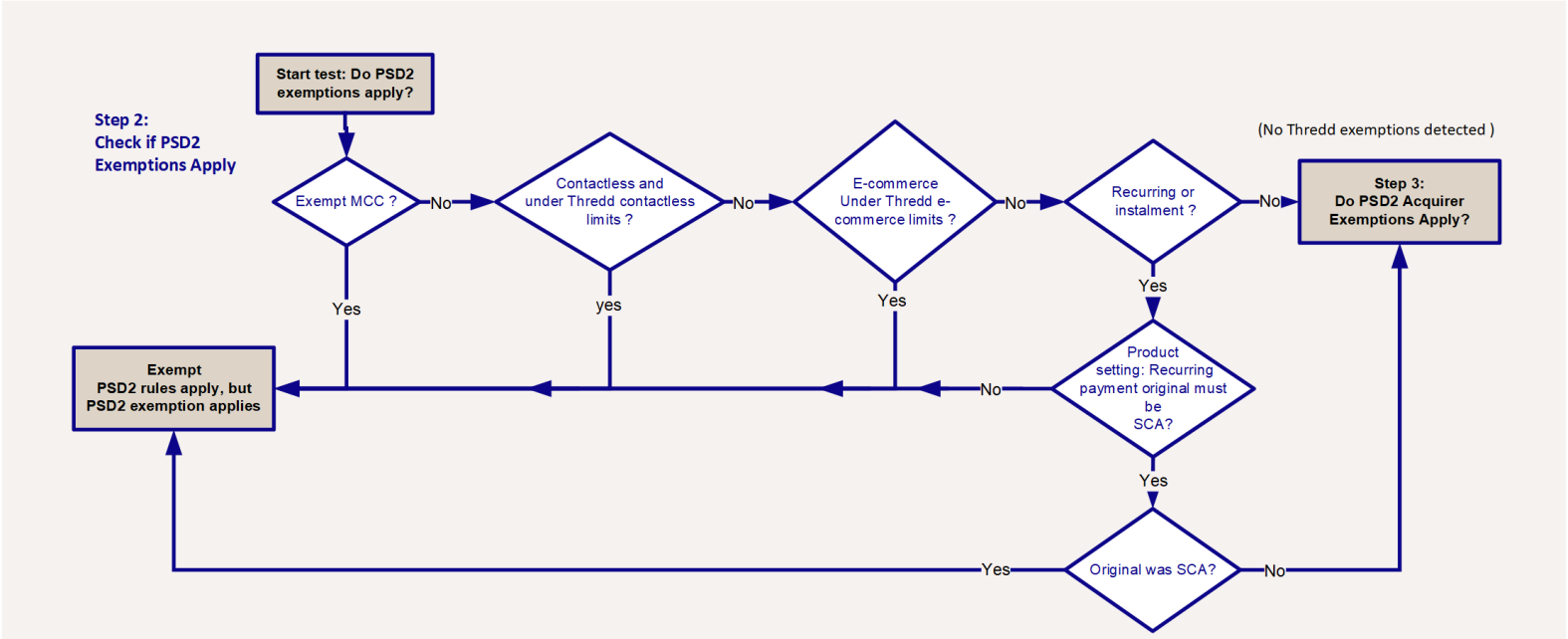


Figure 5: PSD2 Check Step 2 : Determine if any PSD2 Exemptions Apply

The following exemption checks are made:

- Exempt Merchant Category Codes (MCC)[1] - for example, Commuter Transport and Parking which are exempt from PSD2 for cardholder-present transactions at unattended terminals[2]. For details, see Which Merchant Category Codes are Exempt from SCA?
- Transaction is Contactless and the transaction value is under the Thredd Contactless limits
- Transaction is e-commerce and the transaction value is under the Thredd e-commerce limits
- Transaction is a Recurring Payment or instalment payment[3]

If none of these exemptions apply, then Thredd performs Step 3: Check for PSD2 Acquirer Exemptions.

---

[1] Thredd only applies the MCC exemption where the cardholder is present (we ignore the terminal unattended status, as this is often incorrectly set by the acquirer).

[2] We can optionally configure your programme to apply MCC exemptions to the following: Hotel merchants and Car rental merchants doing PAN key entry or manual or manual, cardholder present (or unknown) transactions.

[3] We can optionally configure your programme to check that the original payment was SCA before applying the exemption.

Step 3: Check for PSD2 Acquirer Exemptions

In this step Thredd checks for any PSD2 Acquirer Exemptions. Acquirer exemptions include low value transactions, transaction risk analysis and recurring transactions, which enable the acquirer to process as many transactions as possible without Strong Customer Authentication.

