Strong Customer Authentication

A Merchant Guide

Revised February 2020

J.P.Morgan

About J.P. Morgan

J.P. Morgan offers a full suite of payments services to enable a seamless connection across the payments continuum for clients. We bring our consultative expertise, data-driven insights, and local service around the globe to provide a more unified view of payables, receivables and cash management. Merchant Services is the payment acceptance and merchant acquiring business of JPMorgan Chase & Co. (NYSE: JPM) – a global financial services firm with assets of $2.7 trillion and operations worldwide.[i] According to The Nilson Report, it is also the top merchant acquirer of e-commerce transactions in Europe.[ii]

[i] JPMorgan Chase & Co. Q4 2019 Earnings Report 2019. [ii] The Nilson Report #1153, May 2019.

Information in this document has been obtained from sources believed to be reliable, but neither Chase Paymentech Europe Limited nor any of its affiliates warrant the correctness, completeness, or accuracy of the information contained herein. Chase Paymentech Europe Limited or any of its affiliates are not liable or responsible for decisions made or actions taken in reliance on any of the information contained in this document. The information herein or any document attached hereto does not take into account individual client circumstances, objectives or needs and is not intended as a recommendation of a particular product or strategy to particular clients and any recipient of this document shall make its own independent decision. The information provided herein may not be copied, published, or used, in whole or in part, for any other purpose other than expressly authorised by Chase Paymentech Europe Limited.

Chase Paymentech Europe Limited, trading as J.P. Morgan, is regulated by the Central Bank of Ireland.

Registered Office: J.P. Morgan, 200 Capital Dock, 79 Sir John Rogerson's Quay, Dublin 2, D02 RK57, Ireland.

Registered in Ireland with the CRO under the Registration No. 474128.

Directors: Brian Gaynor, Carin Bryans, Dara Quinn, Steven Beasty (US), Eilish Finan

Contents

1. E-commerce payments are changing in Europe

The European Union's Second Payment Services Directive (PSD2) aims to reduce online fraud while stimulating innovation in the payments industry.

One of the key elements of the directive, Strong Customer Authentication (SCA), introduces additional security for most transactions. It means that customers will need to share information that confirms their identity when buying online. 3D Secure 2.X (3DS 2.X, incorporating versions 2.1 and above) is the framework the card industry is adopting to facilitate SCA.

Although SCA became effective on 14 September 2019, the European Banking Authority (EBA)[1] has allowed for flexibility on enforcement until **31 December 2020**, while the UK's Financial Conduct Authority will not enforce SCA until **14 March 2021[2].**

If you do not take action to prepare for SCA, e-commerce card-based payment transactions will be declined after these dates.

J.P. Morgan's recommendation to all merchants is to implement 3DS 2.1 by 3Q 2020. This will allow enough time to fully test and ensure you are not at risk of declined transactions, which may impact your business. While certain transactions may be exempt from SCA, J.P. Morgan's recommendation, in line with advice from the EBA, is to deploy 3DS 2.1 first, then consider any exemptions that may apply to your business.

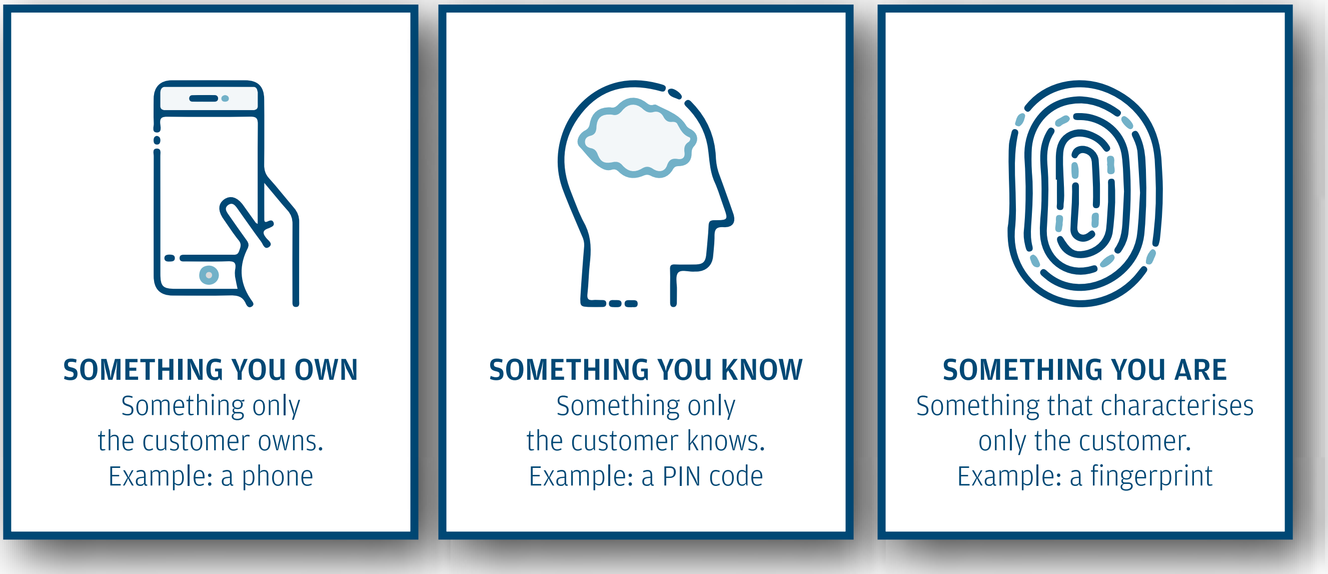
J.P. Morgan has the infrastructure you need today to help you prepare for SCA. This guide outlines the steps you need to take to help ensure that you are prepared to meet the deadline, whether you connect directly to J.P. Morgan or through a third party gateway.

