UK FINANCE

Strong Customer Authentication (SCA)

Proposed Managed Rollout

26 July 2019

Version 20

Request for a managed rollout

Why does the industry need a managed rollout

Context: UK Finance and our members are fundamentally committed to fighting fraud and have been working on the implementation of PSD2 and the accompanying requirements in both spirit and letter of the law for a number of years. The related EBA Regulatory Technical Standards on Strong Customer Authentication (SCA), aimed at making electronic transactions more secure, apply from the 14 September 2019.

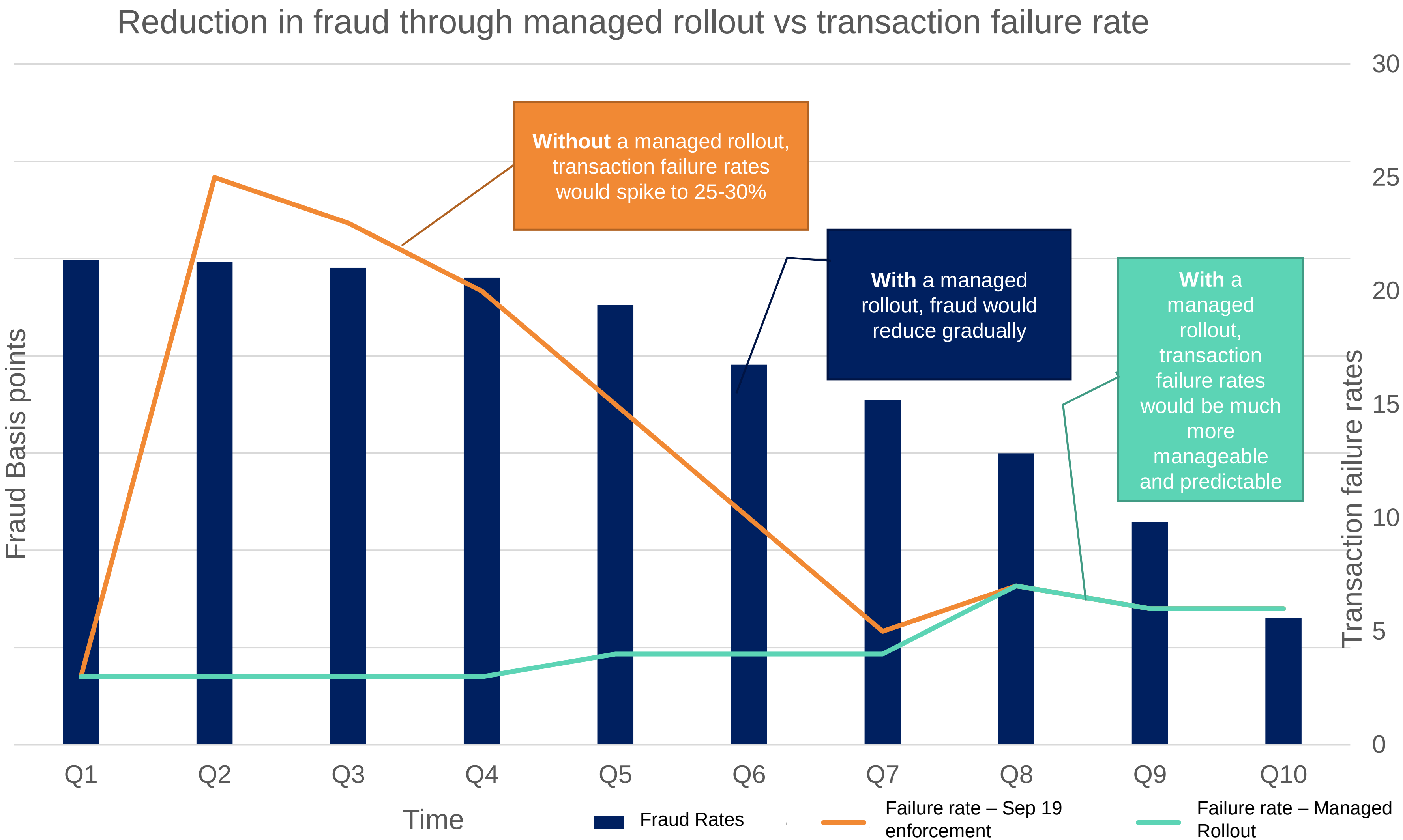
Issue: Despite the best efforts of the payments and retail sectors, introduction of these new rules has experienced a number of setbacks, including regulatory uncertainty (e.g. EBA Q&A tool and recent EBA Opinion still revising guidance), insufficient or delayed availability of technological solutions, and low awareness among merchants. **Research indicates that more than 75% of merchants are unaware of SCA requirements and less than 5% of merchants are currently using 3D Secure 2.1.** The implementation of SCA requires merchants and PSPs to work together with technology suppliers, card schemes and many others to deliver SCA in a way which works well for customers. The assumptions and goals which the industry was previously working towards was also moved significantly by the EBA Opinion.