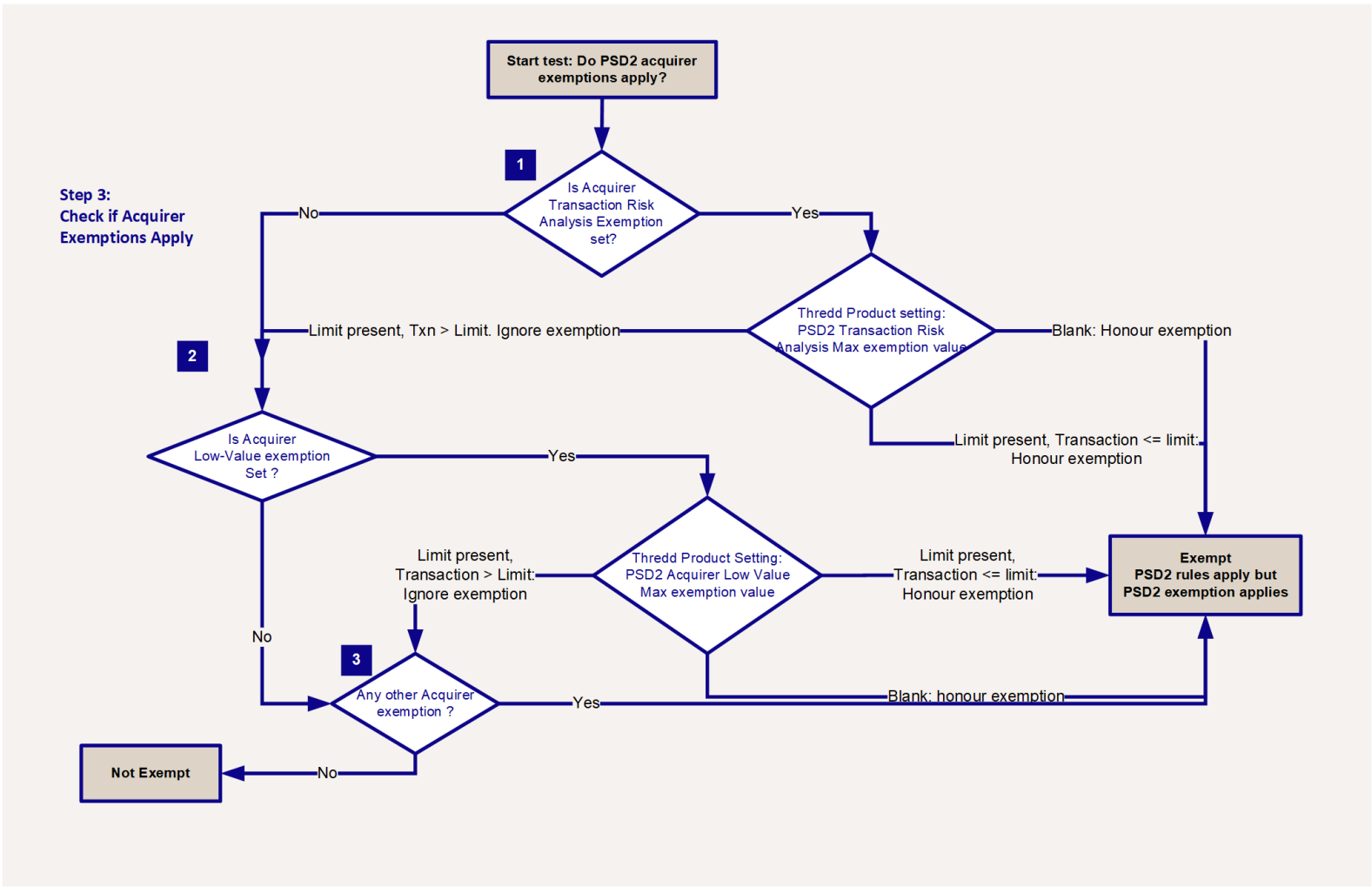


Figure 6: PSD2 Checks Step 3: Acquirer Exemptions

The numbers in orange in the figure above correspond to the steps described below.

The following acquirer exemption checks are made:

1. Is the *Acquirer Transaction Risk Analysis Exemption* specified in the transaction?

   If no, then the next check is carried out (see step 2 below).

   If yes, then Thredd checks your product's *Acquirer Transaction Risk Analysis Exemption* transaction limit:

   - If this limit is blank (Thredd has not set a limit) for your product, then the transaction is exempt
   - If the transaction value is below or equal to the limit, then the transaction is exempt
   - If the transaction value is above the limit, then the exemption is ignored and the next check is carried out (see step 2 below).

2. Is the *Acquirer Low-Value Exemption* set for your product?

   If no, then the next check is carried out (see step 3 below).

   If yes, then Thredd checks your product's *Acquirer Low-Value Exemption* transaction limit:

   - If this limit is blank (Thredd has not set a limit) for your product, then the transaction is exempt
   - If the transaction value is below or equal to the limit, then the transaction is exempt
   - If the transaction value is above the limit, then the exemption is ignored and the next check is carried out (see step 3 below).

3. Are there any other acquirer exemptions? (see PSD2 Acquirer Exemptions)

   - If no, then the transaction is not exempt
   - If yes, then the transaction is exempt

What happens after exemption checking is complete?

For a transaction that was not strongly authenticated, then after exemption checking is complete:

- If no exemptions apply, then Thredd soft declines the transaction. See Soft Declines.
- If any exemptions apply, then Thredd can approve the transaction (provided there are no other reasons to decline).

For details of the full end-to-end transaction checking process, see PSD2 Transaction Checks.

Detailed Thredd PSD2 Exemption Check Workflow

The figure below describes the full Thredd PSD2 exemption checks. Click on each step for details.

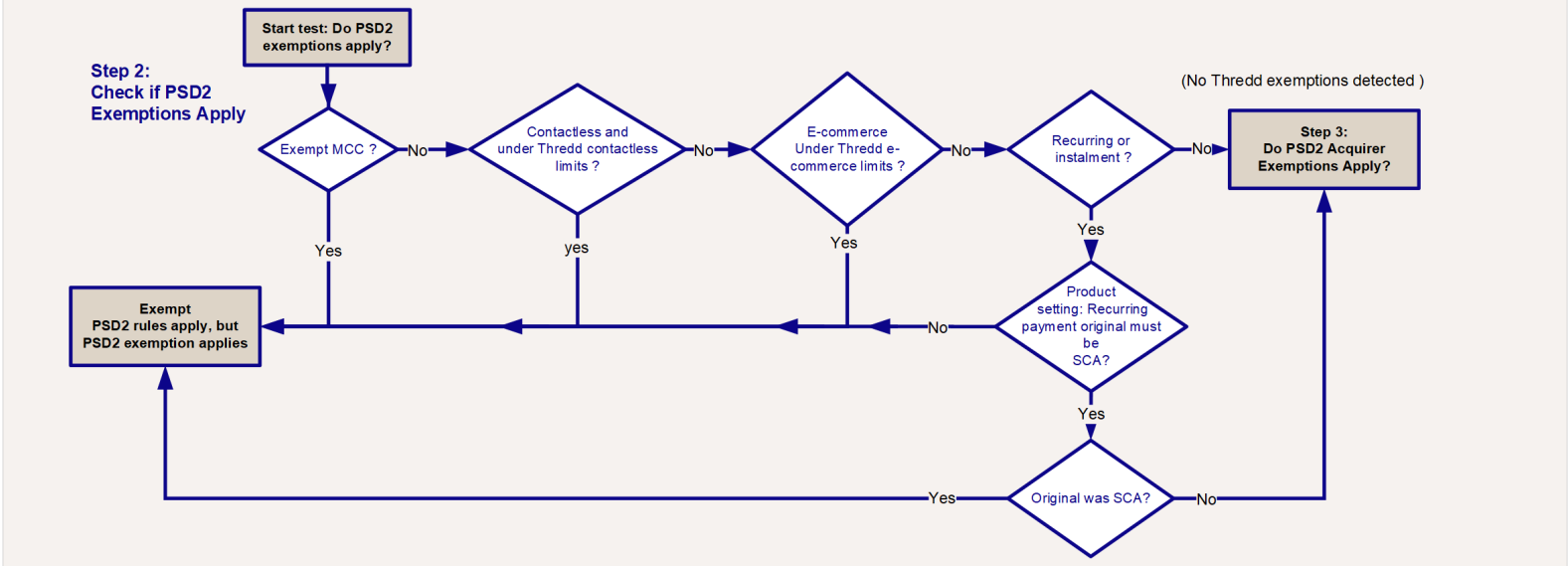


Figure 7: PSD 2 Checks Performed by Thredd - Detailed View

Identifying the SCA Status

This section provides details of how to check the SCA status of a transaction.

