



UK
FINANCE

Implementation and Strong Customer Authentication (SCA) Ramp Up Plan

Driving UK SCA Readiness

July 2020

UK Industry SCA Implementation Plan



Introduction

In the context of the UK rollout of Strong Customer Authentication (SCA), the Financial Conduct Authority (FCA) announced and agreed to a managed rollout for SCA with UK Finance to give the payments and e-commerce industry extra time to implement SCA with minimum customer impact.

In light of the impact of Covid-19 on key stakeholders, and to minimise the impact on both consumers and e-merchants, the FCA has updated its Strong Customer Authentication page to give an additional six months to implement SCA for e-commerce, with a revised date of 14 September 2021. This can be found [here](#).

The FCA statement clearly expects momentum to be maintained but recognises that additional time may be needed due to the impacts of Covid-19.

The UK Finance SCA programme team has developed this revised detailed implementation plan and the high-level plan. We urge all stakeholders active in e-commerce to take note of the various deadlines and the introduction of a gradual SCA ramp up which will require all parties to be ready by the end of May 2021.

This plan is structured in three key phases and focuses on SCA compliance based on scheme-based payments solutions in order to cover the majority of card-based transactions. The focus of this roll out is a technology called 3DSecure which will help to facilitate the authentication of the majority of card-based transactions.

However, there are other SCA compliant solutions available in the market, such as those provided by Payment Initiation Services (e.g. through Open Banking), Apple Pay, Google Pay as well as other potential solutions.

Executive Summary

UK Implementation Plan and SCA Ramp Up



Following the FCA announcement on the revised date for UK SCA enforcement, which is now 14 September 2021, there is a need to ensure all parties continue working on the delivery of all elements required for SCA readiness and compliance. For that reason UK Finance PMO has focused on the delivery of two elements:

- 1. UK Implementation Plan** – aiming at ensuring all parties are aware of two key points: readiness of all SCA elements is required by May 2021 and UK issuers will start checking randomly from 1 June 2021 if e-commerce transactions are SCA compliant (non-compliant transactions will be soft-declined).
- 2. UK SCA ramp up guidance** – raise awareness about the Issuer led SCA ramp up which starts with the activation of low risk SCA transactions in February 2021 with all SCA transaction flows being activated by May 2021.

The two elements above are crucial foundations to avoid a cliff edge implementation as they are aimed to drive a call to action from e-merchants, acquirers, gateways, issuers and ultimately customers. However it is acknowledged that at least two other critical elements need to be developed to drive a successful outcome:

- 1. Communication** – aiming at delivering an ongoing message to e-merchants which evolves over time
- 2. Monitoring and controlling** – aiming at understanding market readiness and development toward the target environment