Impact of no change: Blanket introduction of SCA in September 2019 will lead to significant negative impacts for consumers across the EU. Transactions will be declined, bill payments missed, and high levels of confusion experienced by consumers not understanding why they cannot make purchases. **Estimates suggest around 25-30% of transactions will fail as issuers will decline any non-3D Secure transaction not subject to an exemption**; or that they may be unable to identify exemptions. This would have a significant impact on consumers and the retail sector across the EU. We focus in this paper on 3D Secure as it facilitates the vast bulk of e-commerce transactions. The impact of no change in the authentication journey also results in additional friction, the industry proposes to smooth this journey as far as possible through our proposals on two strategic solutions (see later slides).

Request: The payments and retail sectors have prepared this managed rollout. Due to the cross-border nature of payments, we believe this should be a European-wide solution as merchants are often centrally acquired i.e. from another member state. A managed rollout will achieve the overall aims of PSD2 and SCA in a way which gradually reduces fraud whilst protecting retail business and encouraging better customer experience across the EU. **Having engaged across the retail sector and finance sector, we believe an 18 month managed rollout is plausible for the rollout of OTP. However, for full compliance and in order to avoid delivering a sub-optimal solution (i.e. OTP + knowledge), the industry needs an additional six months (i.e. 24 months) in order to deliver an accessible solution based on behavioural biometrics (OTP + inherence).** The industry is fully committed to fighting fraud and over and beyond the managed rollout are working on a number of other strategic solutions which fight fraud and will continue to invest in these in the medium to longer term initiatives outside of the scope of this proposal.

Projected reduction in fraud rates with a managed rollout*

For e-commerce channels



Without a managed rollout, transaction failure rates would spike to 25-30%

With a managed rollout, fraud would reduce gradually

With a managed rollout, transaction failure rates would be much more manageable and predictable

* UK Finance in conjunction with members performed the accompanying prediction in fraud rates as transactions move towards full SCA operational readiness. However, this is based on a best endeavours basis and cannot be relied upon. There are a number of assumptions UK Finance has had to make, including:

- We have not been able to account for seasonal adjustments i.e. there is a usual spike in fraud around periods of high sales e.g. Black Friday and the festive period.
- This does not discount a significant rise in fraud that a data breach may lead to. Experience has pointed to the fact there are significant spikes in fraud following mass data breaches outside of the financial sector.
- We did not have full availability of all data which has resulted in estimations being made in some cases.

Even at 5% transaction failure, several organisations from the merchant community have noted they would consider having to make profit warnings to the market

Outline of strategic direction

UK FINANCE

Two concurrent paths

Summary: The UK is and will remain one of the most sophisticated payment markets in the world with some of the best anti-fraud tools currently in use. The UK will maintain this long term view of the fight against fraud and with the problems that come with a lack of readiness for Strong Customer Authentication (and with the clarification from the EBA), by implementing a long term rollout of compliant SCA solutions which deliver the best for customer experience whilst being at the cutting edge of innovative authentication to drive down fraud. We therefore propose two strategic but concurrent paths. The first is a biometric and mobile app based solution for more sophisticated customers, however considering that not all customers use mobile banking, we also propose a long term accessible solution which suits the majority in society. This takes the form of a one time passcode (OTP) plus behavioural biometrics (inherence) to deter fraudsters and combat effectively against scams and social engineering. The industry will also focus on the rollout of exemptions to ensure the best customer experience, but also alternative authentication mechanisms for the most vulnerable in our society.