2. What is Strong Customer Authentication?

Strong Customer Authentication is an advanced form of two-factor authentication, in which a consumer will share two of the factors (see Fig. 1) when making an online transaction.

The primary aim of SCA is to reduce online fraud by requiring consumers to authenticate with secure credentials when they use their payment methods – in effect, proving their identity as part of their purchase.

Fig. 1. Overview of Strong Customer Authentication



SOMETHING YOU OWN
Something only
the customer owns.
Example: a phone

SOMETHING YOU KNOW
Something only
the customer knows.
Example: a PIN code

SOMETHING YOU ARE
Something that characterises
only the customer.
Example: a fingerprint

[1] European Banking Authority, 16 October 2019

[2] Financial Conduct Authority, 13 August 2019

3. What is 3D Secure 2.X and what role does it play in SCA?

3D Secure 2.X (3DS 2.X) is a solution which enables consumers to authenticate themselves when performing an online transaction. Also known as EMV 3D Secure, 3DS 2.X is the solution the card industry is using to deliver SCA.

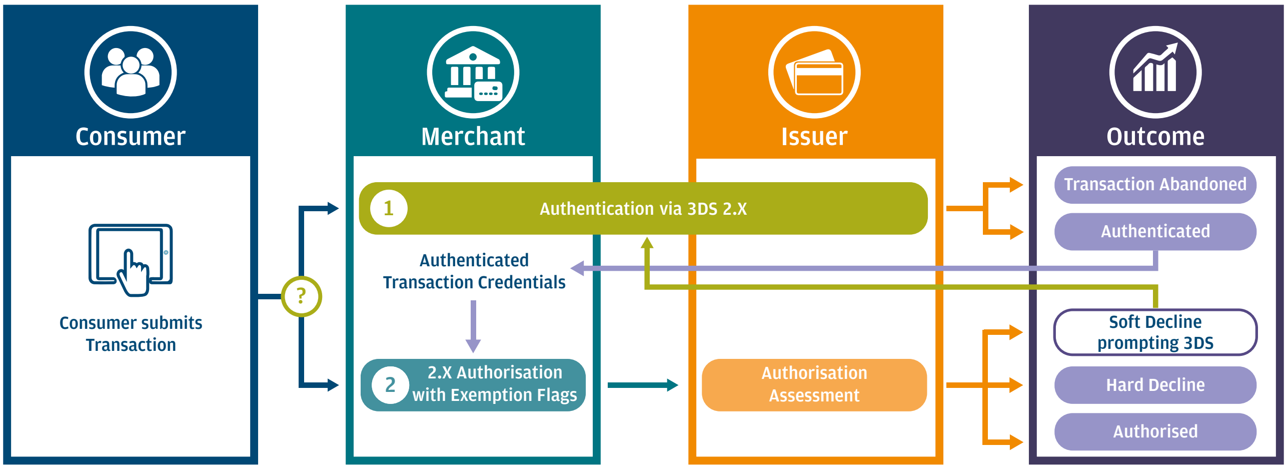

Consumer
Consumer submits Transaction
?
Merchant
1
Authentication via 3DS 2.X
Authenticated Transaction Credentials
2
2.X Authorisation with Exemption Flags
Issuer
Authorisation Assessment
Outcome
Transaction Abandoned
Authenticated
Soft Decline prompting 3DS
Hard Decline
Authorised

Fig. 2. Authentication and Authorisation via 3DS 2.X

There are two distinct actions a merchant needs to perform when they use 3DS 2.X:

1 **Authentication** – In this step, the consumer's ownership of their card is confirmed through the merchant's 3DS 2.X authentication solution. As evidence of this confirmation, the issuer will return a unique identifier to the merchant.