Identifying the SCA Status In EHI

You can use messages received from the External Host Interface (EHI) to identify the SCA status of a transaction.

Note: If you do not have access to EHI, please contact your Account Manager, who can advise you on bespoke reports that may be available.

Identifying if a transaction is Point of Sale (POS) or e-commerce (remote)

Use the EHI field `GPS_POS_Data`. Positions 1, 2 and 3 provide information about the type of transaction.

For more information, see the EHI Guide > GPS_POS_Data.

Identifying if Thredd considered the transaction SCA

The EHI `GPS_POS_Data` field positions relevant to SCA include: 18,19,20,21,22,23,25 and 26.

If the transaction is flagged as non-SCA, then the exemption that permitted the non-SCA transaction is specified in the EHI `GPS_POS_Data` field `ExemptFromSCA` indicator.

For more information, see the EHI Guide > GPS_POS_Data.

Note: If 3D Secure occurred and Thredd considered the 3D Secure transaction as SCA, then the transaction will be automatically flagged as having passed the SCA Knowledge and Possession tests.

Identifying the SCA Status In Smart Client

You can identify the SCA status of a transaction in Smart Client as follows:

1. Log in to Smart Client and select **Card Activity > View Transactions**.
2. Right-click the transaction you want to view and select **View Transaction Details**. See the example below

> **Note:** Some details have been removed for data protection.

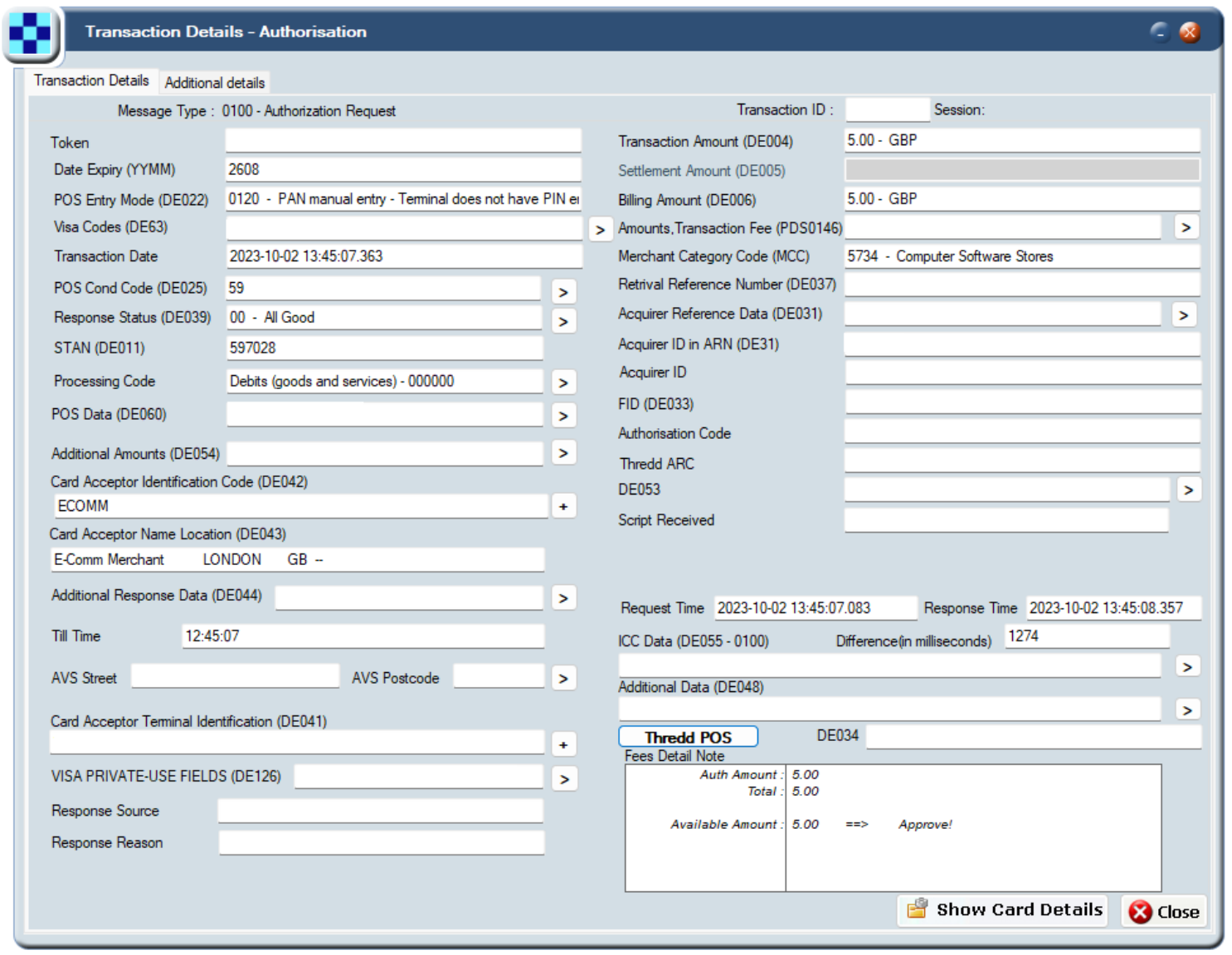


Figure 8: Transaction Details Screen in Smart Client

3. To view the Thredd_POS data details, click **Thredd POS** (near bottom-right of the screen) to display the **Thredd POS Data** screen.