To facilitate ongoing commitment to the strategic direction outlined, UK Finance is setting up a central programme management office which will begin work in mid-August. This PMO will come up with additional planning and metrics. Its governance will be broad and open.

UK Finance are also scoping a consumer and retail communications plan for SCA to ensure both retailers and customers are aware of the changes coming over and above existing member communications. Once fully scoped and agreed we will share directly with the FCA.

Biometric and mobile app based solutions

The industry recognise that long term, the solution which works best for many (and a growing number) of customers is to allow for authentication through biometric and mobile app based solutions. However, there are a number of dependencies related to mobile banking adoption, versioning of 3DSecure (app to app redirection is needed) and the potential build of biometric solutions for many issuers. This will take time to fully implement.

18-24 Months

Long term accessible solutions

Plus

The long term accessible solutions of the industry will be one time passcode based (possession) plus another factor (knowledge or inherence). Given the views expressed in the EBA Opinion the industry will need time to implement an issuer controlled behavioural biometric (such as keystrokes + spending data) over and above the OTP, but also to retrofit their implementations with a knowledge factor such as passcode or question (only as a fallback).

18-24 Months

Tactical solutions

The industry was prepared and ready to implement SCA through one time passcodes. Given the impact of the EBA Opinion (with card details not being considered a factor) the industry will need time to implement the additional factors proposed. However, given the industry's commitment to reducing fraud, OTP will be phased in through active testing, whilst the second factor is built.

For a number of reasons the recommended implementation is an OTP in combination with behavioural biometrics, however as a fallback the industry needs to retrofit to include another knowledge factor, the industry will need 24 months to fully implement a behavioural biometric solution which is fully future proofed.

Exemptions

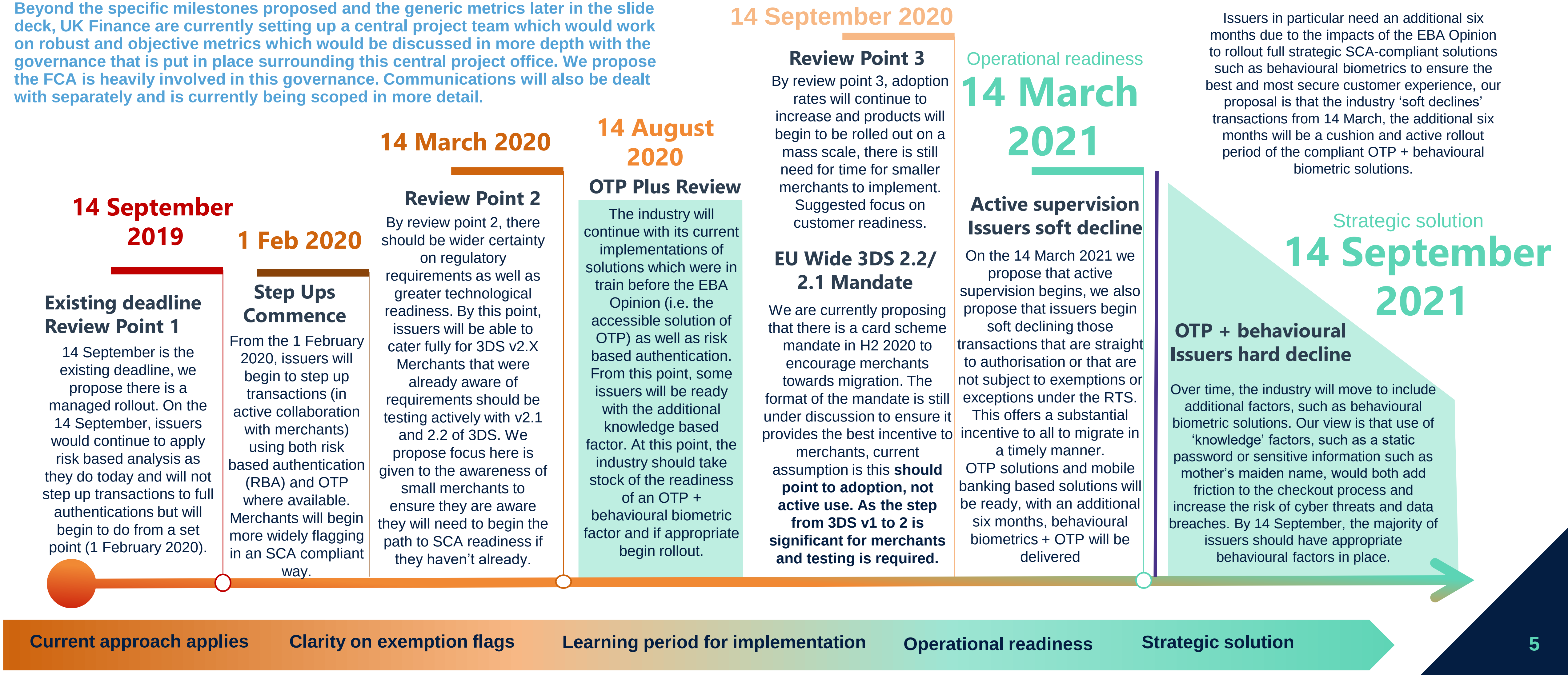
To create the right incentives for industry and merchants, exemptions should also be phased in over time, however it will take some time for some to be fully scoped and operationalised to be as consistent as possible. These are 1. Transaction Risk Analysis (our view is this should be phased in over the 24 month period in a way agreed under the project management office) and 2. Trusted beneficiaries (our view is that the industry will need time to deliver more holistic solutions for this, but again these will be phased in over time but will take 18+ months to come in)