2 **Authorisation** – This step confirms the issuer's approval of the transaction. After successful authentication, the merchant sends the authorisation request, together with the authentication identifier returned in step 1 to the issuer. Once authorised, merchants can proceed to a settlement request.

A note on Dynamic Linking
Linking is a requirement of SCA - it requires the merchant to take a cryptogram from the authentication output and submit that data as part of the transaction authorisation. The merchant also needs to ensure that: 1) the authorisation value does not exceed 15% of authentication value and 2) if possible, the merchant name matches closely between authentication & authorisation.

4. 3D Secure - a quick guide to the versions

3D Secure version 1.0 - Does not support the latest and most secure authentication methods such as mobile banking app, or embedded biometrics, nor SCA exemptions via authentication. **Please Note: Due to the limitations, more transactions via 3DS version 1 are likely to fail or be declined by issuer** (Source: UK Finance Communication on Strong Customer Authentication 28 January 2020)

3D Secure version 2.1 *(recommended minimum version for SCA)* **-** Offers the ability to adapt to in-app payments and to authenticate a card transaction through a mobile banking app. Issuers may choose to deploy biometric authentication via their mobile banking app through 3DS 2.1.

3DS Secure version 2.2 - Provides an improved consumer experience for mobile banking app authentication, as well as adding support for embedded biometric authentication methods such as fingerprints and facial recognition. Version 2.2 also provides support for exemptions, as well as useful features for more complex use cases.

5. 3D Secure: Specification comparison

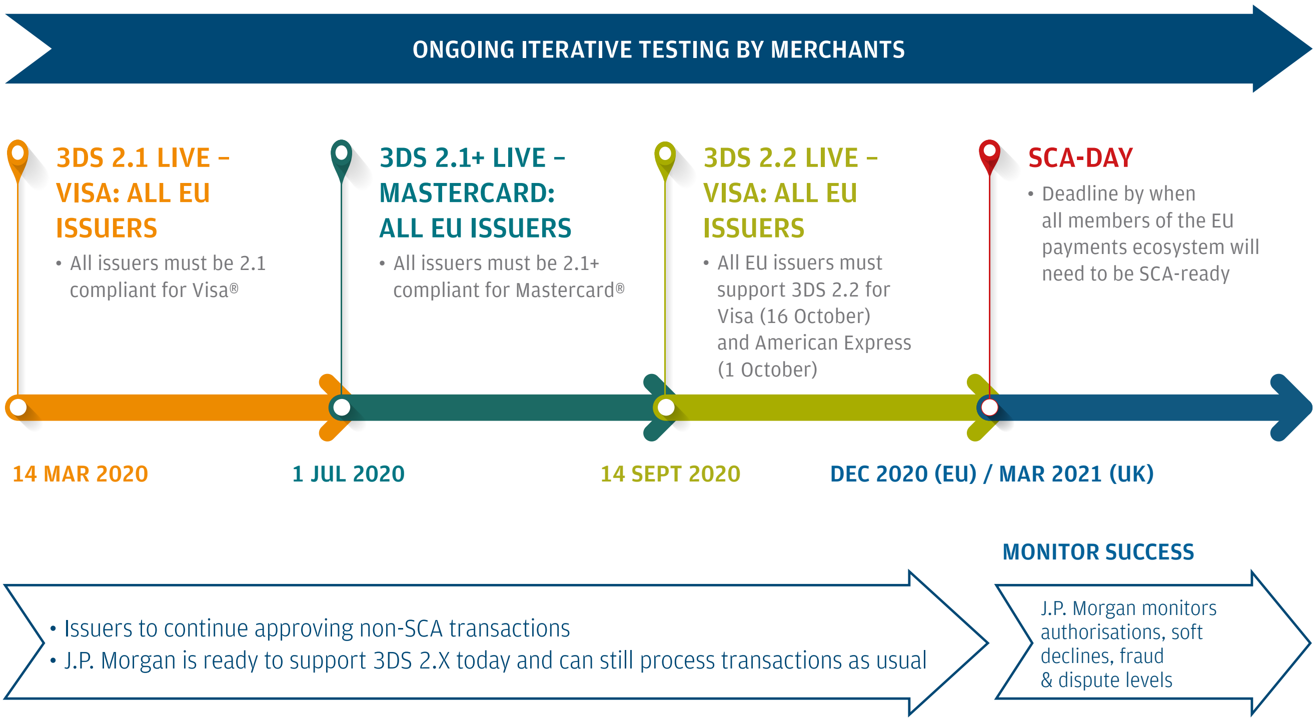
	Feature	3DS 1.0	3DS 2.1	3DS 2.1+	3DS 2.2
Merchant Impacting	**SCA compliant** (While 3DS 1.0 is compliant with SCA, it provides a basic service. Merchants should support 3DS 2.1, at a minimum)	✓	✓	✓	✓
	Supports exemptions (Merchants can flag that they are claiming an exemption when they submit an authentication – issuers can accept the exemption, or ask the consumer to authenticate)			✓	✓
	Works effectively on mobile devices		✓	✓	✓
	Supports games consoles (Games consoles work on different types of browsers, which require unique support)				✓
	Supports 3RI (3 Requester Initiated) (Enables reauthentication while the customer is not present e.g. split shipments)		✓	✓	✓
	100+ data elements (3DS 2.1 includes more data elements e.g. IP address of the end customer)		✓	✓	✓
Issuer Impacting	**Mobile banking app integration** (Issuers can enable their customers to authenticate through their mobile banking application)		Basic	✓	✓
	Biometric authentication (Issuers can enable their customers to authenticate with their fingerprint, face recognition, etc.)		Basic	✓	✓
	Dynamic linking (Issuers can link the authentication and authorisation based on the cryptogram)		✓	✓	✓