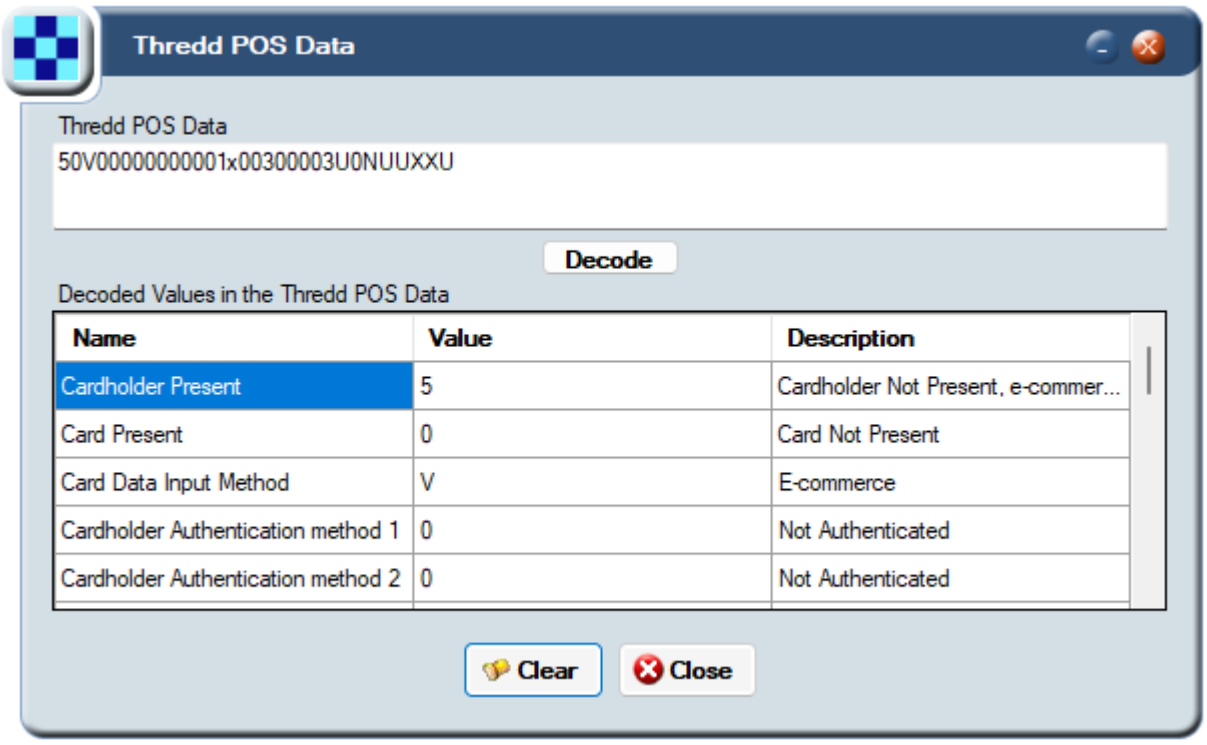


Figure 9: Thredd POS Data in Smart Client showing some of the SCA information

PSD2 Product Settings

Thredd PSD2 settings for your card product are set up at a Product Master level. See the example below.

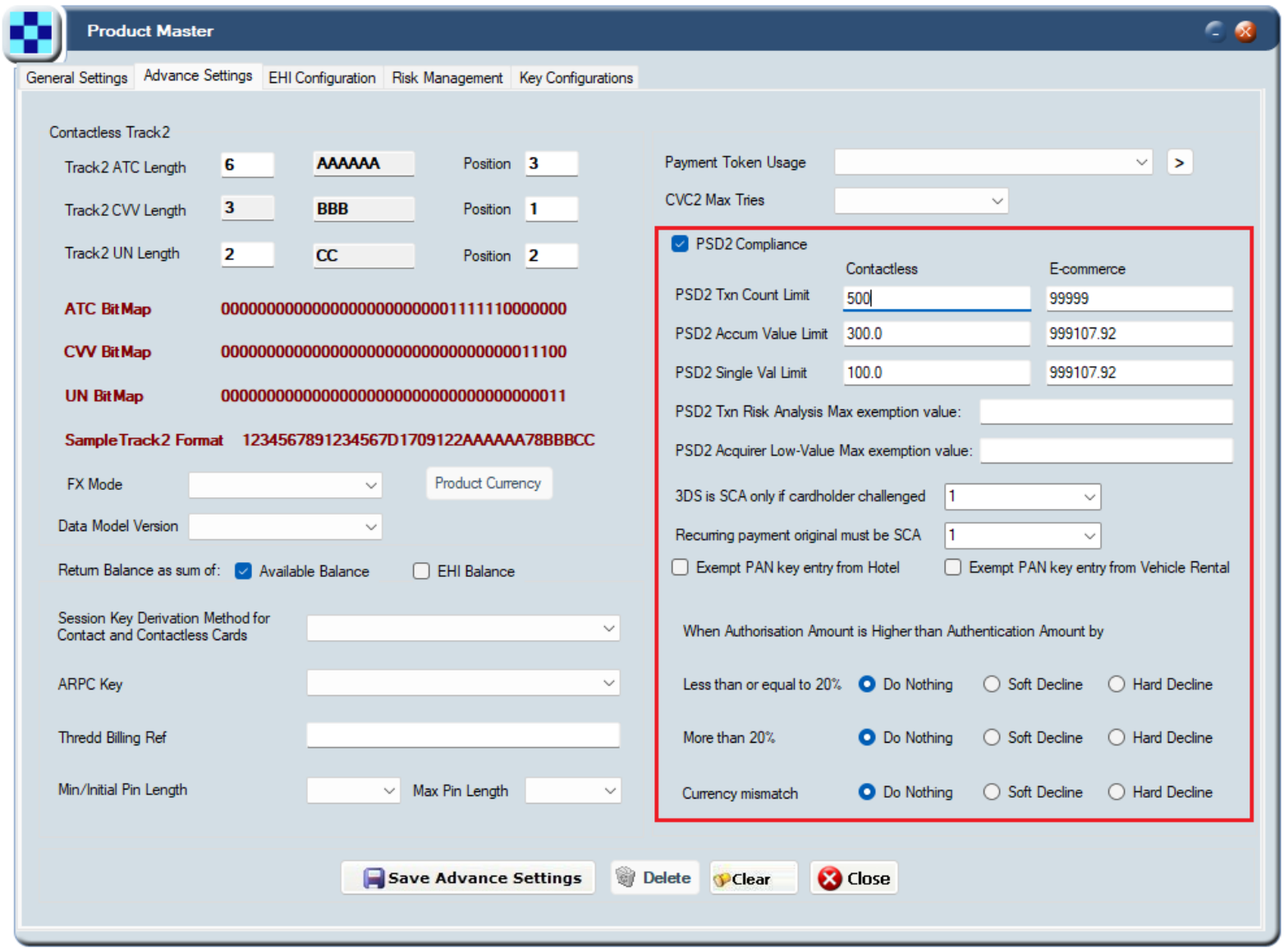


Figure 10: PSD2 Settings on the Product Master screen in Smart Client

Note: This screen is an internal Thredd screen available to Thredd administrators only. For further information, please contact your Account Manager.

Refer to the table below for details. These exemption checks are based on SCA Exemptions (EBA Articles 11, 15, 16).