Proposed managed rollout

UK FINANCE

Overall high level timelines for the roadmap

Beyond the specific milestones proposed and the generic metrics later in the slide deck, UK Finance are currently setting up a central project team which would work on robust and objective metrics which would be discussed in more depth with the governance that is put in place surrounding this central project office. We propose the FCA is heavily involved in this governance. Communications will also be dealt with separately and is currently being scoped in more detail.



14 September 2019

Existing deadline Review Point 1

14 September is the existing deadline, we propose there is a managed rollout. On the 14 September, issuers would continue to apply risk based analysis as they do today and will not step up transactions to full authentications but will begin to do from a set point (1 February 2020).

1 Feb 2020

Step Ups Commence

From the 1 February 2020, issuers will begin to step up transactions (in active collaboration with merchants) using both risk based authentication (RBA) and OTP where available. Merchants will begin more widely flagging in an SCA compliant way.

14 March 2020

Review Point 2

By review point 2, there should be wider certainty on regulatory requirements as well as greater technological readiness. By this point, issuers will be able to cater fully for 3DS v2.X Merchants that were already aware of requirements should be testing actively with v2.1 and 2.2 of 3DS. We propose focus here is given to the awareness of small merchants to ensure they are aware they will need to begin the path to SCA readiness if they haven't already.

14 August 2020

OTP Plus Review

The industry will continue with its current implementations of solutions which were in train before the EBA Opinion (i.e. the accessible solution of OTP) as well as risk based authentication. From this point, some issuers will be ready with the additional knowledge based factor. At this point, the industry should take stock of the readiness of an OTP + behavioural biometric factor and if appropriate begin rollout.

14 September 2020

Review Point 3

By review point 3, adoption rates will continue to increase and products will begin to be rolled out on a mass scale, there is still need for time for smaller merchants to implement. Suggested focus on customer readiness.

EU Wide 3DS 2.2/ 2.1 Mandate

We are currently proposing that there is a card scheme mandate in H2 2020 to encourage merchants towards migration. The format of the mandate is still under discussion to ensure it provides the best incentive to merchants, current assumption is this **should point to adoption, not active use. As the step from 3DS v1 to 2 is significant for merchants and testing is required.**

Operational readiness

14 March 2021

Active supervision Issuers soft decline

On the 14 March 2021 we propose that active supervision begins, we also propose that issuers begin soft declining those transactions that are straight to authorisation or that are not subject to exemptions or exceptions under the RTS. This offers a substantial incentive to all to migrate in a timely manner. OTP solutions and mobile banking based solutions will be ready, with an additional six months, behavioural biometrics + OTP will be delivered

Issuers in particular need an additional six months due to the impacts of the EBA Opinion to rollout full strategic SCA-compliant solutions such as behavioural biometrics to ensure the best and most secure customer experience, our proposal is that the industry 'soft declines' transactions from 14 March, the additional six months will be a cushion and active rollout period of the compliant OTP + behavioural biometric solutions.

