Impact of implementing SCA on e-Commerce

June 2019

cleverAdvice

EXECUTIVE SUMMARY

The industry is not ready to launch Strong Customer Authentication in September 2019 as set by PSD2.

Implementing SCA requirements is complex and time consuming as involves upgrading payment systems of issuers, acquirers, card schemes, processors and merchants. The implementation period allowed by the regulation was actually shortened due to amendments to the requirements after the final version of the regulatory technical standards was issued.

As such many issuers and acquirers will not be in a position to offer harmonized SCA solutions with a comprehensive set of features including exemptions, and most merchants have not integrated their systems accordingly. Inconsistent implementation will expose consumers and businesses to a variety of processes but also to potential inconveniences as payments systems have not being tested at scale and may not be able to handle the much larger volumes of SCA requests.

Issuers had no sufficient time to develop optimized authentication processes with the level of user-friendliness to retain customer conversion at checkout. Also, they will have to invest time and resources in collecting/updating their customer contact details to ensure they will be able to smoothly authenticate transactions.

Impact of fragmented implementation will cause the decline of several non-fraudulent transactions, resulting in lost sales – estimated at € 50bn – significant rise in abandonment, higher processing costs and customer complaints, and disrupt trust in the new security standard and confidence in e-commerce.

We call for an 18-month managed transition period to allow the industry as a whole to get ready. During this period issuers, acquirers, payment schemes and processors will have a chance to upgrade their payment systems to embrace all features including exemptions and merchants restructure their checkout flow. This will allow offering uniform procedures and consistent approaches, retaining online sales and ensuring a satisfactory customer experience.

As three out of four merchants and many consumers are unaware of SCA a managed transition period will be useful to build awareness to ensure a smooth transition to the new security standard. Acquirers will have an opportunity to properly inform merchants of integrations and testing required, while PSPs and payment schemes will guide merchants to educate consumers and businesses on the benefits of SCA and engage them in dealing with the new authentication process.

INTRODUCTION

As the digital economy plays an increasing part in our lives it is vital that electronic payments are increasingly secure. In an effort to increase European payments security and reduce fraud, all electronic payments will need to be authenticated via Strong Customer Authentication before the end of 2019.

Strong Customer Authentication (SCA) is an authentication method based on the use of two or more elements categorized as *knowledge* (something only the user knows), *possession* (something only the user possesses) and *inherence* (something the user is). These elements must be independent from one another, so that the breach of one does not compromise the reliability of the others, and designed to protect the confidentiality of the authentication data.

On 27 November 2017 the European Commission amended the European Banking Authority Final Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication – often referred as RTS on SCA and CSC – published on 23 February 2017.

The RTS on SCA and CSC is a set of rules aimed at improving security of internet payments that supplement the EU Directive 2015/2366 – known as Revised Payment Services Directive or PSD2 – that mandates the requirements for payment services providers to:

a. Apply the procedure of strong customer authentication as per Art. 97 of PSD2;
b. Exempt from applying strong customer authentication under specific limited conditions;
c. Protect the confidentiality and the integrity of the payment service user's personal security credentials;
d. Establish common and secure open standards for the communication between the parties involved in a payment transaction – i.e. account servicing payment service providers, payment initiation service providers, account information service providers, payers, payees and other payment service providers.

The RTS on SCA and CSC were published in the Official Journal of the European Union on 13 March 2018 and will apply from 14 September 2019.

Strong customer authentication (SCA) will strongly impact the convenience and speed of online shopping as the mandate to apply the RTS on SCA and CSC will result in significant burden for the industry due to the high cost of amending existing IT platforms, long implementations, higher processing cost and loss of online sales resulting from higher abandonment at checkout caused to the wider application of SCA.

1. Readiness to PSD2

i. Complying with PSD2: current state of play

Most banks currently do not have an optimized SCA solution. They were not able to develop one due to the large effort– in terms of budget and resources – they needed to deploy in the last couple of years to meet the PSD2 Open Banking requirements. Another reason is the late availability of specification for 3DS 2.2, the only comprehensive solution that support all exemptions from SCA along with full Transaction Risk Analysis capabilities and the level of user-friendliness needed to prevent the decline of non-fraudulent transactions and a significant rise in abandonment. The late availability of 3DS 2.2 is due to a number of important clarifications on the SCA requirements that were issued months after the final RTS were published, so the card schemes had to amend the 3DS 2.1 protocol that was under development. As such the actual time that has been allowed to amend platforms and integrate solutions to support all features provisioned in the RTS has been shorter than the regulators intended. In fact, changes in the actual requirements after the final regulations were issued were not followed by the provision

of additional time to implement the amended technical standards and resulted in a high degree of inconsistency.