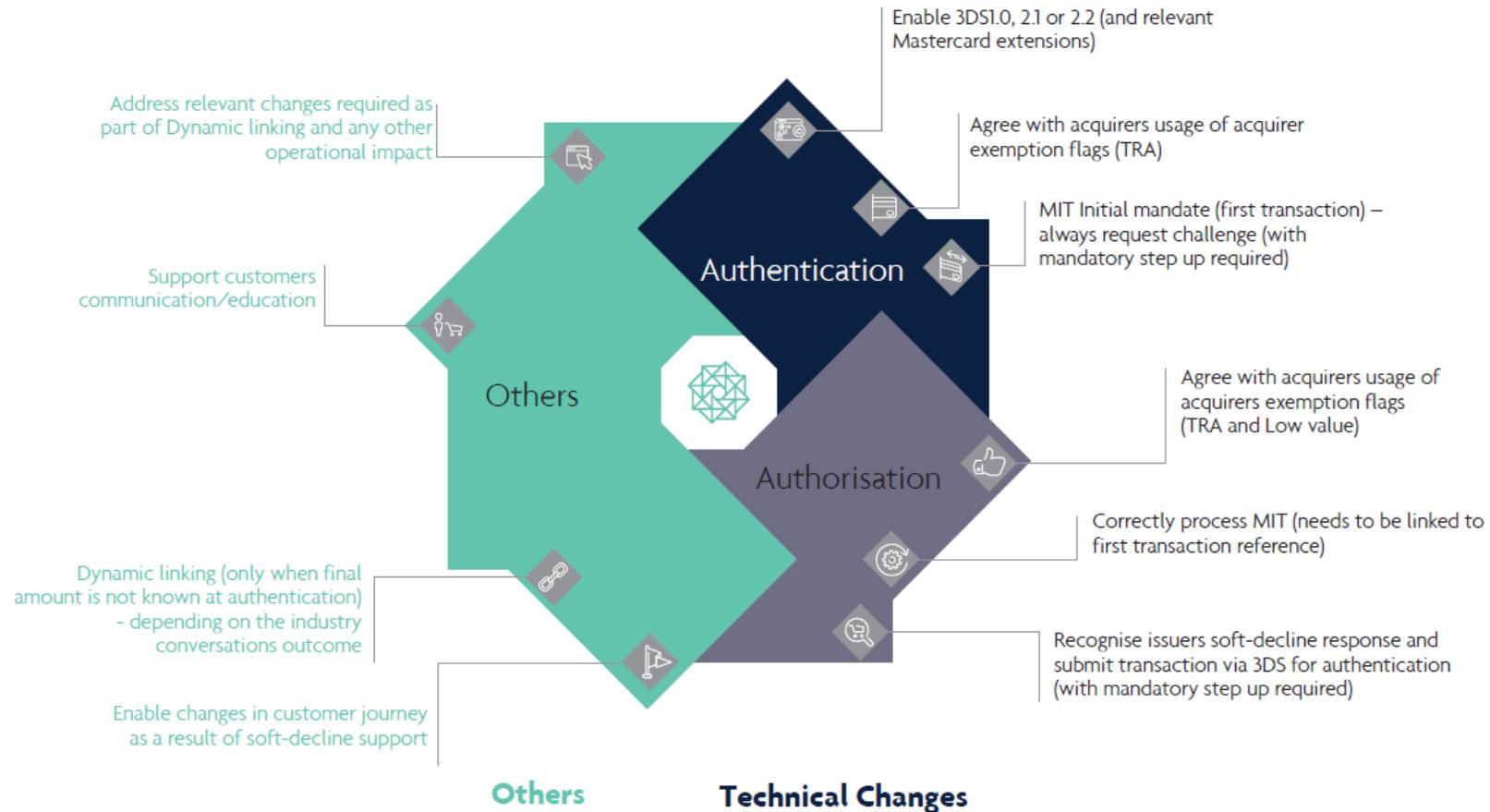
UK Finance's SCA PMO will work on defining a detailed structure for communication and monitoring as a next step

The UK issuer led SCA ramp up proposal outlined in this document has been developed to provide the tools to acquirers and schemes to drive e-merchant readiness to avoid a cliff edge implementation by the SCA enforcement date.

The plan focuses on the UK market only. As the SCA enforcement date is 31 December 2020 across the rest of the EU, e-merchants need to check the specific plans in each of the relevant jurisdictions.

UK SCA Readiness: e-commerce Merchant

E-commerce Merchants target position to ensure SCA compliance and support of exemptions



Merchants high level target SCA position is comprised of mandated and optional activities. Merchants should speak with their gateways and acquirers to define and agree their specific SCA readiness requirements.

