

July 2022

Guide for European Card Issuers to Improve UX-challenged 3DS 2.x Processes



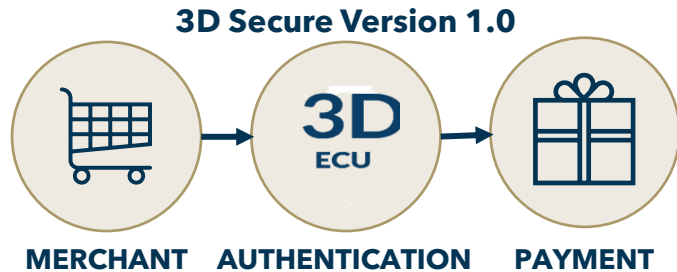
Document Contents

State of 3DS in European Markets

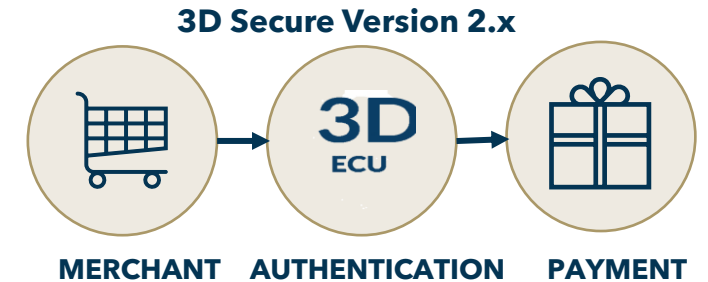
Recommendations for Issuers to Improve 3DS UX

3D Secure has been on the market for some time, but PSD II regulation brought significant updates which provide optionality for issuers.

Summary of 3D Secure



PSD II (Strong Customer Authentication)



- **3-D Secure 1.0** has been on the market for **20 years**.
- **Purpose** of 3-D Secure is to **reduce risk of fraud** for e-commerce transactions.
- 3D-Secure is required **for e-commerce transaction only**.
- **Authentication** requires 3-digit code **CVV/CVC** from back of a card and **SMS Password**.
- 3D Secure is supported by most major card schemes.

- **PSD II** (Strong Customer Authentication) **came into force in September 2019**, and it was issued by **European Parliament**.
- Strong Customer Authentication (SCA) **applies for e-commerce card transactions and payments**.
- An SCA Customer must be authenticated by **three factors**:
 - "Something you are"
 - "Something you have"
 - "Something you know"
- Every PSP must **support SCA** otherwise it will be **finned by a local regulator**.

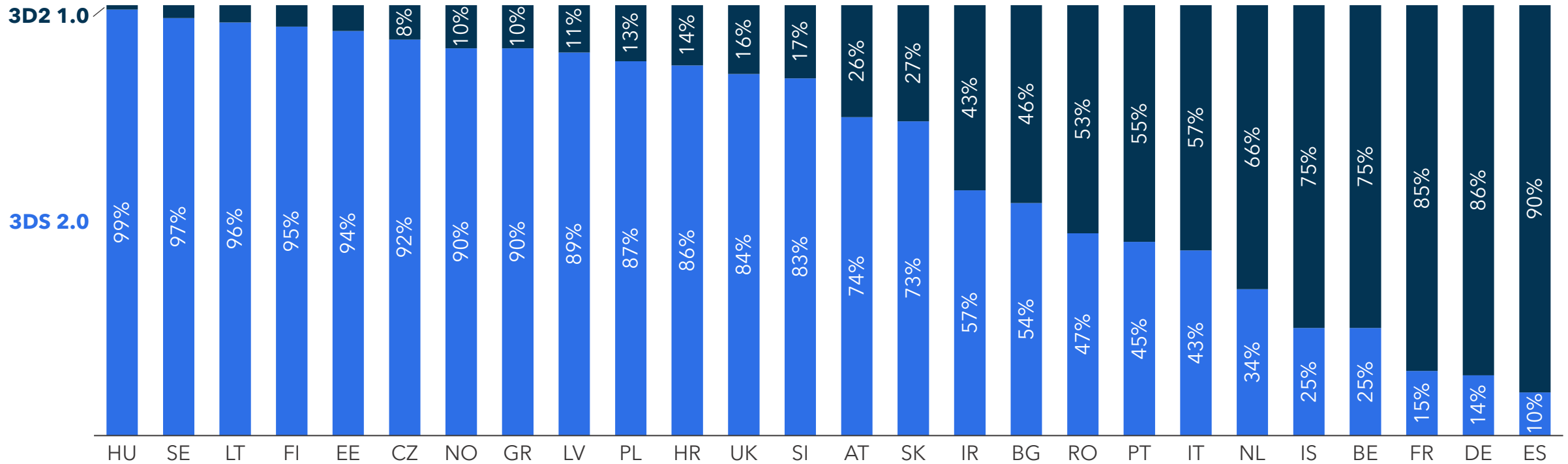
- In response to PSD II, **3D-Secure Version 2.0** came to market.
- The new version came to market to **significantly extend data contained in the transaction sentence**.
- It also **enhanced security** via new authentication protocols.
- 3DS2 **enables issuers to perform Risk-Based Authentication (RBA)**. This process facilitates the exchange of over **100 data points during a transaction**.
- If **PSPs** want to be **compliant with SCA requirement they must support 3DS 2.X**.



While 3DS 2.X has obvious benefits, clunky UX has resulted in an increase in failed transactions. Issuers can take steps to improve their UX and corresponding authentication rate.

Adoption of 3DS 2.X is low across many European countries...

Transactions Using 3D Secure Version 1.0 & 2.x
(2022; % of transactions)



... And many 3DS 2.X UXs are clunky, resulting in low authentication success rates.