Most merchants across Europe are also not ready to support SCA. As most European online purchases are regulated via payment cards, assessing merchant readiness in applying SCA to card payments it key. Currently approximately 75% of European merchants do not offer 3DSecure at checkout and 20% have deployed 3DS version 1.0 which offers no mobile interface, a clear disadvantage when over 50% of European consumers make purchases via their mobile devices[1].

Today fewer than 5% of merchants offer 3DS 2.0 or 2.1, both RTS compliant, but unable to support a number of key exemptions from the application of SCA as provisioned by the RTS. Only a handful of merchants are planning to test 3DS 2.2 after September 2019, when protocols will be available and certified vendors expect to be ready for testing.

	Features (incremental)	Specifications available	EMVCo testing available	Certified vendors ready for testing	Commercial availability
3DS 2.1	• Real time dynamic linking • Mobile device interface • Non-payment authentication • Transaction Risk Analysis (limited capability) • Enhanced data sharing • Biometric authentication • Merchant Initiated Transactions *(varied implementation)*	Oct 2017	Aug 2018	Nov 2018	Feb 2019
3DS 2.2	• Additional device compatibility • Transaction Risk Analysis (full capability) • Trusted beneficiary exemption • Enhanced user experience • Merchant Initiated Transactions	Dec 2018	Jun 2019	Sept 2019	Jan 2020

Chances are that in September many merchants, consumers and businesses will not be able to take advantage of exemptions and must apply SCA to all transactions, resulting in 25-30% of genuine, non-fraudulent transactions expected to be declined and a significant increase in abandonment at checkout from today's level resulting in lost sales and dissatisfied customers. In addition, due to the lack of sufficient time the level of reliability of the SCA solutions will be uncertain as no testing was carried-out.

Parts of the regulation are still open to interpretation with a number of questions unanswered and issues unresolved which explains the ongoing initiatives from several market players aimed at a correct interpretation of the norms, which triggered the EBA to publish their opinions[2] aimed at providing guidance on a number of aspects.

The PSD2 timeline to meet both the September mandate for SCA and the provision of an environment for third-party service providers to test APIs by 14 March is resulting too challenging for many banks, as nearly half (41%) failed to meet the March deadline.

Market evidence reflects the widespread difficulties in implementing complex and intertwined requirements – the need of banks to comply with the regulation and the needs of merchants to offer user-friendly checkouts and benefit from a full set of exemptions – all in a timeframe that is proving too tight.

ii. Defining readiness

Defining readiness is paramount to ensure a harmonized level of services and ultimately trust and confidence in the payment ecosystem.

[1] *Mastercard survey 2018*
[2] *Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC 13 June 2018 (EBA-Op-2018-04)*

We define two level of readiness for PSPs and merchants:

- *Compliance readiness*: Ability to offer solutions that offer the minimum set of features to comply with PSD2;
- *Operational readiness*: Ability to offer solutions that offer all features provisioned by PSD2, including exemptions and options. In addition, comprehensive testing has been completed to ensure a high level of reliability.

When a PSP – including issuers and acquirers – or merchant only meets compliance readiness, it is only able to offer solutions that do not allow the application of exemptions from SCA nor authentication via Transaction Risk Analysis as provisioned by the RTS on SCA and CSC. This will result in sub-optimal customer experience, unnecessary decline of genuine, non-fraudulent transactions and a high number of abandonments.

On the other hand, operationally ready PSPs and merchants offer solutions that embrace a comprehensive set of features such as the ability to offer all exemptions from SCA, including whitelisting trusted beneficiary options and Transaction Risk Analysis techniques based on rich customer datasets, aimed at accurately assess transactional risk and exempt lower risk transactions from SCA. This will result in optimal customer experience due to a lower number of transactions requiring SCA – due to their low risk – and a higher mix of seamless checkouts, resulting in more transactions finalized.