Note: 3DS 2.1+ refers to Mastercard only. Mastercard has implemented a specification extension to bring forward exemption support in 3DS

6. What forms of authentication will issuers ask of my customer?

Mobile App Biometrics	**Facial recognition or thumbprint via mobile banking app**	**PROS** • Ease of use • High security • Low abandonment	**CONS** • Inaccessible solution for less tech-savvy users
Behavioural Biometrics + One Time Password (OTP)	**E.g., customer typing input speed, interactions with device + OTP**	**PROS** • Potential to reduce friction • Aligned to EBA view on what constitutes 'inherence' • Ability to reduce fraud	**CONS** • Lack of clarity on what solution would measure • Early stage / unproven technology • Takes time for a profile to become reliable
Knowledge Factor + One Time Password (OTP)	**E.g., Internet banking login password, or memorable data + OTP**	**PROS** • Compliant as a knowledge factor • Tried and tested technology	**CONS** • Poor customer experience • Unclear security benefits, susceptible to scams • Reset process dependent on individual issuer approach
Card Reader or alternative	**Provides a PIN which the customer enters online to authenticate the transaction**	**PROS** • Reliable fallback option for specific low volume customer segments, e.g. vulnerable customers	**CONS** • Disproportionate cost to level of use • Requires cardholder to hold physical device

7. Mandated timelines for SCA



ONGOING ITERATIVE TESTING BY MERCHANTS

3DS 2.1 LIVE – VISA: ALL EU ISSUERS
- All issuers must be 2.1 compliant for Visa®

3DS 2.1+ LIVE – MASTERCARD: ALL EU ISSUERS
- All issuers must be 2.1+ compliant for Mastercard®

3DS 2.2 LIVE – VISA: ALL EU ISSUERS
- All EU issuers must support 3DS 2.2 for Visa (16 October) and American Express (1 October)

SCA-DAY
- Deadline by when all members of the EU payments ecosystem will need to be SCA-ready

14 MAR 2020

1 JUL 2020

14 SEPT 2020

DEC 2020 (EU) / MAR 2021 (UK)

- Issuers to continue approving non-SCA transactions
- J.P. Morgan is ready to support 3DS 2.X today and can still process transactions as usual