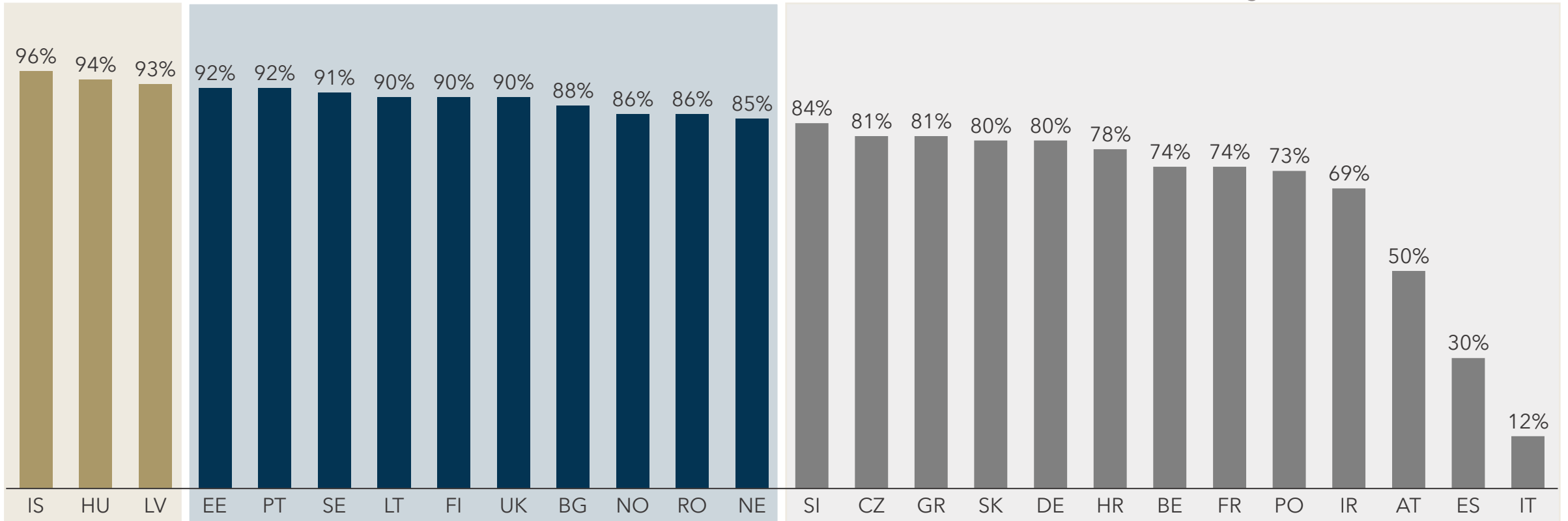
Authentication Success Rate by European Country (2022; % of 3DS 2.X transactions)

Average transaction **success rate** for **3DS 1.0** transactions is **98%**.

Issuers are well adapted.

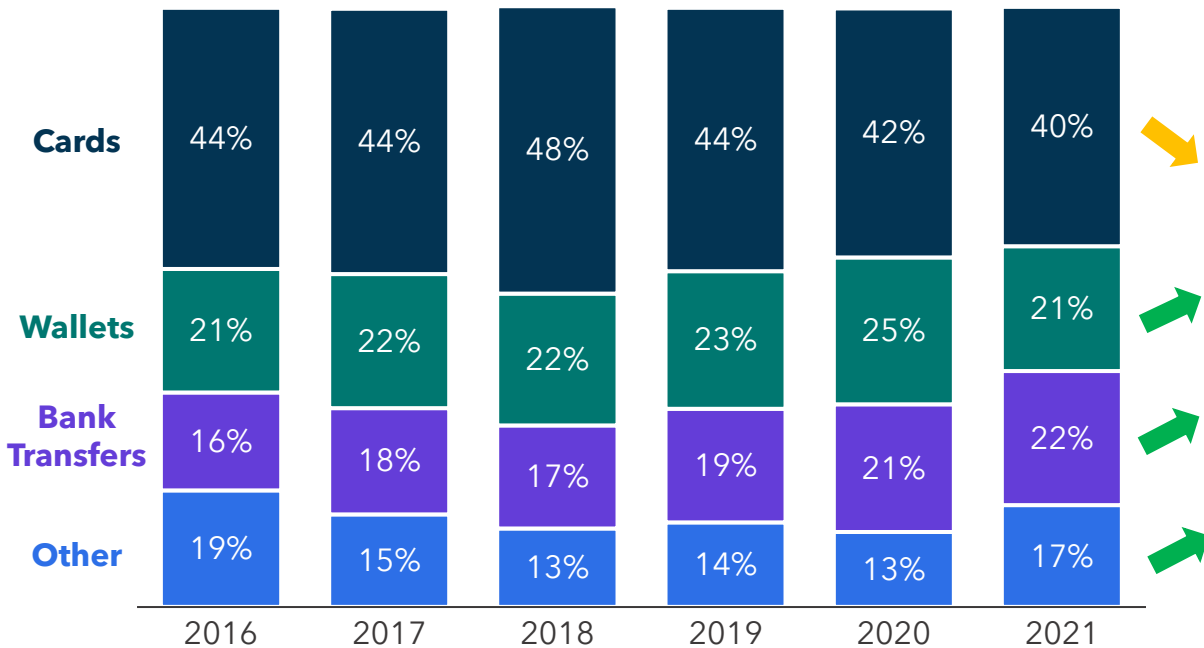
Issuers in these countries need revision of 3DS rules and exemption setting.

Issuers in these countries need significant revision of 3DS rules, exemptions, and authorization settings.



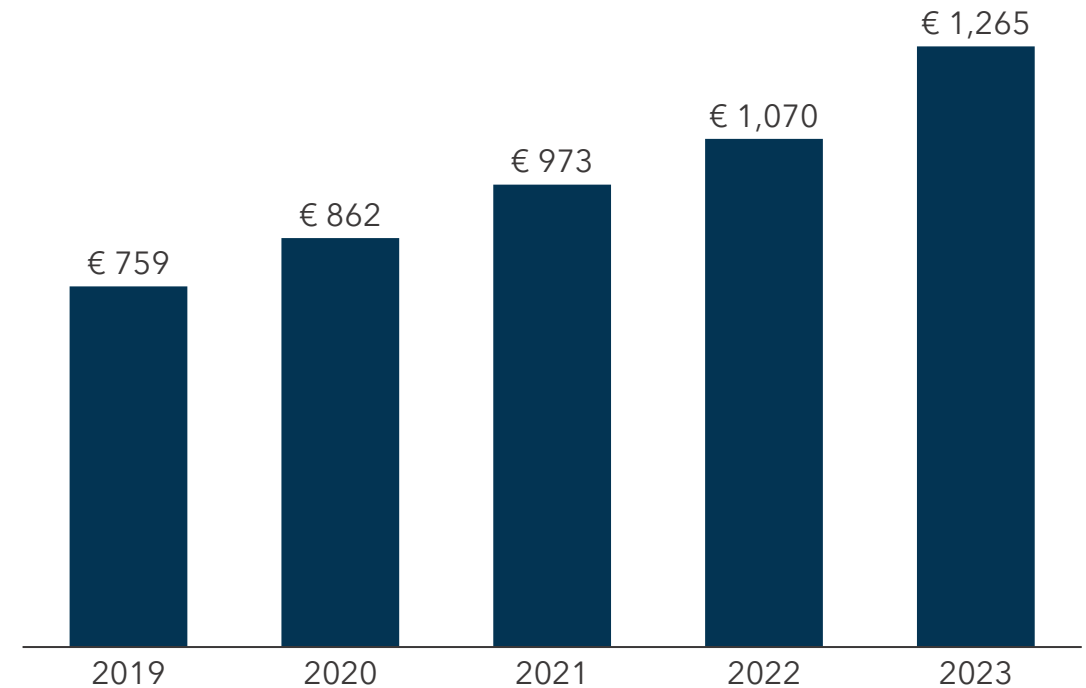
SCA requirements can partially help explain some observed downturns in card usage online between 2019 and 2020.