Strategic solution

14 September 2021

OTP + behavioural Issuers hard decline

Over time, the industry will move to include additional factors, such as behavioural biometric solutions. Our view is that use of 'knowledge' factors, such as a static password or sensitive information such as mother's maiden name, would both add friction to the checkout process and increase the risk of cyber threats and data breaches. By 14 September, the majority of issuers should have appropriate behavioural factors in place.

Detailed roadmap and milestones

Activities undertaken by all parties

Milestone One

Aim for 30% of merchants on 3DS 2.X

14 March 2020

Milestone Two

Aim for 90% of merchants on 3DS 2.X

14 September 2020

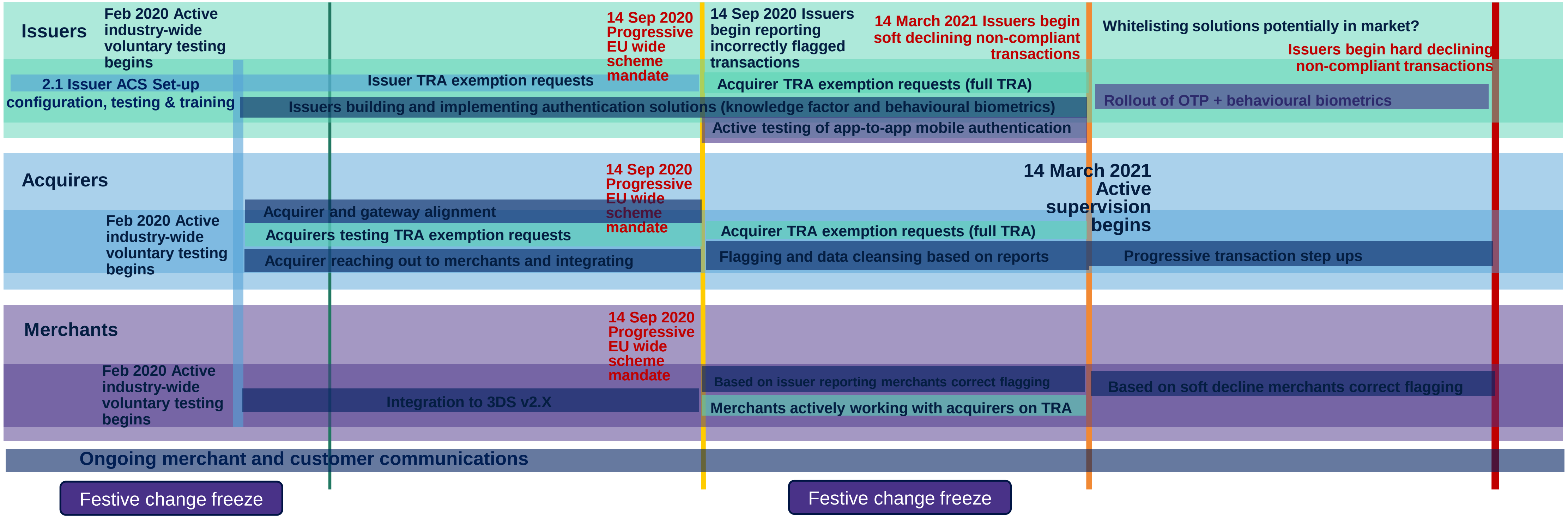
Milestone Three

Aim for 75% of all transactions to be fully SCA compliant and correctly flagged

14 March 2021

End of Rollout

14 September 2021



Issuers

Feb 2020 Active industry-wide voluntary testing begins

2.1 Issuer ACS Set-up configuration, testing & training

Issuer TRA exemption requests

14 Sep 2020 Progressive EU wide scheme mandate

14 Sep 2020 Issuers begin reporting incorrectly flagged transactions

14 March 2021 Issuers begin soft declining non-compliant transactions

Whitelisting solutions potentially in market?