2. Impact of a non-homogeneously ready landscape on e-commerce

i. How a consistent user experience across PSPs and merchants drives trust

A common user experience is critical to drive trust. A consistent user experience across PSPs and merchants is paramount to ensuring a smooth transition to SCA as it will clearly guide customers in dealing with the new authentication process so that they can quickly familiarize with it. However, in September when the new norms will apply, consumers and businesses will experience a variety of flows across merchants and PSPs: some processes will comply with the RTS but manage only part or no exemptions from SCA, while others will offer a comprehensive set of features and include all exemptions.

PSPs will be able to offer a consistent user experience if they fulfil operational readiness with PSD2 – not just compliance readiness. Otherwise consumers will experience different journeys when they shop online or execute online payments via their bank or TPPs and will not understand the rationale behind those differences – which in fact should not exist. Inconsistency will lead consumers and businesses being confused and they will find it difficult to gain trust in the new security standard.

ii. Impact of fragmented implementation across Europe

Confused customers

A fragmented implementation across PSPs and merchants will expose consumers to different journeys when they shop online which will confuse them. This will also have a negative impact on payment security as some consumers may choose to shop at merchants lagging behind with SCA implementation, still offering non-compliant checkouts as they will experience more seamless processes than they would at SCA-compliant merchants while other customers may not proceed with the purchase outright.

This is confirmed by recent data from Ravelin showing that banks who have implemented one-

time password and in-app authentication still lose 19% of transactions through SCA[3]. This is partly due to longer checkouts as websites usually load within 1 second but with SCA loading takes up to 37 seconds. However, the number of SCA requests after the September mandate is estimate to be 20 times more than what they are today so latency will be even longer as systems are still not ready to handle such high volumes, putting merchants that offer SCA at an even greater potential disadvantage.

Compliant merchants should not suffer any disadvantage. If all PSPs and merchants were ready to comply with comprehensive SCA solutions customers would face consistent user experiences and not stimulated to look to more seamless non-compliant processes but more inclined to take up SCA, resulting in a smoother transition to the new security standard.

Non-fraudulent transactions declined

A variety of user experiences across merchants and PSPs will have major effects on conversion as the more burdensome the checkout the higher the abandonment rate. Consumers that deal with operational ready PSPs and merchants – i.e. that fully meet the PSD2 operational requirements – will enjoy smoother checkouts and merchants experience higher conversion rates. On the other hand consumers serviced by PSPs and merchants that are at an earlier phase of development and do not meet operational readiness will face more burdensome checkouts and merchants suffer higher abandonment, resulting in reduced sales and dissatisfied customers.

In particular exemptions from requesting SCA are important features. The customer option to exempt payments to specific beneficiaries from SCA is an example: in compliance with the RTS provisions issuers can create and maintain lists of trusted beneficiaries on behalf of their customers via the whitelisting/trusted beneficiaries' exemption. While merchants cannot manage lists of trusted beneficiaries or auto-enroll in a customer's trusted beneficiaries list, they can inform their customers of the benefits of whitelisting and facilitate the enrolment process through:

1. Promoting the benefits to regular customers and advising them of how they can add the merchant to their trusted beneficiaries list;
2. Requesting that an issuer serve the trusted beneficiaries enrolment option form through an SCA challenge when a customer who has not added the merchant to their list completes a transaction with them.

PSPs that do not offer the ability to apply exemptions will clearly have a negative impact on merchants' revenue. In fact, customers shopping at those merchants will have to undergo a SCA process to finalize all their online purchases resulting in higher abandonment rates than in a seamless authentication scenario through the application of specific exemption rules. In addition, a number of customers may be inclined to shop at merchants that offer the option to be enrolled as trusted beneficiaries thus shifting future revenues away from merchants unable to offer that option. The effect is more significant that it may seem as customers are most likely to include in their trusted beneficiaries list merchants they regularly shop at, due to a combination of trust and convenience.

A survey from Mastercard of April 2019 shows that only 24% of European e-merchants supported 3D Secure so it is very unlikely that the vast majority will be able to offer SCA compliant checkouts in September. As 20% of issuers are expected to decline non-SCA authorized transactions outright, due to inability to support 3DS 2.2 –which enables to apply all exemptions and Transaction Risk analysis based on enriched customer data – several genuine, non-fraudulent transactions will be declined leading to customer complaints and lost sales. The

[3] *https://www.ravelin.com/blog/one-fifth-of-payments-sent-to-3d-secure-are-lost*

expected impact to European e-commerce will be nearly € 50bn in lost sales[4]. In addition, this will disrupt confidence in e-commerce since customers are particularly sensitive to false declines as 33% of cardholders that experienced a false decline with one payment card never use it again[5].