Online EU Payment Tool Usage
(Weighted Average, in %)



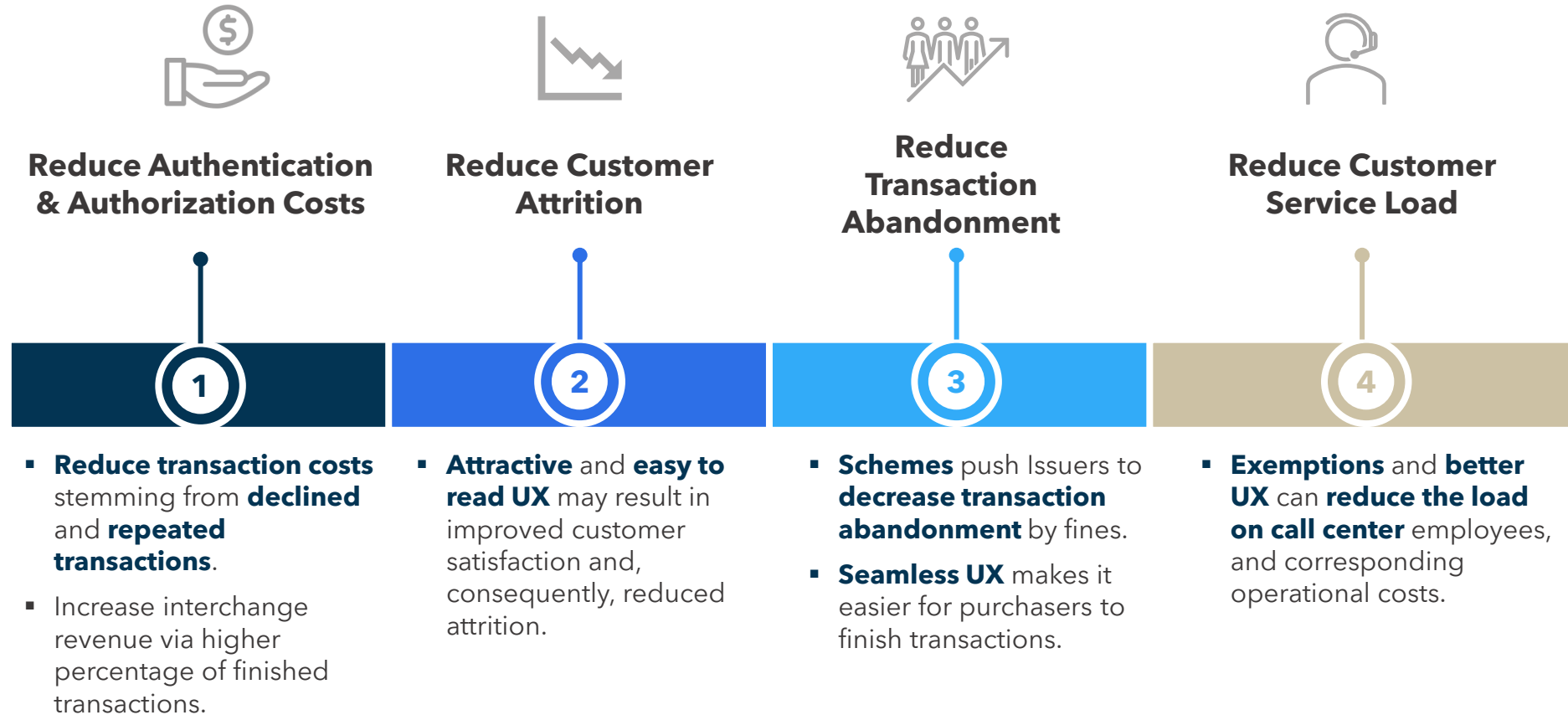
Strong Customer Authentication (SCA) requirements officially went into effect on 14 September 2019.

Total EU e-Commerce Turnover
(2016 – 2020; in € mil.)