Setting	Description
PSD2 Compliance	Indicates whether PSD2 complance checks are enabled for this card product.
PSD2 Txn Count Limit	The cummulative transaction count upper limit that is exempt from PSD2 (e.g., 5). If the number of cummulative transactions is above this limit then Thredd considers the transaction as within scope of PSD2. (See SCA Exemptions: Articles 11 and 15.) Separate limits can be configured for Contactless and E-commerce transactions.
PSD2 Accum Value Limit	The accumulated transaction upper limit that is exempt from PSD2 (e.g., 100.00 EUR). If the accumulated transaction amount is above this limit then Thredd considers the transaction as within scope of PSD2. (See SCA Exemptions: Articles 11 and 15.) Separate limits can be configured for Contactless and E-commerce transactions. The amount limits are in the primary billing currency of the card product.
PSD2 Single Value Limit	The transaction amount upper limit for a single transaction that is exempt from PSD2 (e.g., 30.00 EUR). If the transaction amount is above this value then Thredd considers the transaction as within scope of PSD2. (See SCA Exemptions: Articles 11 and 15.) Separate limits can be configured for Contactless and E-commerce transactions. The amount limits are in the primary billing currency of the card product.

Setting	Description
PSD2 Txn Risk Analysis Max exemption value	Maximum permitted transaction value (in primary billing currency of the product) up to which an Acquirer claimed *Transaction Risk Analysis* exemption will be honoured. See Step 3: Check for PSD2 Acquirer Exemptions.
PSD2 Acquirer Low-Value Max exemption value	Maximum permitted transaction value (in primary billing currency of the product) up to which an Acquirer claimed *Low Value* exemption will be honoured. See Step 3: Check for PSD2 Acquirer Exemptions. **Note**: Thredd recommends you set this to zero (this will ensure that only Thredd does the low value exemption test).
3DS is SCA only if cardholder is challenged	For e-commerce 3D Secure transactions, only consider the transaction as SCA if the cardholder is challenged (asked to authenticate during a 3D Secure session).
Recurring payment original must be SCA	For recurring transactions, only apply the exemption if the original transaction was SCA.
Exempt PAN key entry from Hotel	Treat hotel merchants (MCC 3501-3999, 7011) doing PAN key entry or manual cardholder present (or unknown) transactions as exempt from SCA.
Exempt pan key entry from Vehicle Rental	Treat car rental merchants (MCC 3MCC 3351-3500, 7512,7513,7519) doing PAN key entry or manual cardholder present (or unknown) transactions as exempt from SCA.
When Authorisation Amount is higher than Authentication Amount by: Less than or equal to 20% More than 20% Currency Mismatch	This setting is used when checking the transaction amount value and currency provided during a 3D secure Authentication session with the transaction amount value and currency that has been authorised. If there is a mismatch, then Thredd can: • Soft Decline - we return a soft decline code which indicates to the merchant to try again using SCA • Hard Decline - we return a hard decline code which indicates to the merchant not to try again • Do Nothing - Thredd does not decline the transaction **Note**: This check is used to comply with the PSD2 SCA dynamic linking requirements (see PSD2 Dynamic SCA Linking).

Impact of the PSD2 Rules

For card products that are enabled for PSD2 checking, the table below describes the impact on transactions if the PSD2 rules apply.

Note: The rows highlighted below indicate the types of transactions where you should expect to see declines.

Card Data Input Method	Cardholder Verification Method	Impact on card approvals and declines if the PSD2 rules apply
PAN Key Entry (with cardholder present at merchant) *	Any	Nearly all transactions will be declined, as few exemptions apply.
Mail Order / Telephone order / Recurring	Any or none	PSD2 rules do not apply: transactions should be approved (provided there are no other reasons to decline).
Magnetic Stripe *	Any	Nearly all transactions will be declined, as few exemptions apply.
EMV contactless	No verification	Transactions will only be approved if an exemption applies. For example: low value contactless exemption. To reset the low value contactless counters, an EMV contact + PIN transaction is required.
EMV contact **	None or signature	Nearly all transactions will be declined, as few exemptions apply.
EMV contact	PIN	Will always pass SCA checks, therefore will not be declined due to PSD2 rules.
e-commerce (including Credential-on-file)	None	Transactions will be approved, but only up to the configured e-commerce limits. A 3D-secure transaction is required to reset the counters.

Note:

* PAN Key Entry and Magnetic Stripe methods do not pass the possession test, which normally means the transaction cannot be SCA.

** EMV contact with ‘None’ or ‘signature’ cardholder verification methods does not pass the Knowledge test, which normally means the transaction cannot be SCA.

Dealing with a Decline

What happens when there is a soft decline depends on the reason for the decline. For example:

Reason for decline	Actions you can take
PAN Key Entry (with cardholder present at merchant)	Raise with your Card Scheme or the Merchant to double-check whether the cardholder was actually present. If not, then the acquirer should update how they flag the transaction. The cardholder would then need to try again. Advise the cardholder/merchant to repeat the transaction using Chip and PIN.
Magnetic Stripe	Advise the cardholder/merchant to repeat the transaction using Chip and PIN or Contactless.
EMV contact with none or signature cardholder verification	Advise the cardholder/merchant to repeat the transaction using Chip and PIN or Contactless.
EMV contactless with no cardholder verification	Advise the cardholder/merchant to repeat the transaction using Chip and PIN. Alternatively, if the Program Manager has verified that the real cardholder is still in possession of the card and this transaction is within the Contactless single value limit, then they can use the Clear Accumulator (Ws_ResetAccumulator) web service call to reset the Contactless counters for the card.
E-commerce where the Merchant did not do 3D Secure	If the Program Manager has verified that the real cardholder is attempting the transaction, and this transaction is within the e-commerce single value limit, then they can use the Clear Accumulator (Ws_ResetAccumulator) web service call to reset the e-commerce counters for the card. The cardholder would then need to try again.

For more information on soft declines, see Soft Declines.

PSD2 Acquirer Exemption Types

This section provides details of how acquirers are able to flag transactions as exempt from SCA checks or delegate authority for SCA to their merchant.

Acquirers can use the following exemptions in order to process transactions without Strong Customer Authentication (SCA):

- Low value transactions
- Transaction risk analysis
- Recurring transactions
- Delegated authentication
- Other exemptions

Using these exemptions can help acquirers to bypass SCA checks, reducing the number of abandoned customer purchases and improving conversion. Acquirers will try to balance between security and customer ease of use, based on a risk assessment and using the available exemptions. This requires a continuous analysis of transaction and fraud data as well as a continuous improvement of risk management.