MONITOR SUCCESS

J.P. Morgan monitors authorisations, soft declines, fraud & dispute levels

8. How do I ensure my business is SCA compliant?

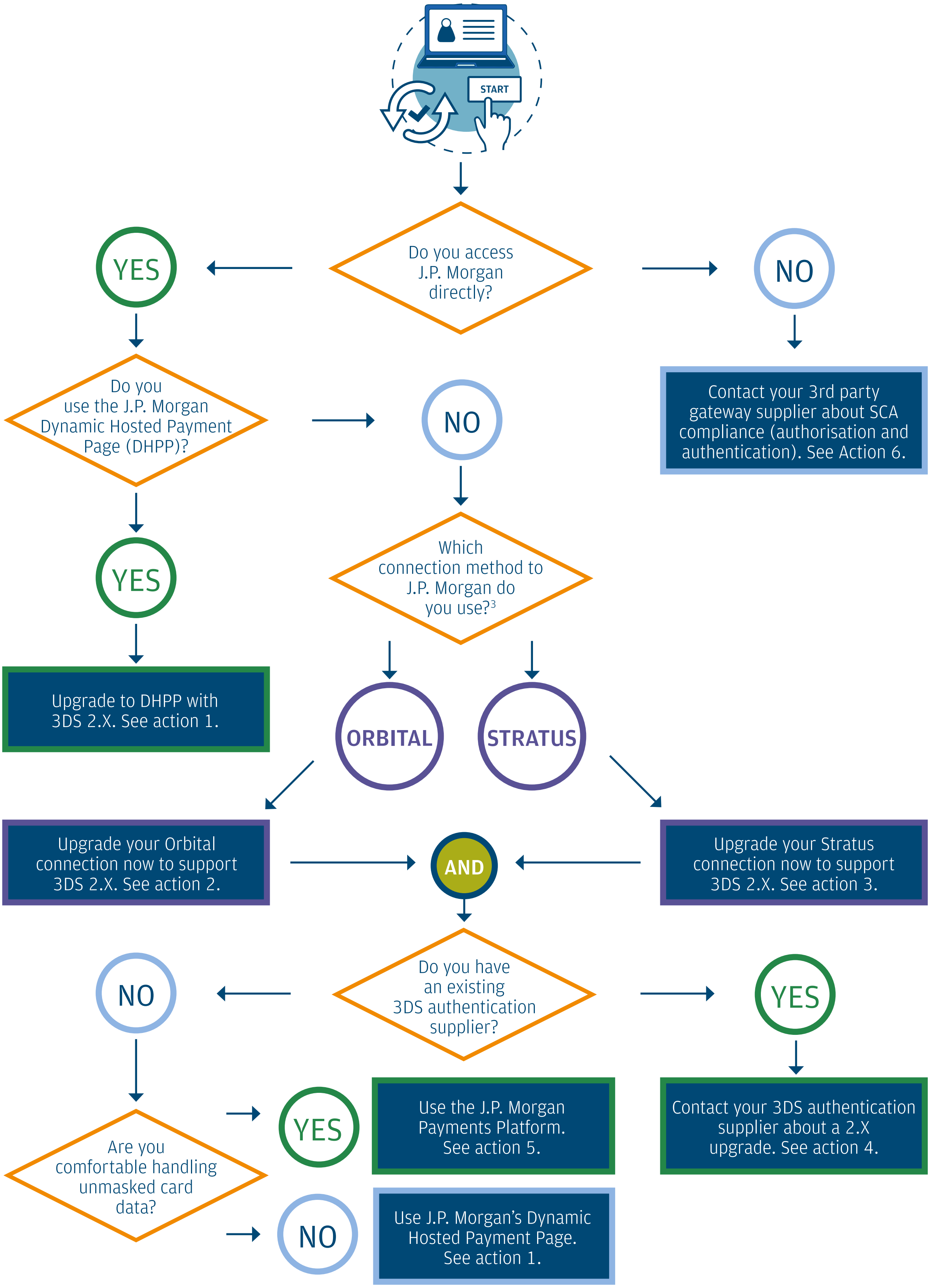
Merchants must be able to perform both authentication and authorisation within the 3DS 2.X framework. To achieve this, you need to have a solution in place for both Authentication and Authorisation from the options below:

Solution	Supplied by	Authentication	Authorisation
Orbital	J.P. Morgan		✓
Stratus	J.P. Morgan		✓
Dynamic Hosted Payments Page (DHPP)	J.P. Morgan	✓	✓
J.P. Morgan Payments Platform (JPM PP)	J.P. Morgan	✓	
3rd party authentication solution	Merchant’s selected provider	✓	
3rd party gateway product *	Merchant’s selected provider	✓	✓

* Confirm with your gateway provider

9. Which is the best solution for me?

Use this decision tree to find the best solution for your business:



START

Do you access J.P. Morgan directly?

YES

Do you use the J.P. Morgan Dynamic Hosted Payment Page (DHPP)?

YES

Upgrade to DHPP with 3DS 2.X. See action 1.

NO

Which connection method to J.P. Morgan do you use?[3]

ORBITAL

Upgrade your Orbital connection now to support 3DS 2.X. See action 2.

STRATUS

Upgrade your Stratus connection now to support 3DS 2.X. See action 3.

AND

Do you have an existing 3DS authentication supplier?

YES

Contact your 3DS authentication supplier about a 2.X upgrade. See action 4.

NO

Are you comfortable handling unmasked card data?

YES

Use the J.P. Morgan Payments Platform. See action 5.

NO

Use J.P. Morgan's Dynamic Hosted Payment Page. See action 1.

NO

Contact your 3rd party gateway supplier about SCA compliance (authorisation and authentication). See Action 6.