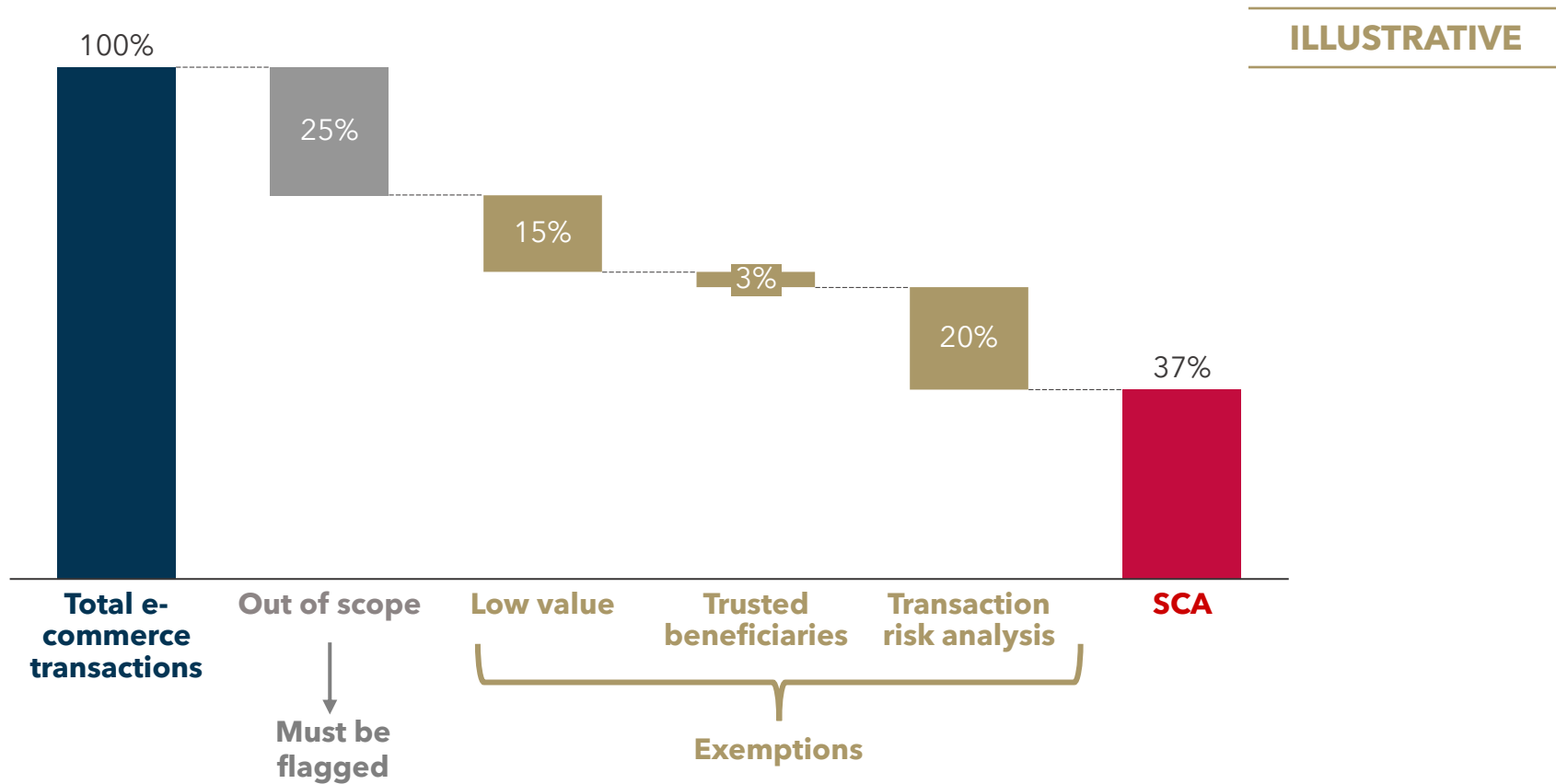
Issuers can significantly reduce abandonment and boost e-commerce volume by setting up SCA and UX properly.

Issuers and Acquirers Benefits from Proper Setting of 3D Secure Rules







Issuers can drastically reduce the number of SCA-required transactions by setting up detection of out-of-scope transactions and by using exemptions.

Illustrative *Moderately-Optimistic Scenario* of % of Transactions Requiring SCA






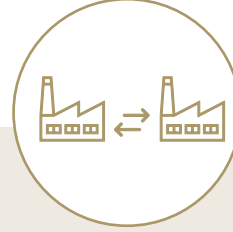






The first step to improving UX is to identify out-of-scope transactions and decrease the rate of failed or abandoned transactions.

Out of Scope Transaction Types

	1	2	3	4
	 <p>"ONE-LEG OUT" TRANSACTIONS</p>	 <p>MERCHANT-INITIATED TRANSACTIONS</p>	 <p>OCT AND ANONYMOUS TRANSACTIONS</p>	 <p>MAIL / TELEPHONE ORDERS MOTO</p>
DESCRIPTION	<ul style="list-style-type: none"> Transactions originating from an acquirer or issuer based out of Europe 	<ul style="list-style-type: none"> Transactions that are initiated by the recipient of the payment, not the payer 	<ul style="list-style-type: none"> Original credit transfers (OCTs) and anonymous payments 	<ul style="list-style-type: none"> Transactions made via mail or telephone
EXAMPLES	<ul style="list-style-type: none"> German cardholder shopping online at a merchant who's acquirer is based in Asia 	<ul style="list-style-type: none"> Monthly or annual subscription (e. g. streaming services, app, software, magazine) 	<ul style="list-style-type: none"> P2P Transactions in which a cardholder receives funds Anonymous prepaid gift cards 	<ul style="list-style-type: none"> Booking a hotel room via phone with a credit card

After flagging out-of-scope transactions, the second step to improving 3DS UX is to determine 3DS exemption protocols.

Exemptions for Strong Customer Authentication

	1	2	3	4								
												
	LOW-VALUE PAYMENTS	TRUSTED BENEFICIARIES	TRANSACTION RISK ANALYSIS	SECURE CORPORATE PAYMENTS								
DESCRIPTION	<ul style="list-style-type: none"> Remote transactions up to €30 do not require SCA Capped at a maximum of 5 transactions or a cumulative limit of €100 from last authentication. 	<ul style="list-style-type: none"> Cardholders can add trusted merchants to a list of "trusted beneficiaries" held by their Issuer. Only cardholders can choose the merchant usually via self-service channel. 	<ul style="list-style-type: none"> Allows for certain remote transactions to be exempted from SCA provided a robust risk analysis is performed, and specific fraud thresholds are met. <table border="1"> <thead> <tr> <th>Thresholds</th> <th>Fraud Rate</th> </tr> </thead> <tbody> <tr> <td><€100</td> <td>0.13%</td> </tr> <tr> <td>€100-€250</td> <td>0.06%</td> </tr> <tr> <td>€250-€500</td> <td>0.01%</td> </tr> </tbody> </table>	Thresholds	Fraud Rate	<€100	0.13%	€100-€250	0.06%	€250-€500	0.01%	<ul style="list-style-type: none"> Transactions made through dedicated corporate processes and protocols, initiated by business entities. Payment instrument must be dedicated for B2B payment type.
	Thresholds	Fraud Rate										
<€100	0.13%											
€100-€250	0.06%											
€250-€500	0.01%											
WHO CAN APPLY	 Issuer  Acquirer	 Issuer	 Issuer  Acquirer	 Issuer								
	Implement in Authorization System and 3D Secure ACS	Implement 3D Secure ACS	Implement Separate Risk Module connected to ACS	Implement in Authorization system								













Document Contents

State of 3DS in European Markets

Recommendations for Issuers to Improve 3DS UX

Issuers should invest in 3DS UX to improve the authentication process for customers.