Higher abandonment and costs

Fragmented implementation of issuers and merchants in managing exemptions will ultimately result in increased abandonment and higher costs for merchants, consumers and businesses.

To limit both abandonment and cost it is paramount to support all exemptions provisioned by the RTS. SCA requires customers to take additional steps in authenticating a transaction and higher processing cost, so the mix of SCA vs. non-SCA authenticated transaction drives both abandonment and processing cost.

Worldpay estimates that exempting from SCA when the RTS allow will limit the increase in abandonments to 5% while requesting to authenticate all transactions via 3DS will increase the number of abandonments by 27%, over five times as much. On the cost side, applying exemptions whenever possible will make processing cost 4% higher while applying SCA to all transactions will increase processing cost by 9%, more than twice as much.

As mentioned earlier, many issuers expect to decline outright non-SCA authenticated transactions where they cannot see a request to apply an exemption. This is due to the inability of the issuer's platform to acknowledge the request to exempt a transaction to be SCA authorized due to an allowed exemption. Most of these declines will be toward genuine, non-fraudulent transactions so customers will not understand the rationale behind the declines and will be dissatisfied. Some customers may retry using the same or another mean of payment – e.g. another payment card – but they will experience a decline again, they will be more dissatisfied and perceive e-commerce as inconvenient.

Lower sales and higher processing cost are likely to drive merchants to increase prices of goods and services and/or fees while reducing advantages for their customers such as free shipping.

3. Awareness of the new regulation

i. Merchants awareness

Mastercard recently conducted a quantitative survey among European merchants to understand to what extent small and mid-size online merchants are aware of and prepared for PSD2's SCA requirements. According this survey 75% of European online merchants are not aware of the new security standard set to come into effect in September 2019, while 86% do not currently support SCA.

In addition to indicate low awareness – particularly among smaller merchants – the survey highlights that very little communication took place so far:

- Only 25% of European online merchants are aware of SCA requirements under PSD2. Awareness is twice as high among merchants with over 500 transactions per month (40%) compared to those with less than 500 transactions per month (20%). The particularly low awareness of smaller merchants is of particular relevance as their share is the highest making overall awareness very low, possibly lower than the 25% reported in the survey;
- As of April 2019, out of the top 30 acquirers operating in Europe 30% have informed fewer

[4] *Considering just European small online merchants, with annual sales of € 75bn, it will make € 15bn of their revenue at stake. Revenue at stake for larger online merchants will be ~11% but due to their combined revenue of € 300bn that will be € 33bn*

[5] *Source: Mastercard Advisors*

than 25% of the merchants they serve about SCA, while an additional 27% informed between 25% - 60% of their merchants;

- European online merchants would welcome receiving information on PSD2 and only 13% believe that they don't need any further information.

Also, the majority of online merchants are not aware of the challenges the new regulation may pose to their business. In particular merchants are unaware if their PSP has made investments geared at supporting exemptions or has a fraud rate above a certain threshold, so they have no clue of whether they can benefit from specific exemptions and/or to what extent.

This is a call to action for acquirers and PSPs to step up their communication effort to properly educate merchants and actively contributing to a smooth transition to SCA.

Merchants will be able to support SCA only if they are appropriately informed of the new authentication measures, the rationale behind them, how the new process actually works and whether exemptions exist under specific circumstances.

ii. Consumers awareness

As of 14 September 2019, consumers must authenticate payment transaction executions via a SCA process. A successful, smooth transition toward the new security standard will be achieved only if consumers fully embrace it.

Consumers must be aware not just of the process but also of the benefits it brings along with any practical implications of the new procedure. In fact, when customers are not expecting change and/or don't understand the rationale behind it they are very likely to resist to it.

Unfortunately, most PSPs and merchants have taken little action so far to inform their customers of the effect the new regulatory regime would have on the payment authorization and checkout processes they are dealing with today.

This is reflected in the results from a recent survey from FICO. The survey shows that the share of European adults with no awareness of upcoming needs for a different authentication process at checkout is between 23% and 37% depending on the country.

4. Conditions to launch Strong Customer Authentication

i. Fully tested, reliable solutions

Strong Customer Authentication should be mandated after payment systems have been appropriately tested and prove to be able to offer highly reliable services. Reliability is in fact an important driver of confidence and trust.