Implementation plan

Background and approach

Enabling all SCA journeys

Outlining all SCA transaction flows in scope of the ramp up

Transaction flows			Description	Merchant/Acquirer action	Issuer action	Friction	
Authentication (3DS)	SCA exemptions	Issuer exemptions	<ul style="list-style-type: none"> TRA thresholds: <£90, <£215, <£430 Others: trusted beneficiaries, delegated authority 	Via 3DS	TRA Applied	Low	
		Acquirer exemption: TRA ^{LR}	<ul style="list-style-type: none"> TRA (triggered by acquirers – 3DS2.2): <£90, <£215, <£430 		TRA accepted or declined		
	SCA step ups	Above issuer TRA	<ul style="list-style-type: none"> Triggered by issuers 		Transaction stepped up	Medium	
		E-merchant request ^{LR}	<ul style="list-style-type: none"> Triggered by e-merchants/acquirers and recognised by issuers (e.g. first MIT, soft decline, etc) 				
Authorisation	Correct flagging ^{LR}	Acquirer exemption: TRA	<ul style="list-style-type: none"> All journeys are triggered by e-merchants/acquirers and recognised by issuers TRA threshold based on acquirer fraud ratios LVT exemption up to £30 	Authorisation with correct flag	Transaction to be decided	None	
		Acquirer exemption: LVT					
		Secure Corporate Payment exemption					
		MIT (recurring)					
	Soft declines	CLV	Out of scope	<ul style="list-style-type: none"> Triggered by issuers 	Authorisation with incorrect/no flag	Soft declined (<i>request to send via 3DS</i>) OR Declined (<i>new transaction to be sent via 3DS or correct flag applied</i>)	High
			Total Low Value exemption (up to £90)				
	Non-flagged	In scope with no exemptions (and issuer unable to authenticate)	<ul style="list-style-type: none"> Issuers will need to soft-decline or decline the transaction 				

^{LR} Low risk transaction flow

UK SCA Implementation Plan Approach

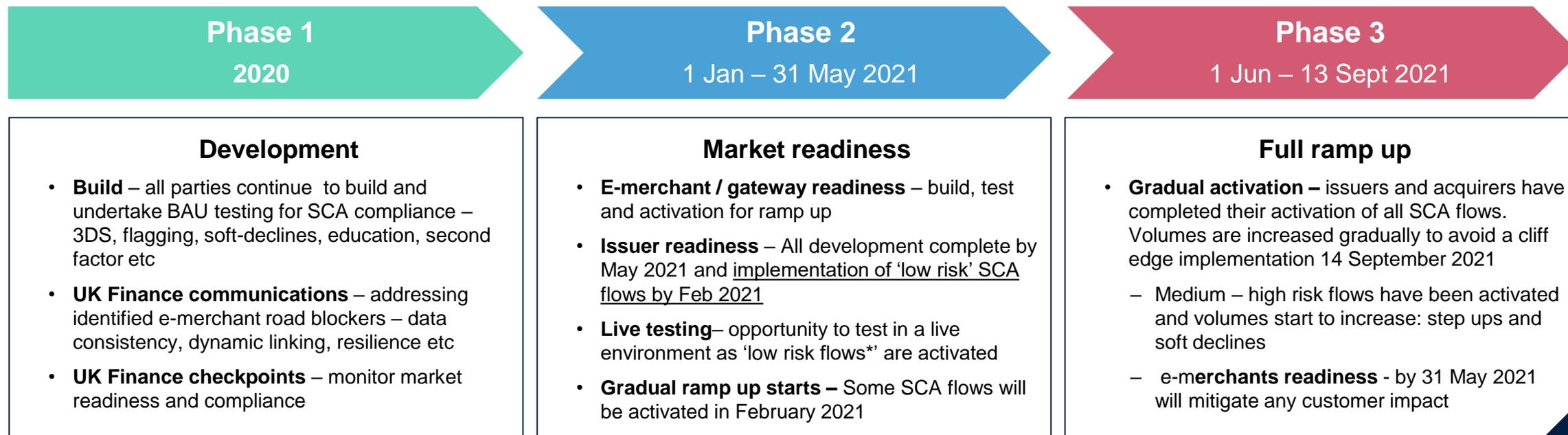
Driving action by raising awareness



Key Objectives

- Ensure all parties understand the key high level milestones and the industry plans for a SCA ramp up
- Ensure all parties continue working towards their SCA readiness by **31 May 2021**