Summary of Recommendations for Better 3DS UX

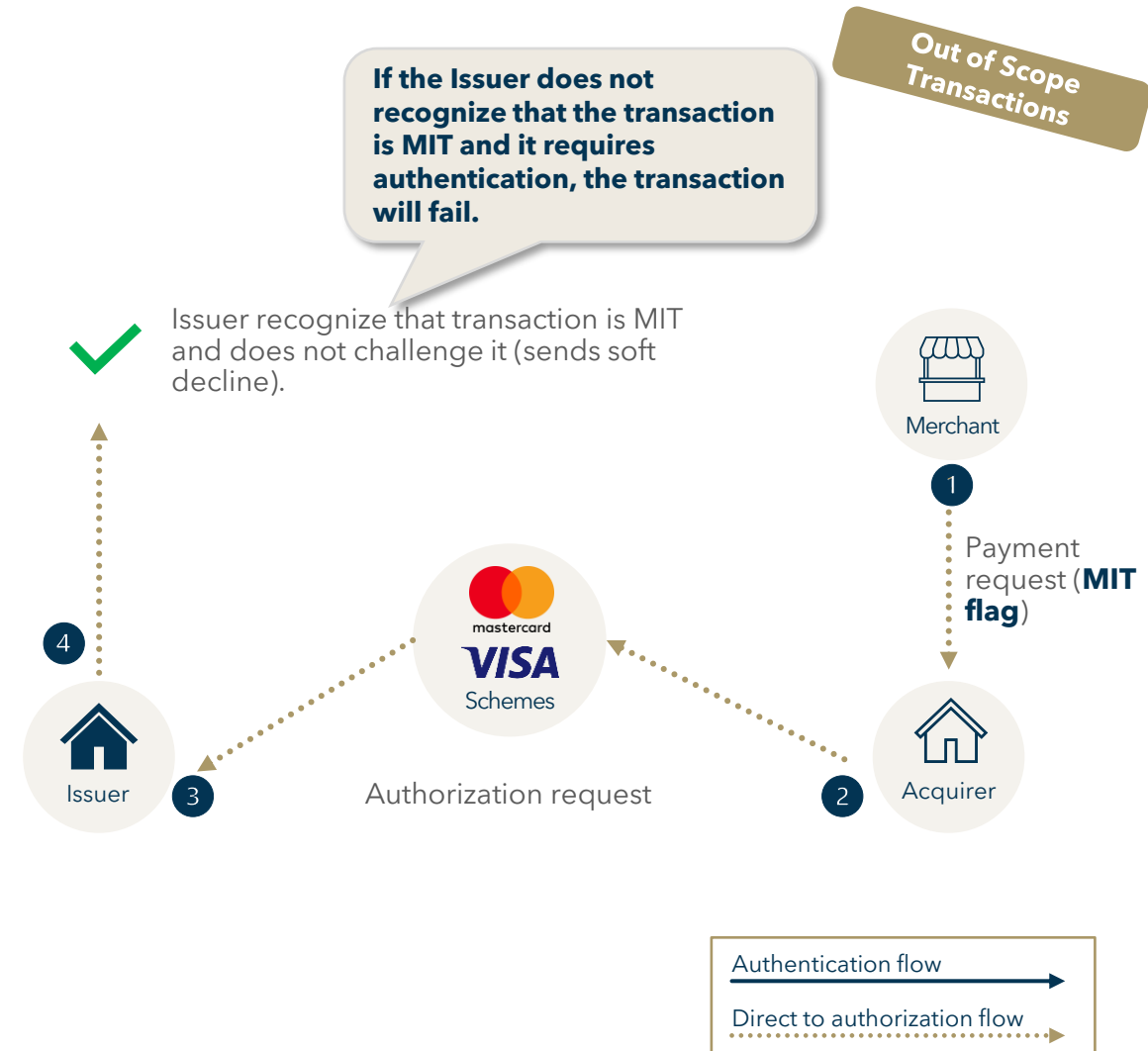
	Description of Recommendation	Implementation difficulty	Impact
1	Recurring Transactions <ul style="list-style-type: none"> ▪ Flag recurring transactions ▪ Acquirers do not mark these types of transactions very often, resulting in declines, especially in subscription payments. 		
2	Low-Value Exemption <ul style="list-style-type: none"> ▪ Apply a low-value exemption on as many transactions as possible because the risk of fraud is already low, and it simplifies the authentication process. 		
3	Trusted Beneficiaries <ul style="list-style-type: none"> ▪ Allow customers to choose trusted merchants, not requiring authentication during ecommerce transactions. 		
4	Transaction Risk Analysis <ul style="list-style-type: none"> ▪ Exempt a particular transaction from SCA if the issuer determines that the transaction is performed by a specific customer based on their data pattern. 		
5	Combine Payment and Card Databases for TRA <ul style="list-style-type: none"> ▪ Combine transaction databases to achieve more effective and accurate decision processes for TRA. 		

Recurring transactions are out of PSD2 scope, but issuers and acquirers need to adapt their systems to support these types of transactions, otherwise all of them will fail.

Recommendation #1: Support recurring transactions

Overview

<p>What is it?</p>	<ul style="list-style-type: none"> Recurring transactions or Merchant-Initiated transactions (MIT) are transactions initiated by the payee, not the payer. MIT transaction must be always authenticated. They are out of scope for PSD2, but issuers and acquirers must adapt their systems to ensure that transactions will not be declined.
<p>What are the benefits?</p>	<ul style="list-style-type: none"> + Smooth transaction flow + Subscription model + Reduce costs for authentication + Higher volumes
<p>How to set it up?</p>	<ul style="list-style-type: none"> MIT/Recurring Transactions are routed directly to authorization so issuers must adapt systems to not challenge them. Acquirers must flag these transactions per scheme guidelines.
<p>Who is Liable?</p>	<p>Acquirers are responsible for MIT/Recurring Transactions</p>