Reliable solutions are achieved only after appropriate testing, which in many instances have not taken place. Due to the lack of sufficient time to develop appropriate testing facilities many European PSPs were not able to carry-out appropriate testing so in September their SCA solutions will not be as reliable as the market would expect as they were not tested in a simulated-live environment via testing protocols able to deal with all possible circumstances. In several instances this means that if something goes wrong no fall back mechanisms are in place. Testing is particularly critical in light of the volumes of SCA requests generated after the September date which are expected to increase 20X from today' level.

As they have not properly tested in these situations payments systems of issuers, acquirers, schemes and merchants are not prepared to handle these extremely high volumes with potential system failures. This will result in non-fraudulent transactions declined, lost sales and dissatisfied customers. Consumers and businesses are likely to experience even longer checkout

times when asked to authorize a transaction via SCA, resulting in more inconvenience. Payment failures may also result in customers being locked-out from their account, a particularly annoying experience that could potentially disrupt trust in the new security standard.

Impact of inconveniences and system failures is likely to be even more significant than anticipated due to the holiday season following the September due date. This has the potential to turn the convenience of online purchases into an inconvenience and limit the natural growth that European e-commerce have experienced in the last few years, with a potential more negative effect in countries with lower e-commerce sales with respect to the European average.

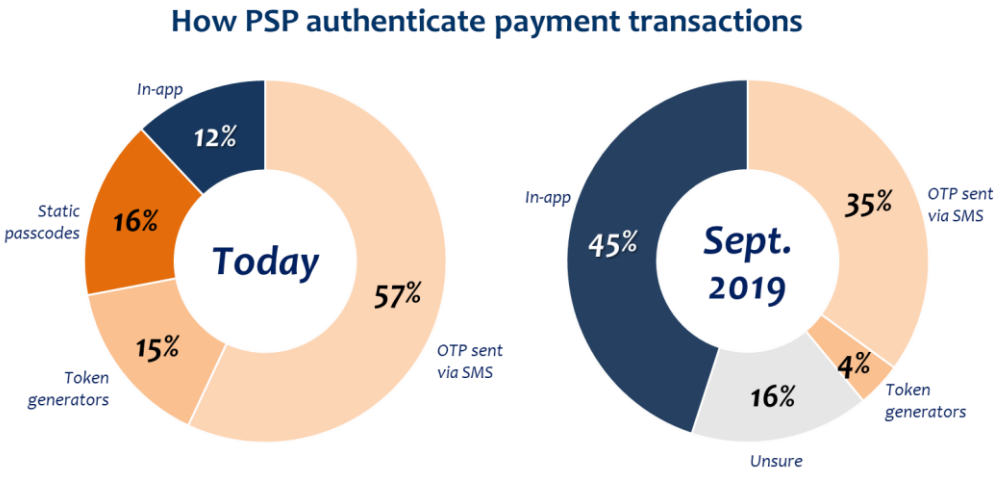
Carrying out proper testing is therefore required to understand if additional developments are needed and/or bugs need to be fixed.

ii. Comprehensive solutions

Strong Customer Authentication should be mandated when there is sufficient industry-wide operational readiness to ensure a harmonized approach across Europe in terms of user experience.

Market evidence suggests we are experiencing a fragmented approach. A recent study[6] across 21 European countries surveyed 100+ leading banks on how they are coping with the Strong Customer Authentication requirements including managing of exemptions.

RTS requirements related to dynamic linking make physical tokens not compliant so a number of banks must amend the way they authenticate payment transactions in the near future. This leaves just 12% of banks offering in-app authentication – compliant with PSD2. Although in September 2019 the share of banks that will authenticate in-app is expected to increase to nearly 45%, 1/5 of European banks will likely provide non PSD2-compliant authentication