Phased Delivery



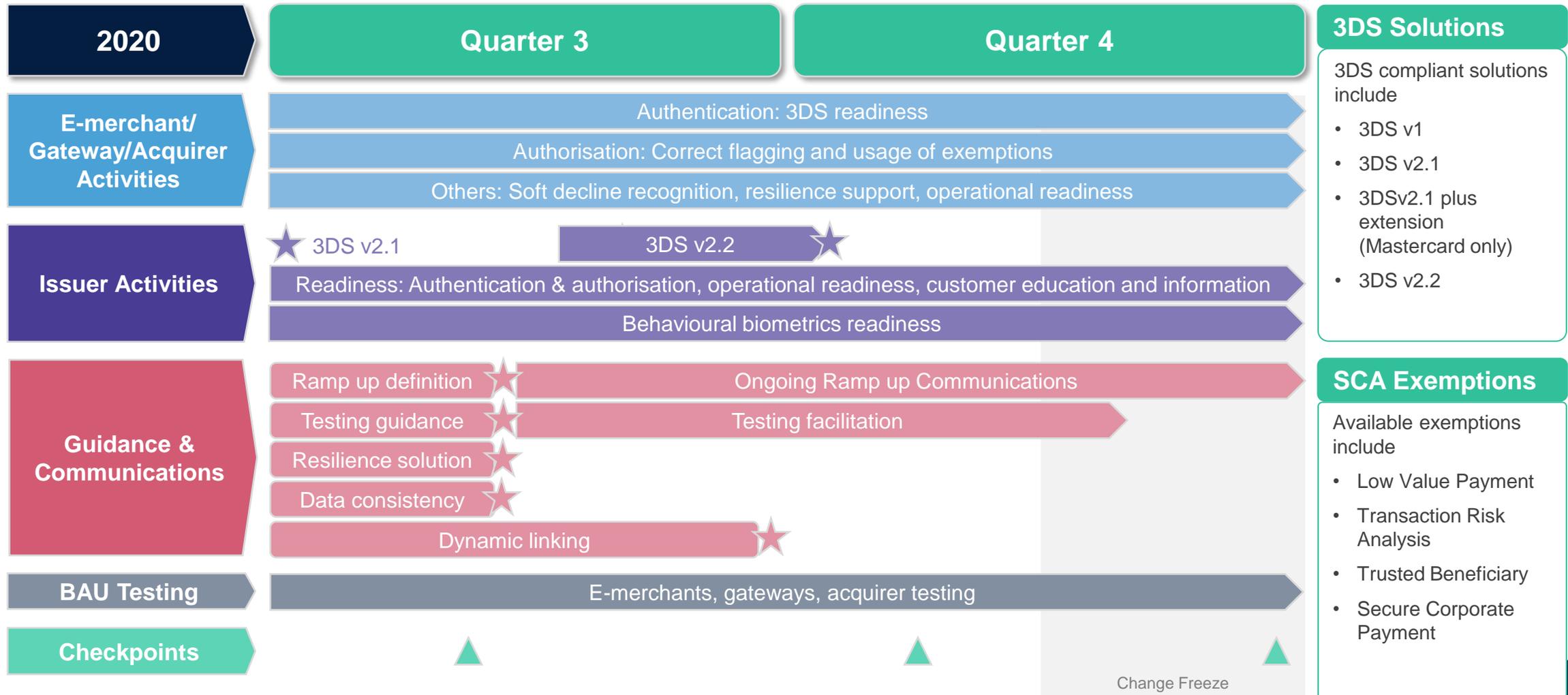
* Low risk flows: Issuer recognition of acquirer TRA and e-merchant step up request (via 3DS) and correct flagging (via authorisations). See slide 13 and 14 for detailed information

Implementation Plan

Infographic

UK Industry SCA Implementation Plan

UK Only – 2020 activities (The enforcement date is 31 December 2020 across the rest of the EU)