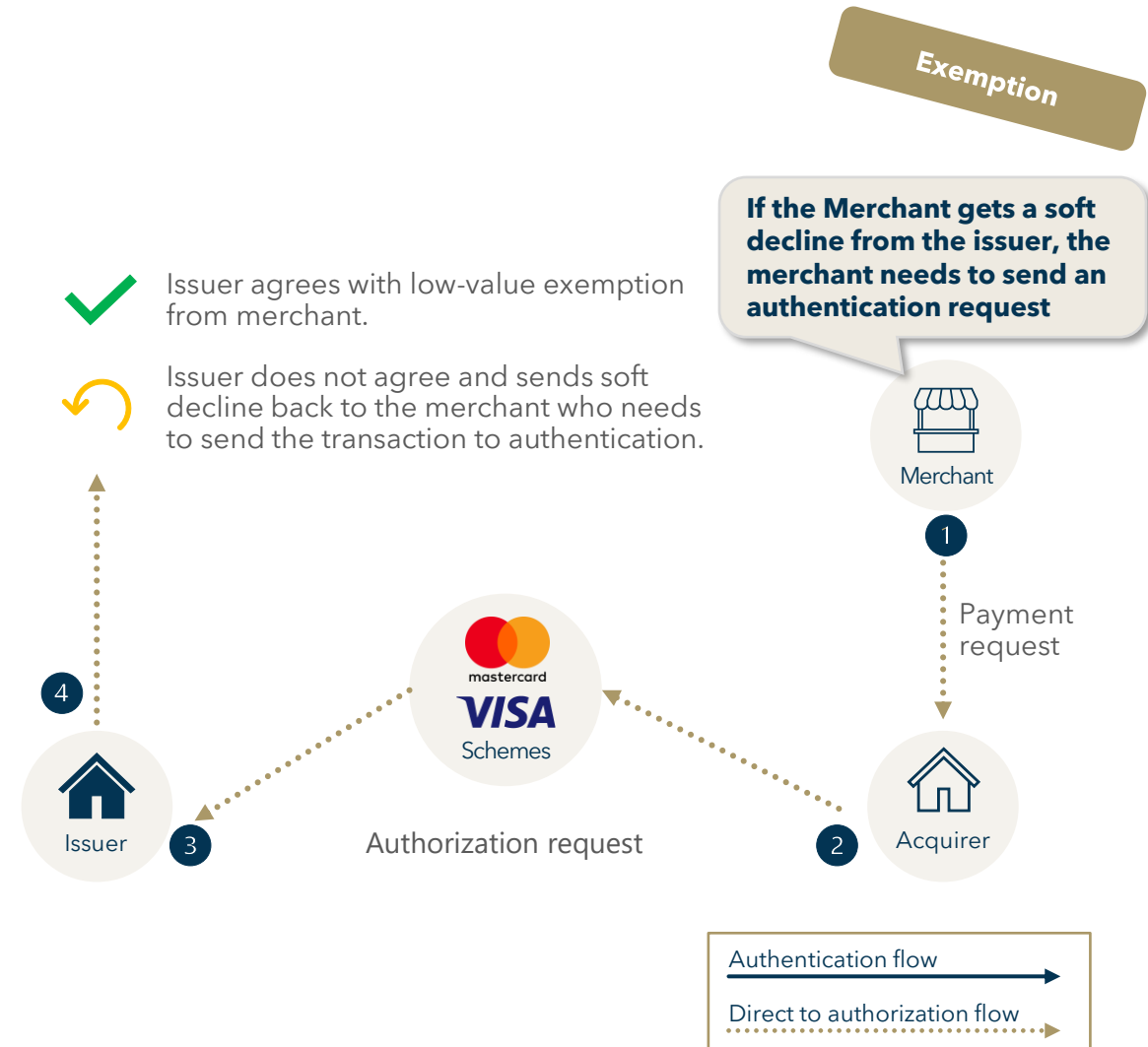


Issuers and acquirers can exempt 'Low Value Transactions' <€30. Issuers are better positioned for this type of exemption as they have a velocity limit tracker.

Recommendation #2: Low Value Exemption

Overview

<p>What is it?</p>	<ul style="list-style-type: none"> Issuers can use the low-value exemption to avoid SCA. The transaction must be under €30 (exemption is also capped at 5 consecutive transactions)
<p>What are the benefits?</p>	<ul style="list-style-type: none"> + Smooth transaction flow + Lower abandoned rate + Reduce costs for authentication + Higher volumes
<p>How to set it up?</p>	<ul style="list-style-type: none"> Issuers must set up in 3DSecure ACS Risk Module and Authorization System. Acquirers can also apply this exemption. Issuers or acquirers needs to set up velocity limit checks (<i>Issuers are better positioned for velocity tracker</i>).
<p>Who is Liable?</p>	<p>Whoever applies the exemption, Issuer or Acquirer, is reliable for potential fraud.</p>