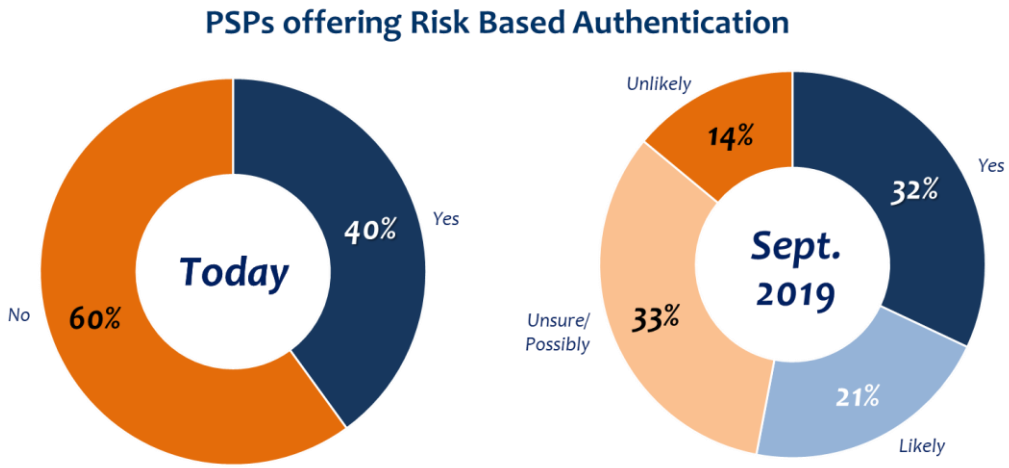


solutions, which will result in fragmented user experience across PSPs and potentially confuse consumers.

A survey of April 2019 shows that 40% of issuers would authorize payment transactions if acquirer exemptions were applied, but nearly half of banks will not be able to apply exemptions due to delays in properly amend their platform to support all exemption rules provisioned in the RTS and lack of Risk Based Authentication capabilities. This will result in many non-fraudulent transactions declined from September 2019 with consequent lost sales and customer complaints, potentially turning the convenience of online shopping into an inconvenience. Also,

[6] *Mastercard`s Top100 issuer survey*

this may trigger press releases that will echo the negative market impacts of the new security standard undermining trust in SCA and confidence in e-commerce.



Applying exemptions properly it is not an easy task. Circumstances where they can be applied must be dynamically identified and issuer abilities to support specific exemptions must be taken into account – including their 90-day rolling fraud rate – as the issuer has the final transaction approval decision. In addition, merchants must be able to resubmit the transaction approval in the event the exemption is declined.

Many merchants underestimate the complexities and development and testing needs to properly handle exemptions: one in 2 merchants plan to manage exemptions internally, rising to nearly 60% among merchants with less than 100 employees[7]. This also indicates that smaller merchants be hit harder in term of lost sales as they lack sufficient dedicated resources and budget to meet full readiness in the short time frame that is mandated.

iii. Customer-centric solutions

As digital commerce is becoming the norm and new regulatory requirements are coming into play, innovative solutions need to ensure merchants are continuing to delight customers online.

A recent survey[8] highlights that across all countries 50% - 75% of European adults think that when purchasing online they are dealing with enough or too many security checks, so they are unlikely to welcome more. To ensure consumer retain confidence in e-commerce, PSPs and merchants must understand in-depth where customers perceive enough or too many checks, and look to implement low-friction methods in those instances where PSD2 asks for more stringent authentication requirements and customers would not to welcome them.

As different customers have different habits, an authentication procedure may be user-friendly for some customers while more burdensome for others. So orchestrating authentication offering a wide choice of authentication methods creates a customer-centric SCA strategy.

The success of an authentication is dependent on multiple factors, which may change depending on circumstances. The same survey shows that customers are concerned about several factors that could be an impediment in completing a successful authentication and prevent them from completing a payment transaction. The factors consumers felt to be an impediment if they needed to authenticate an online payment via mobile phone are:

- Mobile phone isn't a secure or intelligent way for banks to contact me

[7] *451 Research survey*
[8] *FICO Survey 2019: PSD2 Strong Customer Authentication – What Do Consumers Think?*

- Not sure if a passcode would come to me
- It would be too complicated
- Other people can access my mobile phone
- My disability means I can't use a phone this way
- I might not have my phone with me
- I wouldn't trust a passcode sent this way
- There's poor mobile coverage where I live or work

Most SCA-based authentication processes rely on a mobile number stored with the bank but 15%-35% of banks do not have a mobile number for their customers[9] nor mobile apps. To allow online shopping for customers for whom they have no mobile number or for those with no smartphones, banks will need to create processes that allow sending OTPs via emails or the bank website. This involves interaction with multiple devices, so offering a user-friendly customer experience is particularly challenging, but paramount to ensure confidence in the new security standard.

Banks, PSPs, payment schemes and merchants would need to consider customer perceptions when designing their SCA procedures, including offering a range of choices aimed at maximizing conversion. This will benefit consumers and businesses through increasing their trust and confidence in e-commerce and delivering a low-friction purchasing experience, even when SCA is required.