[3] Please contact your relationship manager if you are unsure which method you use

10. Actions for Merchants, depending on your gateway and connection

1. Upgrade to Dynamic Hosted Payment Page (DHPP) with 3DS 2.X

If using the J.P. Morgan DHPP

- Merchants using J.P. Morgan's DHPP can upgrade their connection to include the DHPP 3DS 2.X authentication service which will be integrated with their authorisation connection. Merchants who already use 3D Secure through the DHPP should also upgrade to the 3DS 2.X specification
- If you are not currently using the DHPP, but require an integrated authentication / authorisation solution whereby you do not handle sensitive card data, J.P. Morgan recommends you to migrate to the DHPP which will address your needs
- The specifications for the DHPP 3DS 2.X authentication solution through DHPP are available from the Merchant Services DHPP developer centre
- To learn more about DHPP, please contact your relationship manager

2. Upgrade Orbital to support 3DS 2.X

If you connect to J.P. Morgan via Orbital

- Merchants will need to upgrade their Orbital authorisation connection to support 3DS 2.X
- The updated authorisation specifications are available now from the Merchant Services Orbital developer centre
- Merchants who authorise card transactions through J.P. Morgan's Orbital connection can either use the J.P. Morgan Payment Platform, (see action 5), or a 3rd party solution
- If you need support upgrading your Orbital solution, please contact your relationship manager

3. Upgrade Stratus to support 3DS 2.X

If you connect to J.P. Morgan via Stratus

- Merchants will need to upgrade their Stratus authorisation connection to support 3DS 2.X
- The updated authorisation specifications are available now from the Merchant Services Stratus developer centre
- Merchants who authorise card transactions through J.P. Morgan's Stratus connection can either use the J.P. Morgan Payment Platform (see action 5), or a 3rd party solution
- If you need support upgrading your Stratus authorisation connection, please contact your relationship manager

4. Contact your existing 3DS authentication supplier about 3DS 2.X

If you already have a 3DS authentication supplier

- Merchants will need to provide their supplier with credentials provided by their acquirer (e.g. Mastercard ID). Please contact your J.P. Morgan Merchant Services relationship manager for support
- If you are already using the J.P. Morgan 3D Secure 1.0 Standalone MPI (i.e. when you are not using our DHPP service), please contact your relationship manager to plan your upgrade to our 3DS 2.X solution
- Don't forget that you will also need to upgrade your Stratus or Orbital authorisation connection to support the 3DS 2.X authentication result. Please contact your J.P. Morgan Merchant Services relationship manager if you need support

5. Integrate J.P. Morgan's Payments Platform

If you don't already have a 3DS 2.0 authentication supplier

- The J.P. Morgan Payments Platform is a standalone authentication solution which facilitates authentication via 3D Secure. The platform is used in tandem with a merchant's authorisation connection, and merchants manage the transfer of data between the two solutions. This requires the merchant to handle sensitive card data
- Specifications are available from the J.P. Morgan Payments Platform developer centre
- Please contact your relationship manager if you wish to use the J.P. Morgan Payments Platform to authenticate your transactions

6. Contact your gateway supplier

If using a third-party gateway supplier

- Merchants who use a third-party gateway to process with J.P. Morgan, should work with them to implement their 3DS 2.X solution
- It is important to note that you should confirm with your gateway provider that their connection to J.P. Morgan is 3DS 2.X compliant and that your certification to the gateway supports it. If you plan on submitting SCA exemptions, please note this to your provider
- Merchants will need to give their supplier credentials provided by their acquirer (e.g. Mastercard ID).
  Please contact your J.P. Morgan relationship manager for more information

KEY ACTION FOR MERCHANTS:

Take immediate action now to plan the deployment of your SCA solution by Q3 2020 to avoid the risk of declined transactions after the deadline of 31 December 2020.

11. What about exemptions?

SCA allows merchants to avail of exemptions in certain scenarios. Once you have identified your 3DS 2.X solution, it is then time to understand whether any SCA exemptions apply to your business.

SCA exemptions available to all merchants

Exemption	Description	Qualification
Recurring Transactions	Applicable to merchants who perform recurring transactions with the same amount, with the same payer. Strong Customer Authentication is required for set-up/first transaction.	Transactions with a recurring agreement should perform authentication on enrolment. All subsequent transactions are out of scope when the transactions are coded as recurring under the stored credential framework. Read our guide to stored credentials here Merchants who have existing recurring agreements with their customers will be able to 'migrate' these relationships so SCA authentication is not required in this scenario.
Low-Value Transactions	Transactions below €30 can be exempt under the "Low-Value" exemption.	Merchants can send a "Low-Value" exemption flag through either the authentication or authorisation message for transactions below €30. If the customer initiates more than five consecutive low value payments or if the total payments value exceeds €100, SCA will be required. Where the "Low-Value" flag has been passed by the merchant they will retain the liability if there is a chargeback.