For details of which acquirer exemptions are verified and which are accepted, see Step 3: Check for PSD2 Acquirer Exemptions.

Note: You can find out whether any acquirer SCA exemptions apply using the `GPS_POS_Data` field, position 23: *Acquirer Exempt from SCA indicator*. See the EHI Guide > GPS_POS_Data.

Low Value Transactions

Low value transactions are payments with a value of less than 30 EUR*. The total cumulative value of all transactions since the last Strong Customer Authentication must not exceed EUR 100* and no more than five transactions in total may have taken place since the last SCA.

Note: The card issuer needs to track the number of total transactions and the cumulative value of a card, since the acquirer will not have this data. Acquirers will be unaware of transactions on other acquirers with the same card, so will not be in a position to check for the cumumulative total limit since the last SCA. For this reason, Thredd recommends that you set your Thredd card product *PSD2 Acquirer Low-Value Max exemption value* to 0.00. See PSD2 Product Settings.

* Values may vary per country, as set by the local Financial Regulator.

Transaction Risk Analysis

In transaction risk analysis, the exemption rule depends on the acquirer's fraud rate, in combination with the transaction value. For transactions of more than 500 EUR*, the Transaction Risk Analysis no longer applies. For transaction values between 250 and 500 EUR*, the acquirer must prove a fraud rate of no more than 0.01 percent in order to be allowed to process a transaction without Strong Customer Authentication. For lower transaction values, slightly higher fraud rates are tolerated (up to a maximum of 0.13%).

Note: Thredd suggests you consider set a limit for this exemption, if you want to avoid honouring this exemption for very large amounts. See the *PSD2 Txn Risk Analysis Max exemption value* field in PSD2 Product Settings.

* Values may vary per country, as set by the local Financial Regulator.

Recurring Transactions

Recurring transactions are multiple transactions processed at predetermined intervals, representing an agreement between a customer and a merchant to take payments over a period of time. Typically, SCA is performed on the first transaction, while subsquent transactions are treated as cardholder not present and not subject to SCA: the merchant uses card details stored on file and processes the subsequent transactions through their acquirer as a *recurring transaction*.

Tip: Only transactions in which the amount and the payment recipient match the first transaction are recognised as recurring transactions.

Delegated Authentication

In delegated authentication, the merchant carries out strong customer authentication. This provides for an improved customer experience, where a PSD2 and SCA compliant one-click checkout is possible.

Other Exemptions

Below are additional exemptions that may be flagged by the acquirer:

- **Secure Corporate Payment** - the transaction is part of a secure corporate payment transaction (e.g., using a qualifying commercial card where the transaction was initiated in a secure corporate environment).
- **Merchant Initiated Transaction** - the transaction has been initiated by the merchant without interacting with the cardholder (e.g., London Underground transport billing after the journey is complete).
- **Authentication Outage Exemption** - where the merchant or acquirer was unable to complete authentication due to an outage (e.g, was unable to connect to the 3D Secure directory server).
- **Trusted Merchant (identified by Acquirer)** - the merchant is part of the acquirer's trusted merchant scheme, which enables transactions to be completed without SCA.

Soft Declines

Where a transaction does not meet the PSD2 SCA rules, Thredd soft declines and sends back the instruction to the merchant to authenticate the cardholder using SCA.

Soft Decline - Card Not Present (e-Commerce)

For a card not present e-commerce transaction, the merchant should retry using 3D Secure.

The figure below summarises the transaction process, including what happpens when Thredd soft-declines.

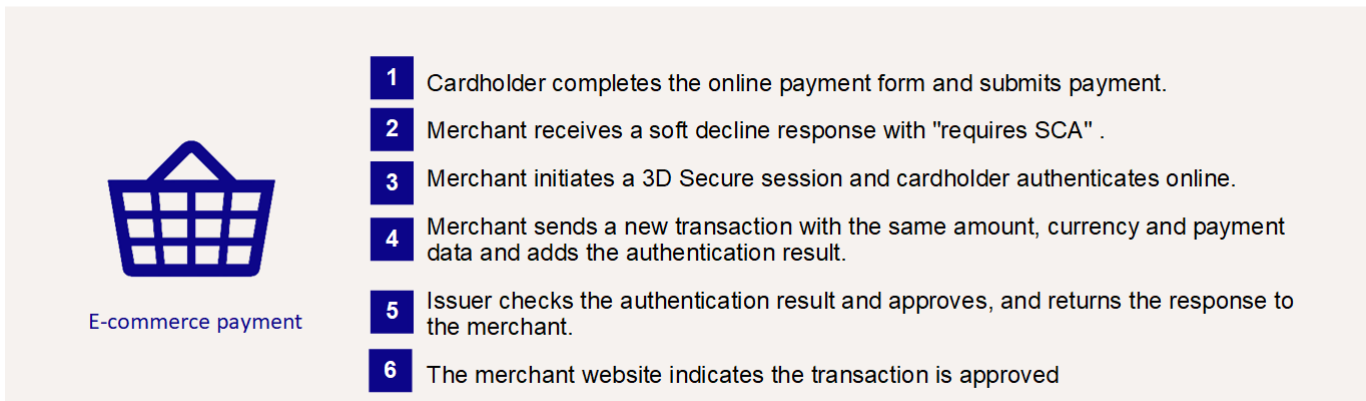


Figure 11: Soft Decline - Card Not Present Transaction

Soft Decline Card Present (Contactless)

For a card present contactless transaction, the POS terminal either:

- asks the cardholder to insert their card and enter their PIN. The terminal then sends a new transaction that has been PIN verified

  -or-

- asks the cardholder to enter their PIN. The terminal then sends a new transaction, for the same amount and with same chip data, but this time including the online PIN.

Note: To support the soft decline flow, the POS terminal must be able to read the card chip and accept a PIN.

The figure below summarises the transaction process, including what happpens when Thredd soft-declines.