Issuers begin hard declining non-compliant transactions

Acquirer TRA exemption requests (full TRA)

Issuers building and implementing authentication solutions (knowledge factor and behavioural biometrics)

Rollout of OTP + behavioural biometrics

Active testing of app-to-app mobile authentication

Acquirers

Feb 2020 Active industry-wide voluntary testing begins

Acquirer and gateway alignment

Acquirers testing TRA exemption requests

Acquirer reaching out to merchants and integrating

14 Sep 2020 Progressive EU wide scheme mandate

14 March 2021 Active supervision begins

Acquirer TRA exemption requests (full TRA)

Flagging and data cleansing based on reports

Progressive transaction step ups

Merchants

Feb 2020 Active industry-wide voluntary testing begins

Integration to 3DS v2.X

14 Sep 2020 Progressive EU wide scheme mandate

Based on issuer reporting merchants correct flagging

Merchants actively working with acquirers on TRA

Based on soft decline merchants correct flagging

Ongoing merchant and customer communications

Festive change freeze

Festive change freeze

Other cases that need flexibility

Vulnerable customers and hospitality

Vulnerable customers – indefinite flexibility

There are customers that have genuine difficulties with the requirements of Strong Customer Authentication, due to blindness, mental health problems or physical disabilities and the requirements for these customers vary, with some unable to use a phone, card reader or other form of token and therefore unable to react to the challenge stage required under SCA.

Firms will continue to cater for these customers and take an indefinite risk-based approach to compliance and in many cases disapply the requirements of SCA whilst still using tools like risk based authentication which are invisible to the customer to continue to keep these customers protected from fraud.

Hospitality and travel – three year flexibility

The hotel sector is incredibly complex with many parties involved and transactions flowing through a multitude of systems at a global level. As just one example, hotels operate under a variety of ownership models despite, in some cases, trading under a common brand or as part of an international group.

This sector therefore requires changes through their many intermediaries such as Online Ticket Agency (OTA), Global Distribution System (GDS), Booking Engine (BE) or Central Reservation Office (CRO).

Given the complexity of this industry we therefore propose they are given additional time to fully meet SCA requirements. Industry will seek to do further analysis on how this is operationalised through the UK Finance project management office.

Other considerations we have through physical channels such as in the charities sector will be addressed through our concurrent paper on contactless.

Proposed metrics to be measured

High level metrics and dependencies

Customer Readiness

Phone Numbers Captured

Email Addresses Captured

Mobile Apps in Active Use

Merchant Readiness

Implementation of 3DS 2.X

Number testing or actively using

Fraud Reduction

Constant monitoring of fraud

Building of transaction risk analysis

Issuer dependencies:

Integration and full testing with Access Control Server (ACS) providers. Practically, issuers use a limited number of gateways and therefore if there is a delay with the ACS provider it affects a number of issuers concurrently. To address this dependency, UK Finance proposes to work actively with ACS providers through the managed rollout to help ensure the best sequencing of activities and 'air traffic control' of requirements.

Issuer metrics

Phone Numbers and Emails Captured (30% at Milestone one) (60% at Milestone two) (90%+ at Milestone three)

Mobile Apps in Active Use

By Milestone three majority of issuers should facilitate biometric and app based solutions based on app-to-app redirections