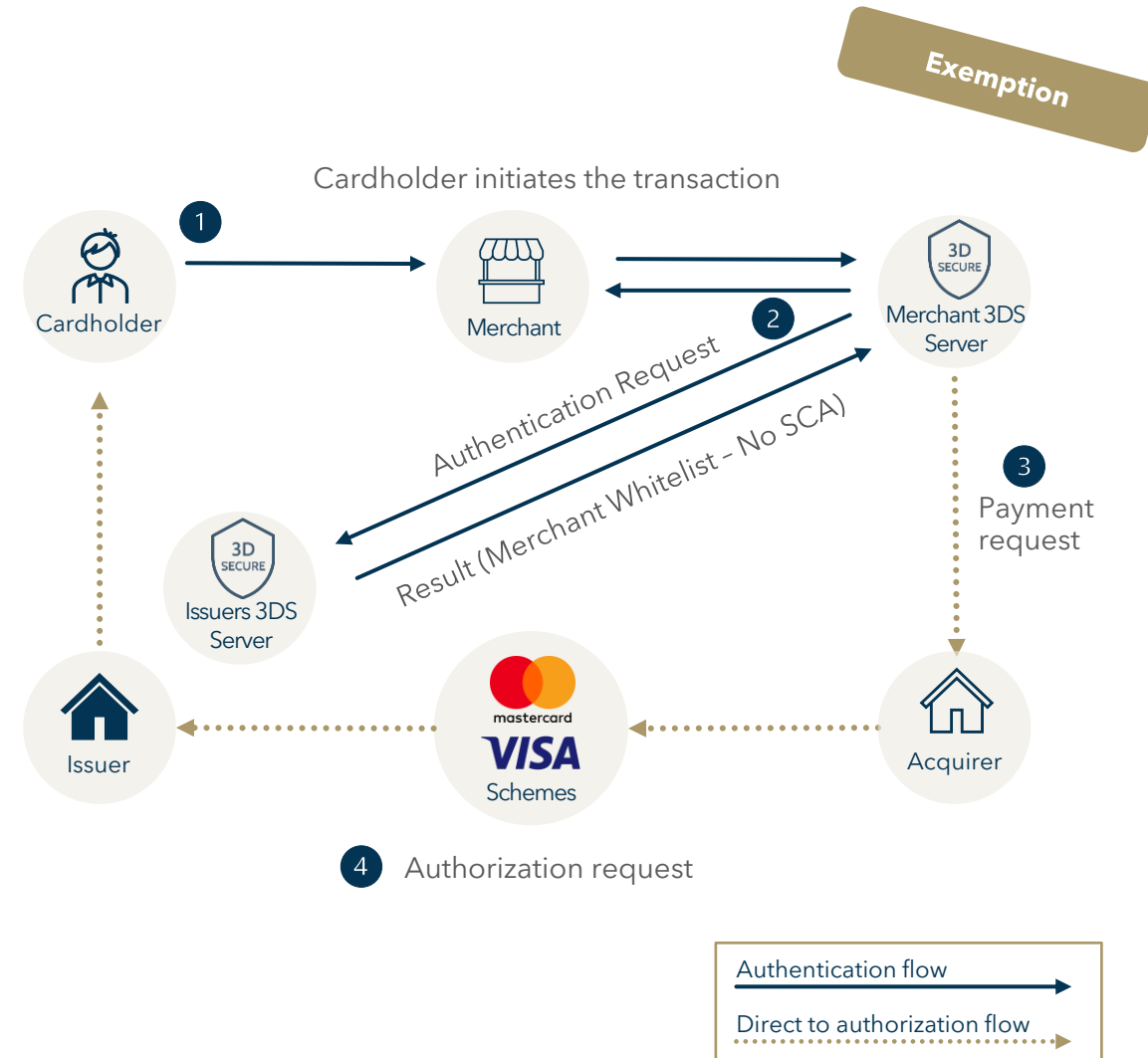


Only Issuers can apply trusted beneficiary exemptions based on fraud exposure. It is an easy, effective, and safe exemption which will ensure a higher approval rate and reduce the authentication costs.

Recommendation #3: Support Trusted Beneficiaries

Overview

<p>What is it?</p>	<ul style="list-style-type: none"> ▪ Cardholders can apply this exemption to have the merchant with which she/he is transacting excluded from SCA. ▪ The Issuer will have the final decision, based on the merchant's fraud exposure. ▪ Issuer has to set up a process via which cardholders can choose the merchant
<p>What are the benefits?</p>	<ul style="list-style-type: none"> + Smooth transaction flow + Lower abandoned rate + Reduce costs for authentication
<p>How to set it up?</p>	<ul style="list-style-type: none"> ▪ Issuer has to set up in 3D Secure ACS Risk Module (authentication server). ▪ Transaction is always sent to authentication, but other exemption is used.
<p>Who is Liable?</p>	<p>Liability is on Issuer because it has the final decision.</p>



Rules for transaction risk analysis are difficult to set up and require long-term analysis, but can significantly decrease abandonment and improve the customer experience.

Recommendation #4: Support Transaction Risk Analysis

Overview

What is it?

- Transaction Risk Analysis, as outlined by the Regulatory Technical Standard (RTS), looks at risk scores and other account risk factors to confirm that no abnormal spending or behavioral patterns of the payer have been identified.
- An issuer or acquirer can use TRA for transactions within certain thresholds.

Thresholds	Fraud Rate
<€100	0.13%
€100-€250	0.06%
€250-€500	0.01%

What are the benefits?

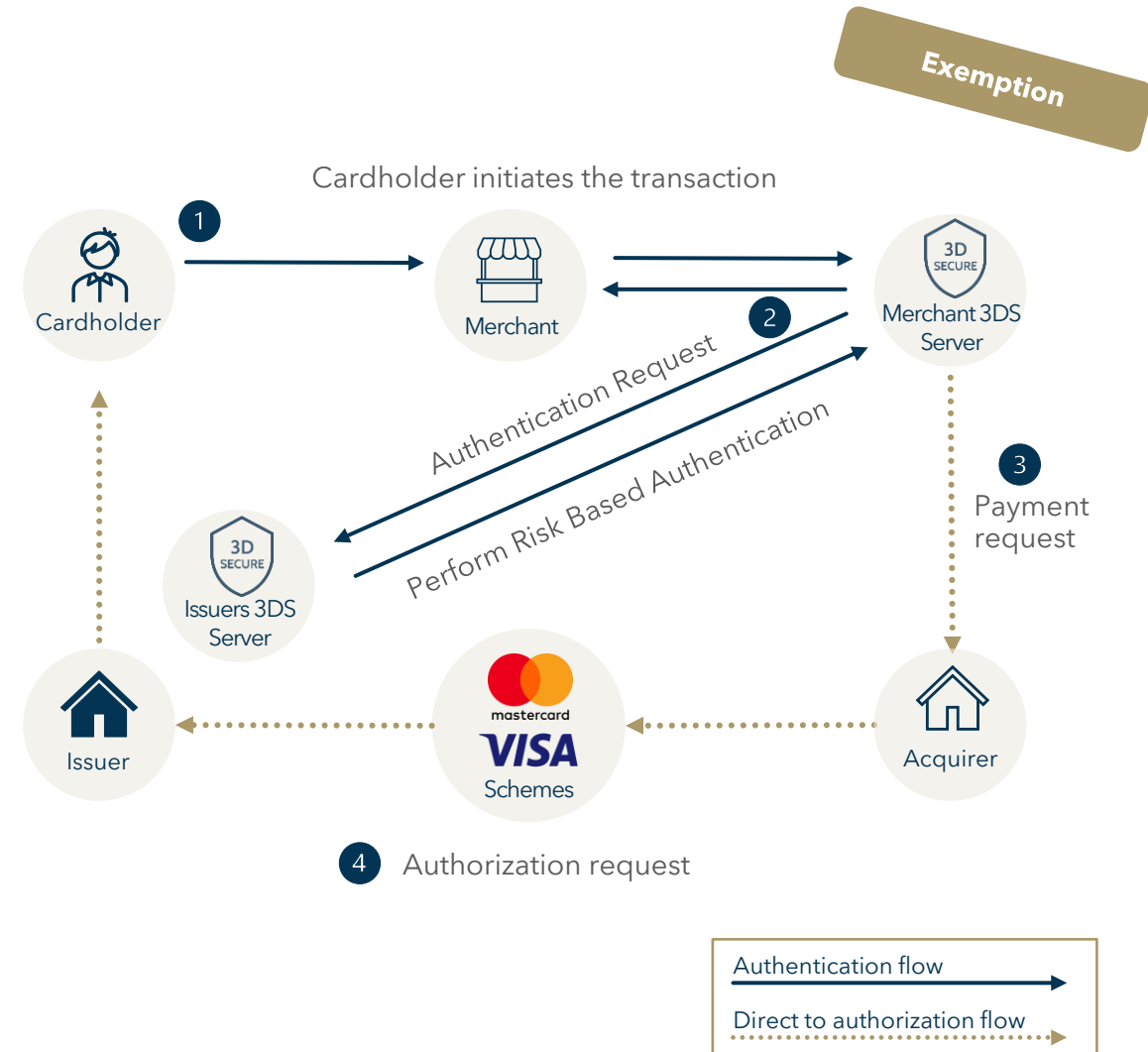
- + Smooth transaction flow and lower abandoned rate
- + Lower abandoned rate
- + Higher volumes and interchange revenue