SCA exemptions available in certain circumstances

Exemption	Description	Qualification
Transaction Risk Analysis	Merchant/Acquirer can claim a TRA (Transaction Risk Analysis) exemption flag based on the acquirer's portfolio fraud rates.	Merchants with an applicable fraud rate of below 6 basis points will be reviewed to assess suitability.
Trusted Beneficiaries	Issuers can offer consumers the option to list a merchant as a trusted beneficiary either via the cardholder's banking portal or after a transaction has been completed. This exemption would then apply to all future transactions from this merchant.	More information on how merchants can avail of this exemption is available from your relationship manager.
Secure Corporate Exemption	This exemption applies to transactions on a specific type of corporate card where the payments are through dedicated processes by payers who are not consumers.	Merchants who process these types of transactions and wish to explore the Secure Corporate Exemption should contact their J.P. Morgan relationship manager for further details.

Where do I flag these exemptions?

Merchants who wish to utilise an exemption for in-scope transactions have two options:

1. **Authenticate, then Authorise**

   Submit your authentication request to the issuer through your 3DS 2.X authentication solution with an exemption flagged. If approved by the issuer, you can then submit your authorisation request with the additional details of the approved exemption. This approach is likely to provide the greatest rate of success, especially for high risk transactions. Please note, your authentication and authorisation solutions will need to support exemption flags. American Express requests the use of SafeKey for every single transaction.

2. **Direct to Authorisation**

   Submit an authorisation request, including the requested exemption. The issuer will then decide whether to approve or decline the authorisation. If the issuer views the transaction as high risk, they may decline the authorisation and issue a soft decline response code indicating that the merchant should authenticate the customer[1]. Merchants should then authenticate the customer. Please note, this approach may not be suitable for merchants who do not submit their authorisation in real-time, as the customer may not be available to perform the authentication if they are requested to do so by their issuer.

[4] If accessing J.P. Morgan via Stratus, the soft decline code is 532 for Visa / Amex and 510 for Mastercard
If accessing J.P. Morgan via Orbital, the soft decline code is 60 for Visa / Amex, and C5 for Mastercard.

12. Are any transactions out of scope for SCA?

Yes, some types of transaction are considered out of scope:

Out of scope transactions		
Out of scope	**Description**	**How to ensure out of scope**
Merchant Initiated Transactions (MIT)	Merchants must be coded to the stored credentials framework in order to ensure that issuers can identify transactions as out of scope. Characteristics of a Merchant Initiated Transaction: • A transaction, or series of transactions, of a fixed or variable amount at fixed or variable intervals, governed by an agreement between the cardholder and merchant that, once agreed, allows the merchant to initiate subsequent payments without any direct involvement of the cardholder.	Merchant Initiated Transactions should perform Strong Customer Authentication with 3DS 2.X on enrolment. All subsequent transactions should be coded to the stored credentials framework in order for issuers to identify the transactions as MIT. Read our guide to stored credentials here
Anonymous Prepaid Cards	Anonymous Prepaid Cards are out of scope.	Issuers will not request SCA authentication from consumers for these transactions as only they can recognise the issued card as anonymous pre-paid.
MOTO	Mail Order/Telephone Order transactions are out of scope.	Ensure transactions are coded as a MOTO transaction.
One-leg transactions	One-leg transactions are transactions in which either the issuer or the acquirer is located outside of the EEA. Only transactions in which **both** the issuer and the acquirer are in the EEA are in scope.	Where the merchant acquires with an EEA acquirer (e.g. J.P. Morgan Merchant Services) and takes payments from EEA issued cards, those transactions are in scope for Strong Customer Authentication. Unless the merchant can ascertain that the issuer is outside the EEA, they should proceed with SCA compliance.
Direct Debit	Direct Debits are excluded from SCA	Direct Debit transactions will be recognised as out of scope and do not have a framework (e.g. 3DS) to perform SCA.

13. SCA - a few scenarios

The below sheet provides guidance on coding for some common transactions on a J.P. Morgan platform. If you are using other gateway providers, please check their specifications.

Please refer to the guidelines published by Visa and Mastercard and speak with your Relationship Manager for further details.