Acquirer metrics

At Milestone one 30% of merchants should be on 3DS 2.X and 90% at Milestone two

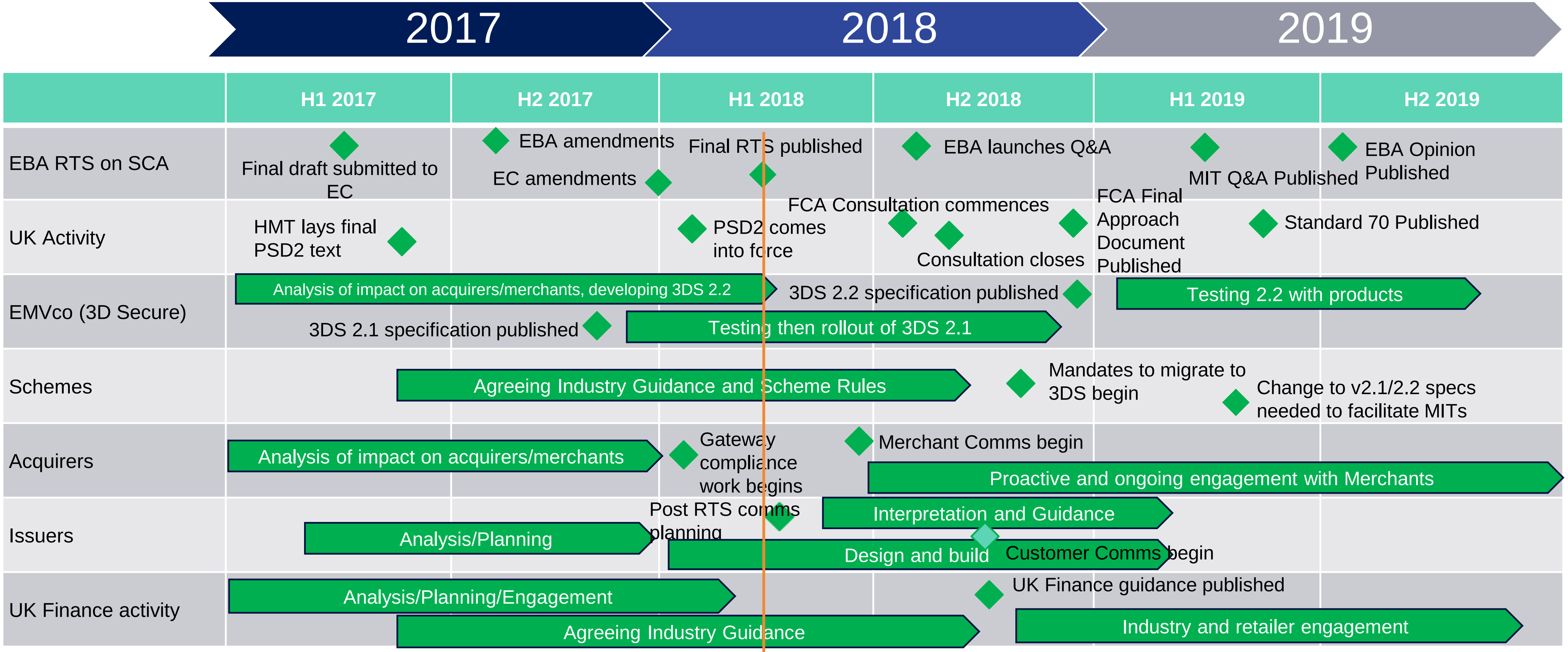
By Milestone three 90% of merchants should be on 3DS 2.2 with 90% correct flagging

Merchant and acquirer dependencies:

Merchants often rely on gateway providers for their solutions and given the large number of gateways, which are often unregulated entities, it is difficult to coordinate between acquirers and gateways. To mitigate this, UK Finance proposes that there are regular gateway events facilitated through the project management office being set up to cater for the proposed managed rollout.

Industry action to date

Backwards looking timeline of change



2017

2018

2019

H1 2017 | H2 2017 | H1 2018 | H2 2018 | H1 2019 | H2 2019

EBA RTS on SCA

Final draft submitted to EC

EBA amendments

EC amendments

Final RTS published

EBA launches Q&A

MIT Q&A Published

EBA Opinion Published

UK Activity

HMT lays final PSD2 text

PSD2 comes into force

FCA Consultation commences

Consultation closes

FCA Final Approach Document Published

Standard 70 Published

EMVco (3D Secure)

Analysis of impact on acquirers/merchants, developing 3DS 2.2

3DS 2.2 specification published

Testing 2.2 with products

3DS 2.1 specification published

Testing then rollout of 3DS 2.1

Schemes

Agreeing Industry Guidance and Scheme Rules

Mandates to migrate to 3DS begin

Change to v2.1/2.2 specs needed to facilitate MITs

Acquirers

Analysis of impact on acquirers/merchants

Gateway compliance work begins

Merchant Comms begin

Proactive and ongoing engagement with Merchants

Issuers

Post RTS comms planning

Interpretation and Guidance

Analysis/Planning

Design and build

Customer Comms begin

UK Finance activity

Analysis/Planning/Engagement

UK Finance guidance published

Agreeing Industry Guidance

Industry and retailer engagement

Industry planning/implementation could not start in earnest until this date (March 2018), with the publication of the final RTS, due to implementation uncertainties. Not all guidance was issued by this point (e.g. MIT question March 2019, Q+A ongoing)