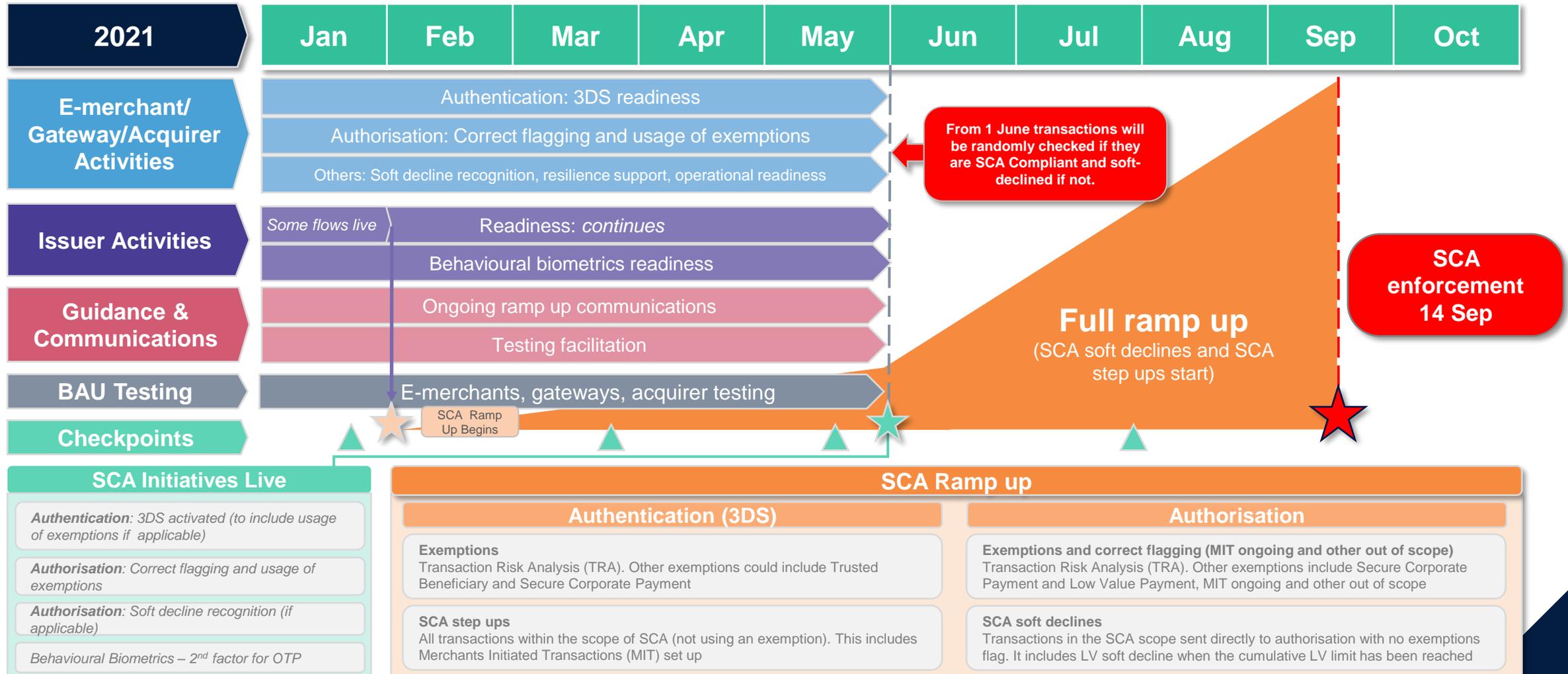


★ Denotes delivery milestone

Through out the period, issuers will continue challenging transactions as per their decisioning strategies

UK Industry SCA Implementation Plan

UK Only – 2021 activities (The enforcement date is 31 December 2020 across the rest of the EU)



Through out the period, issuers will continue challenging transactions as per their decisioning strategies

Merchant readiness

3DS and/or correct flagging via authorisations

Strong Customer Authentication

UK readiness overview: 3DS and/or correct flagging via authorisations



- The UK SCA enforcement date is now 14 September 2021, this means **e-commerce transactions that are unable to be authenticated or those without exemptions will be declined after that date.**
- To avoid a cliff-edge implementation by enforcement date, SCA will be introduced gradually (SCA ramp up) in the UK from 1 June 2021:
 - UK issuers will start checking randomly if e-commerce transactions are SCA compliant (non-compliant transactions will be soft-declined)
- **E-merchants need to be ready by the end of May 2021** as this will be critical to mitigate any SCA impact, to achieve this merchants need to:
 - activate 3DS and/or
 - **correctly flag transactions via authorisations** i.e. acquirer exemptions, out of scope and MIT ongoing