E-commerce scenario	Authentication	Authorisation
Checking out a basket of items using a stored credential, for a known amount that can be fulfilled within 7 days	Authenticate immediately for the full amount, unless exemptions apply	Authorise for the full amount with: • message type 'CUSE' • stored credential = Y • and cryptogram[5]
Delayed shipment with expected delay using a stored credential	Authenticate immediately for the full amount, unless exemptions apply	Account verification without cryptogram Store the returned transaction ID (TXID) When the goods are ready to ship, authorise with: • message type 'MRAU' • stored credential = Y • cryptogram[5] • and TXID
Ordering a car via a mobile app, using a stored credential when final amount is paid at the end of the journey	Authenticate for highest estimated amount at time of ordering	Account verification without cryptogram Store the returned TXID If final amount is within reasonable expectations for the cardholder, authorise for the final amount with: • message type 'MRAU' • stored credential = Y • cryptogram[5] • and TXID
Setting up a new agreement for future Merchant Initiated Transactions (MITs). Note: T&Cs must be disclosed and explicitly accepted by the cardholder	Authenticate for the amount due on the day. If offering a free trial, authenticate for zero € amount	Authorise for the amount due on the day with: • message type 'CREC' • cryptogram[5] • store the returned TXID
Subsequent MITs	Out of scope	Authorise for the amount due with: • message type 'MREC' • stored credential = Y • and TXID

[5] Plus all other applicable authentication data

Note: Please refer to specifications and supplementary guides on the developer center. Merchants should review the latest specs to note requirements for American Express transactions. When using third party gateways, please refer to their specifications.

14. A checklist for merchants

Checklist	
✓	Upgrade your authorisation connection to support 3DS 2.X as soon as possible
✓	Implement a 3DS 2.X authentication solution, such as the DHPP, or J.P. Morgan's Payments Platform
✓	If you have a mobile app, ensure that mobile app-based checkouts support 3D Secure
✓	Ensure that you can provide all the data elements required in the latest specifications, for example, cryptograms
✓	If you have a subscription, or other MIT payment model, ensure that you can support the Visa / Mastercard stored credential framework
✓	If appropriate for your business, plan to adopt or migrate to 3DS 2.2 to ensure you can fully benefit from SCA exemptions

Please contact your relationship manager if you require support with any of these actions

15. Frequently Asked Questions

Q. What if a merchant does not perform Strong Customer Authentication?

A. From 31 December 2020 (March 2021 for UK-issued customers), SCA must be performed in all situations, unless the merchant flags an exemption, or the transaction is out of scope. Otherwise, the issuer will respond with a soft decline requesting a step-up to two factor authentication. If the merchant ignores that request, the issuer will decline the transaction.

J.P. Morgan recommends that, in the absence of exemptions, the merchant should perform SCA authentication at all times.

Q. Is there an order of importance for exemption flags that can be used in the authorisation message and how many flags can be used?

A. There is no hierarchy of exemption flags. You are expected to only pass one flag. The decision as to which exemption flag to use (low-value, recurring, etc.) should be based on your business model.

Q. If a customer introduces a change to a recurring transaction agreement with a merchant, is SCA required?

A. If the customer requests a change to pricing and terms or pauses or stops and then restarts an agreement, authentication is not required, provided that the agreement T&Cs clearly covers the eventuality of such changes and the merchant has appropriate risk management in place.

If there is any doubt that the agreement covers the change or if there is a risk of fraud, then the change should be treated in the same way as setting up a new agreement.

Q. When merchants accept pre-orders, how long before further action is required?

A. Cryptograms are valid for 90 days for Visa and 30 days for Mastercard. Authorisations are valid for a maximum of 7 days.

Q. For Merchant Initiated Transactions (MITs), how do merchants ensure that the issuer identifies that the transactions are either exempt or out of scope?

A. Merchants need to authenticate on the first transaction and pass evidence of the authentication and all subsequent MIT's, which must be coded to the stored credentials framework.

Q. For merchants who process American Express, is there anything unique they need to consider?

A. American Express acquires their own transactions, and J.P. Morgan conveys merchant transactions to them. As such, American Express is the merchant acquirer. American Express has their own 3D Secure programme called SafeKey. J.P. Morgan's payment solutions support SafeKey, but if you are using an alternative supplier, then confirm their support for it.

Q. Is SCA required for EU merchants selling outside the EU? Please explain how 'two-leg' transactions work.

A. Only transactions where both the issuer and the acquirer are in the EEA are in scope. One-leg transactions are transactions in which one of either the issuer/acquirer are located outside the EEA.

If you are processing through J.P. Morgan Merchant Services Europe, your acquirer is in the EEA, hence you should be aware of how the SCA deadline applies to your transactions.

Additional resources

- Mastercard Authentication Guidelines for Europe version 1.1, 2019
- Visa PSD2 SCA Implementation guide version 02, 2019
- A Guide to Stored Credentials

J.P.Morgan