How to set it up?

- Perform analysis of client behavior; set up rules in risk module based on outputs

LIABILITY

Whoever applies the exemption, issuer or acquirer, is liable for potential fraud.

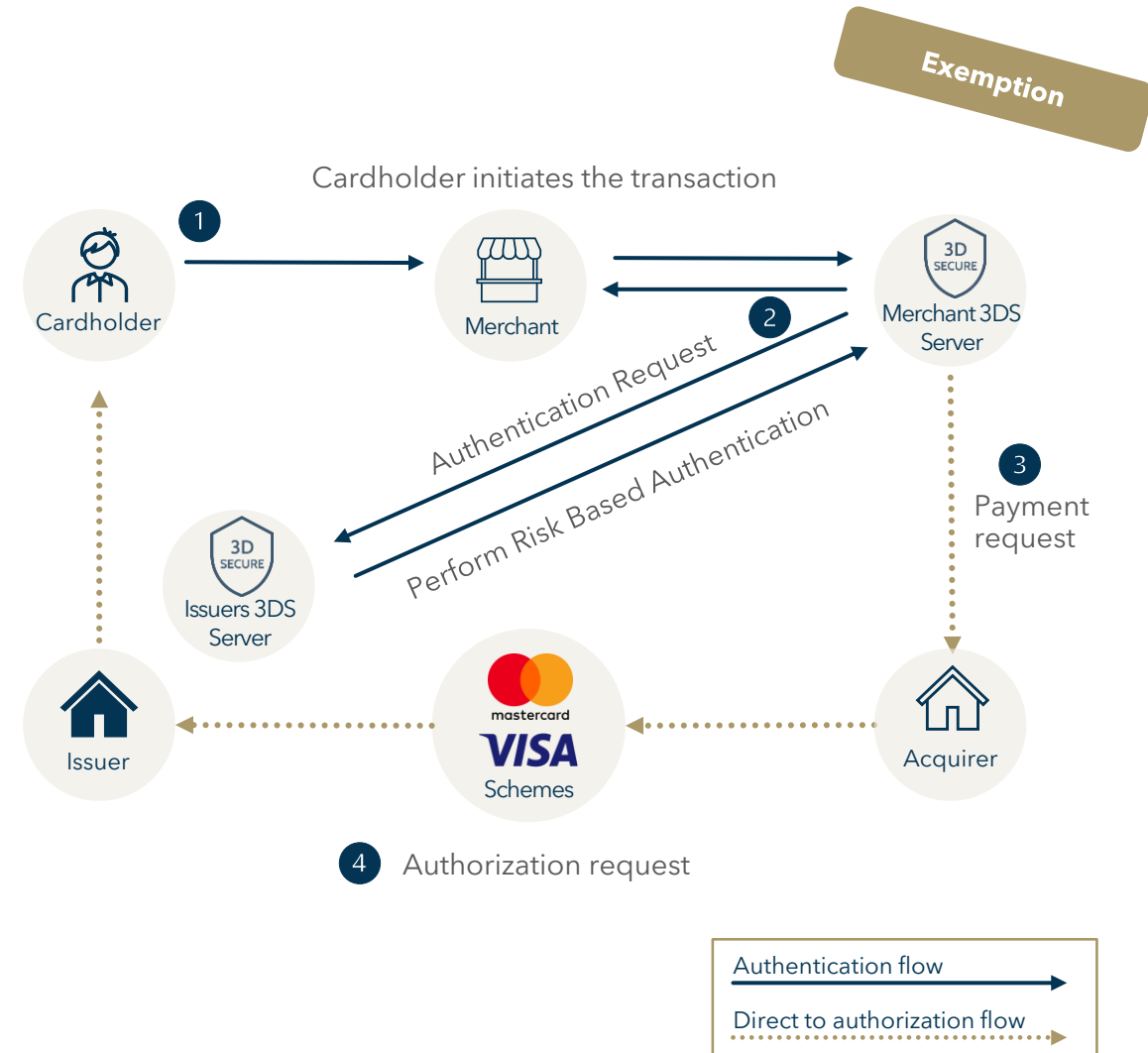


Transaction Risk Analysis is an efficient tool to save authentication cost and avoid the need for SCA. With more data, issuers can improve decisioning.

Recommendation #5: Combine Payment and Card Databases for TRA

Overview

<p>What is it?</p>	<ul style="list-style-type: none"> Issuers can exempt a particular transaction from SCA but only if the PSP determines that the transaction is performed by a specific customer based on their data pattern. To minimize the risk of exempting a transaction, issuers need to have a sufficient level of client data. Combining A2A (bank transfer) payments and card data is an effective strategy for an issuer to expand its dataset. Data sets in both databases should be similar because PSD II expanded transaction data for both payment methods.
<p>What are the benefits?</p>	<ul style="list-style-type: none"> + Smooth transaction flow and lower abandoned rate + Higher volumes and interchange revenue
<p>How to set it up?</p>	<ul style="list-style-type: none"> Issuers need to combine two databases and connect to one risk module. Development is complex but efficient.
<p>LIABILITY</p>	<p>Liability is on the Issuer.</p>



Thank You



Erik Howell
Partner

+420 607 249 640
Erik@FlagshipAP.com



Stanislav Dubský
Consultant

+420 775 376 666
Stanislav@FlagshipAP.com