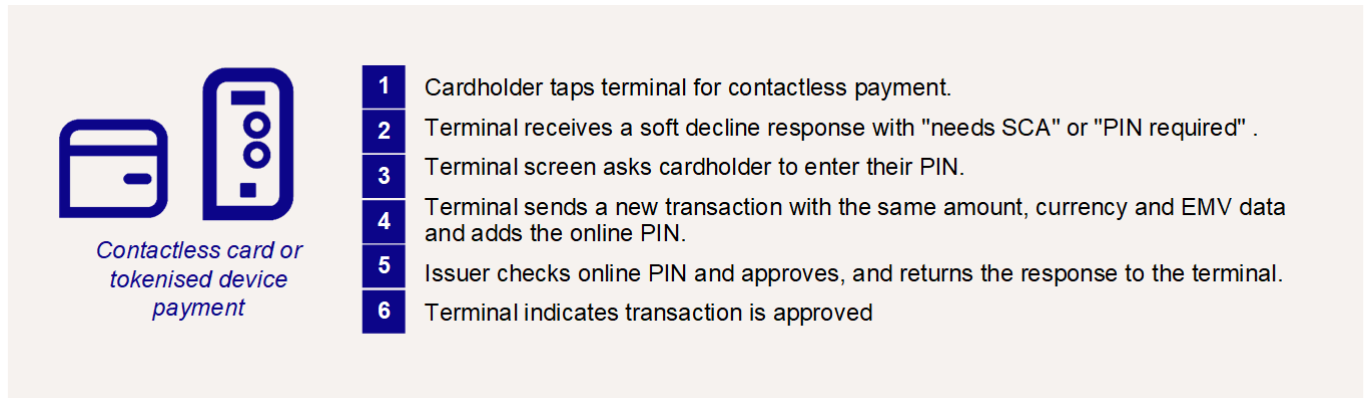


Figure 12: Soft Decline - Card Present Transaction

Soft Declines and Thredd Response Codes

For details of Thredd response codes for soft declines, see the table below.

Scenario	Thredd internal response code	Mastercard response code sent	Visa response sent
Card present, terminal supports PIN	C1	65 requires SCA	70 PIN required

Scenario	Thredd internal response code	Mastercard response code sent	Visa response sent
		With single tap response = Yes ((i.e., repeat transaction with online PIN)	
Card present, terminal does not support PIN	C0	65 requires SCA	1A SCA required
Card not present (e.g. e-commerce)	C0	65 requires SCA	1A SCA required

Note: For Mastercard, the *single tap response = yes* (i.e. repeat transaction with online PIN) is sent if the terminal indicates it supports this and it was a contactless transaction. The single tap response can also be sent for internal response C0, if the terminal indicates it supports repeating the transaction with online PIN.

Reset Counters

You can use the Thredd API to reset transaction and amount counters (since the last strongly-cardholder-authenticated transaction) on a card or payment-token, to re-enable transactions which are blocked as a result of the transaction and amount counters exceeding the defined maximum limits for not secure enough transactions.

- To reset the counters for a contactless transaction, use the **Clear Accumulator** (Ws_ResetAccumulator) web service, with AccumulatorType = 1.
- To reset the counters for an e-commerce transaction, use the **Clear Accumulator** (Ws_ResetAccumulator) web service, with AccumulatorType = 2.

For more information, see the Web Services Guide > Clear Accumulator.

Frequently Asked Questions

Thredd Handling of PSD2 SCA Requirements

Q. Are Thredd systems configured not to request SCA for out of scope of SCA transactions?

Yes, GThredd Systems are configured to not request for SCA for out of scope of SCA transactions (where the PSD2 rules do not apply). See Step 1: Check if PSD2 Rules Apply.

You can identify Thredd flagged Out-of-scope SCA transactions using the ExemptFromSCA indicator in EHI field GPS_POS_Data.

Q. Do Thredd systems decline transactions based on the SCA status?

Yes, if PSD2 checking is enabled for the Thredd Card Product, then Thredd will soft decline all transactions where PSD2 rules apply and where the transaction is non-SCA and no exemption applies. See PSD2 Transaction Flow.

Note: If PSD2 rules apply and there is no applicable exemption, then we will *soft decline* (decline asking the merchant to repeat the transaction using SCA this time). This should therefore result in a second transaction which is SCA and can therefore be approved.

Q. How can I identify the SCA status of a transaction?

You can use messages received from the External Host Interface (EHI) to identify the SCA status of a transaction. You can also use Smart Client. See Identifying the SCA Status.

PSD2 Exemptions

Q. What is the authorisation exemption for low-value transactions?

The following exemptions apply:

- E-commerce transactions of up to EUR 30.00, and cumulatively not exceeding EUR 100.00 or 5 transactions.
- Contactless transactions of up to EUR 50.00, and cumulatively not exceeding EUR 150.00 or 5 transactions.

Note: The exemption limits may vary, depending on the values set by your country's Financial Regulator.

Q.What type of transactions are out of scope for SCA?

The following transactions are not included in the PSD2 rules for SCA:

- Mail and Telephone Order (MOTO)
- One-Leg-Out transactions - occurs when one of the payment service providers (either the payer or payee) is outside the European Union (EU). If the Acquirer is from outside the EU and the payer is from the EU, the Acquirer does not need to comply with PSD2 regulations.
- Anonymous transactions - such as for prepaid gift cards where the cardholder's identify is not known
- Credit transaction - such as credit vouchers and Original Credit Transactions (OCT)
- Refunds

The following merchant initiated transactions are also exempt (where the cardholder is not present):

- Installment/prepayment
- Recurring
- Unscheduled credential on-file
- Incremental
- Delayed charges

- No-show
- Reauthorisation
- Resubmission

Q. Which Merchant Category Codes are Exempt from SCA?

Refer to the table below for SCA exemptions.

Note: These exemptions only apply to card present transactions (i.e., cardholder present and unattended terminal transactions) and excludes all cases where the cardholder is not present (i.e., mail-order, telephone-order, recurring and e-commerce transactions).

MCC	Description
4111	Local and suburban commuter passenger transport, including ferries.
4112	Passenger railways.
4131	Bus lines.
4784	Tolls and bridge fees.
7523	Car parking and parking meters.

We can optionally configure your programme to apply SCA exemptions to hotel merchants and to car rental merchants doing PAN key entry or manual, cardholder present (or unknown) transactions.

MCC	Merchant type
3501-3999, 7011	Hotel merchants
3351-3500, 7512, 7513, 7519	Car rental merchants

Glossary

3

3D Secure

3D Secure (3-domain structure), also known as a payer authentication, is an authentication process involving the issuer's authentication service provider (e.g., Cardinal or Apata) to pre-authenticate the cardholder. This process happens before the Authorisation is sent by the merchant Acquirer, and the critical details from the 3D-secure response are included in the Authorisation message to enable the issuer to prove that 3D-secure authentication was obtained.

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.

Anonymous Transactions

Transactions such as for prepaid gift cards where the cardholder's identify is not known

Authentication

This includes checks to verify the cardholder's identity, such as PIN, CVV2 and CAVV, as well as 3D Secure authentication.