Exemptions	
Exemption	Issuer / acquirer
Low value payment	Acquirer
Transaction risk analysis	Issuer and acquirer
Trusted beneficiary	Issuer
Secure corporate payment	Issuer

SCA Initiatives Required
Authentication: 3DS activated (to include usage of exemptions if applicable)
Authorisation*: Correct flagging (to include usage of acquirer exemptions if applicable)
2nd factor for OTP: Behavioural biometrics (if applicable)

* Acquirers can apply Low Value (LV) and Transactions Risk Analysis (TRA) exemptions for transactions sent directly to authorisations

Strong Customer Authentication

3DS: Enabling authentication and usage of SCA exemptions

3DS

- Enables the issuer to apply SCA
- Facilitates the usage of **issuer** (all versions) and **acquirer** exemptions (version 2.1 plus* extensions and version 2.2 only)
- There are three main versions of 3DS in the market:
 - 3DS version 1.0
 - EMV 3DS version 2.1 (and 2.1 with extensions)
 - EMV 3DS version 2.2 (and 2.2 with extensions)
- All three versions are SCA compliant, however 3DS v2.1 or v2.2 has features that will reduce friction at checkout compared to version 1



However it is important to remember that SCA compliance can be achieved via enabling 3DS and/or flagging transactions correctly (i.e. acquirer exemptions, out of scope or MIT ongoing) via authorisation

* Mastercard only

Strong Customer Authentication

3DS: Considerations when choosing a version to support



3DS Version	3DS v 1	EMV 3DS v2.1	EMV 3DS v2.2*
Journey optimised for mobile and tablet devices	x	✓	✓
A choice of authentication options can be provided to customers during check out (authentication methods to be defined by issuers)	x	✓	✓
TRA exemption can be applied by issuers	✓	✓	✓
TRA exemption can be applied by acquirers**	x	x	✓
Customer journeys with delayed shipment/delivery (post 90 days) are supported (no need for re-authentication using SCA)	x	✓	✓
MIT set up can be flagged and recognised by issuer. Therefore, customers do not need to be authenticated for MIT series	x	✓	✓
Trusted beneficiary exemption support (if offered by issuer)	x	x	✓
Delegated authentication support	x	x	✓

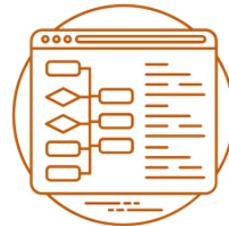
* 3DS v2.1 plus extensions will support most of the functionality of 3DS2.2

** Acquirers can apply TRA exemption directly via authorisations regardless of the 3DS version being used

Second Factor for OTP

Support requested to e-merchants as part of behavioural biometrics

- Behavioural biometrics is the industry recommended solution as the second factor authentication for (non-app) online transactions when using OTP as an authentication.
- This approach aims to minimise any customer impact during the check out by removing the need for customers to have a static password or their card PIN, in addition to an OTP. Past experience in the UK and internationally has shown this to be highly disruptive, whilst creating new opportunities for fraud.
- Behavioural biometrics solutions will require JavaScript integration for 3DSecure browser-based authentication challenge flows.
- Therefore, e-merchants are encouraged **not to implement restrictions** on their websites that could interfere with such scripts. Possible restrictions could be related to the inclusion of third-party content, CORS restrictions, or similar.



E-merchants are encouraged to ensure that when enabling JavaScripts they do so in a safe manner so as to allow the usage of behavioural biometrics for web browser shopping whilst providing customers with a convenient way of authenticating.

This in turn will avoid the unwelcome need to use other authentication solutions which could add friction to the customer's online check out experience.