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.

B

Bank Identification Number (BIN)

The Bank Identification Number (BIN) is the first six numbers on a payment card, which identifies the institution that issues the card. Visa and Mastercard are changing to an eight digit BIN from April 2022.

Biometric Authentication

Biometrics are body measurements and calculations related to human characteristics that are unique to each person (such as face, eyes, voice and fingerprints). Biometrics authentication is used as a form of identification and access control. In practice, this mainly happens on a payment token/DPAN such as a mobile phone, and the cardholder does biometric by the phone checking their fingerprint, before using the phone to do a contactless transaction with it.

C

Card Scheme (Network)

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.

Cardinal Commerce

Cardinal Commerce provide an Access Control Server (ACS) that enables support for the 3D Secure cardholder authentication scheme. Cardinal is now owned by Visa. See: https://www.cardinalcommerce.com

Chip and PIN

Chip and PIN is a verification method used by payment cards which comply with the EMV standard. The cardholder enters a personal identification number (PIN), typically of 4 to 6 digits in length. This number must correspond to the information stored on the chip. This improves the security of the card, since only the cardholder should know the PIN.

E

European Banking Authority (EBA)

The EBA is an independent EU Authority which works to ensure effective and consistent prudential regulation and supervision across the European banking sector.

External Host Interface (EHI)

The External Host Interface provides a facility to enable exchange of data between Thredd and external systems via our web services. All transaction data processed by Thredd is transferred to the External Host side via EHI in real time. For certain types of transactions, such as Authorisations, the External Host can participate in payment transaction authorisation.

F

Financial PAN (FPAN)

The PAN of the card (normally 16 digits), which the Card Scheme (Network) converts when authorisations come through to them from Acquirers on the DPAN. For more information, see the Tokenisation Service Guide.

Fraud Rate

The fraud rate is the percentages of transactions received by the acquirer which are identified as fraudulent. For example, if 10,000 transactions per day are received, and 10 of these are identified as fraudulent, the fraud rate would be 0.01.

H

Hard Decline

A transaction decline which indicates that the card was declined by the issuing bank or card processor due to the card not being valid (e.g., lost, stolen or expired). It indicates to the merchant that they should not retry the transaction on the card.

I

Issuer (BIN Sponsor)

The card issuer or BIN sponsor is a financial organisation authorised to issue cards. The issuer has a direct relationship with the relevant Card Scheme.

M

Mail and Telephone Order (MOTO)

Transaction where payment instruction is taken over the telephone or via a mail order. Since the cardholder is not present, these are classed as "Cardholder Not Present" transactions.

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)

Merchant category codes (MCCs) are four-digit numbers that describe a merchant's primary business activities. MCCs are used by credit card issuers to identify the type of business in which a merchant is engaged.

O

One-Leg-Out transactions

Occurs when one of the payment service providers (either the payer or payee) is outside the European Union (EU). If the Acquirer is from outside the EU and the payer is from the EU, the Acquirer does not need to comply with PSD2 regulations

Online PIN

With online PIN, the PIN is encrypted and verified online by the card issuer. This is in contrast to offline PIN, where the PIN is verified offline by the EMV chip card.

Original Credit Transactions (OCT)

Transaction that can be used to send funds to a card-based account, resulting in a credit of funds to the cardholder's account.

P

Payment Services Directive 2 (PSD2)

PSD2 is an EU Directive which sets requirements for firms that provide payment services. It introduces a number of requirements around how firms treat their customers and handle their complaints, and the data they must report to the FCA.

Point of Sale (POS) Terminal

A hardware device for processing card payments at retail stores. The device has embedded software that is used to read the card's magnetic strip data.

Primary Account Number (PAN)

The card's 16-digit permanent account number (PAN) that is typically embossed on a physical card.

Product Setup Form (PSF)

The Product Setup Form is a spreadsheet that provides details of your Thredd account setup. The details are used to configure your Thredd account.

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

Recurring Transaction

Recurring transactions are multiple transactions processed at predetermined intervals, representing an agreement between a customer and a merchant to take payments over a period of time. Typically, SCA is performed on the first transaction, while subsquent transactions are treated as cardholder not present and not subject to SCA.

S

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 VPN connection to Thredd systems in order to be able to access your account.

Soft Decline

A Soft Decline is a decline response to the terminal or online merchant, indicating that the transaction failed due to being non-SCA. The transaction should be re-attempted with SCA. This may include (for card present transactions) requesting that the terminal authenticates the cardholder using PIN.

Strong Customer Authentication (SCA)

Type of cardholder authentication process where the cardholder is authenticated using a combination of at least two of the following tests: Possession (something the cardholder has), Knowledge (something the cardholder knows) and something they are (such as a fingerprint, face recognition or voice recognition).

U

Usage Group

Group that controls where a card can be used. For example: POS or ATM. For more information, see the Web Services Guide.

W

Wallet Provider

These are providers such as Apple, Android (Google), Samsung etc. who supply the payment apps (also known as Mobile Wallet token requestors).

Document History

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

Version	Date	Reason	Who
1.4	22/03/2024	Updates to content to align with taxonomy updates on our Documentation Portal.	WS
	12/10/2023	Updated Smart Client screen shots in Identifying the SCA Status and PSD2 Product Settings.	MW
	25/07/2023	Added a note to clarify that Merchant Category Code (MCC) exemptions from SCA only apply to transactions where the cardholder is present. See the FAQs.	WS
	07/06/2023	Updated Operations email address to be occ@thredd.com	MW
	27/04/2023	Guide rebrand to new company name and brand identity.	WS
1.3	01/12/2022	Updated the Copyright Statement.	MW
1.2	07/10/2022	Updates to PSD2 flow diagrams and new section on SCA Checks added. Added details of new optional SCA checks and exemptions: •For recurring transactions, only apply the exemption if the original transaction was SCA; see Check for PSD2 Exemptions • For e-commerce 3D Secure transactions, only consider the transaction as SCA if the cardholder is challenged; see PSD2 Transaction Checks • Apply SCA exemption to transactions from hotel and car rental merchants; see Which Merchant Category Codes are Exempt from SCA?	WS
1.1	26/08/2022	Details added of how to reset transaction and amount counters using the Thredd API. See Reset Counters.	WS
	17/08/2022	Layout and Table of Contents updates	MW
1.0	22/03/2022	First version	WS

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

Support Phone: +44 (0) 203 740 9682

Our Head Office

6th Floor,

Victoria House,

Bloomsbury Square,

London,

WC1B 4DA

Telephone: +44 (0)330 088 8761

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.