Checkout timing is also an issue. The industry should be prepared to handle the much higher volume of SCA requests that will be generated from September when the mandate will apply to ensure that it will not result in longer checkouts times, more abandonments, lost sales and customers complaints.

iv. Widespread market awareness

Recent surveys show that many merchants and consumers are not aware of the PSD2 and the new security standard that must be used to authenticate payment transactions from September.

The share of merchants is particularly high with 75% unaware of PSD2 and how it will impact their business[9]. Merchants not prepared to deal with the new security standard will not properly engage with it and most likely will take no actions toward informing their customers. That will result in increased abandonment rates as many consumers are also not aware of the new authentication requirements they must follow during checkout.

Before mandating Strong Customer Authentication, PSPs should guide larger merchants on how to effectively update and test their payment systems, processes and train their personnel. Acquirers and gateway providers should make smaller merchants aware of the actions required and the consequences of inaction. In particular they should emphasize the importance of testing because of the number of combinations of PSPs/Issuers/Schemes/3DS versions that must be tested.

Acquirers, issues and payment schemes should communicate properly the features of 3D Secure 2.2, how to deal with them and the options for exemptions and how to optimize conversion along with specific merchant use cases.

PSPs and payment schemes should offer merchants an opportunity to interactively clarify any doubts they may have, but also educate their consumers and businesses about the upcoming

[9] *Mastercard survey*

changes and highlight the reasons why these changes are brought to them.

PSPs and payment schemes should also work alongside merchants and stimulate them to take similar actions to educate their customers, and guide them to ensure that consumers are given consistent communication not to confuse them. Consumer awareness campaigns should address what to expect, who to expect it from, when, where and why including how to list trusted beneficiaries and update contact details with their PSP.

We recommend to highlight benefits of the new security standard to stimulate engagement – including higher approval rates and potential for lower disputes – and drive away from being perceived as a mere mandate to comply with.

5. Benefits of a managed transition period

i. A managed transition period will allow the industry as a whole to get ready

The industry is not ready to launch Strong Customer Authentication. This is the case for providers of SCA solutions, issuers and acquirers. Widespread evidence clearly indicates that in September many of them will not be operationally ready and not in a position to offer solutions that offer a comprehensive set of features including exemptions nor the user-friendliness to ensure a smooth transition to the new security standard. In addition, most payment systems have not been tested so the level of reliability will be far below what the market would expect.

Offering SCA involves upgrading payment systems of card networks, processors, banks, PSPs and merchants and requires ongoing monitoring actual fraud rates and other KPIs and reporting them to the National Competent Authorities. Meeting full operational readiness requires time to implement the wide range of requirements that need to be met along with their complexity and conduct appropriate testing under all circumstances in a simulated-live environment before rolling-out to merchants and consumers. If given sufficient time the industry will be able to provide consistent and reliable authentication processes, ensuring a common experience across PSPs and merchants resulting in increased consumer confidence in e-commerce and a smooth transition to the new security standard.

As very little communication geared at merchant awareness has taken place so far, we highly recommend providing a managed soft-enforcement period to allow enough time for acquirers, issuers and payment schemes to take the necessary actions to properly educate merchants ensuring they fully embrace SCA and understand the impact on their business.

In addition, a significant share of consumers – the final users of SCA processes – are unaware that from September they will need to authenticate payment transactions through a different process, let alone the rationale behind it, so many will be very likely to resist to it and be dissatisfied. That's mostly due to very little effort from PSPs, payments schemes and merchants in informing and engaging consumers and explaining them the benefits brought by the new security standard.

Over the last few years industry players have dedicated large effort and resources to developments toward meeting the many and complex PSD2 requirements but rolled out little communication initiatives.

Implementing communication actions needed to effectively educate consumers toward a smooth transition to SCA requires time, dedicated resources and specific budgets from PSPs, merchants and payment schemes. As the September deadline is just weeks away there is no enough time to achieve significant consumer awareness before the SCA mandate comes into force. As consumer awareness is paramount for a smooth transition toward the new security standard, we recommend the introduction of a managed transition period to ensure that banks, PSPs, merchants and payment schemes are able to take the necessary actions to make consumers and businesses aware of the new authentication requirements and related

procedures.

Also, merchants will benefit from a transition period as it will allow them to familiarize with the new security standard, understand the impact on their business, inform their customers about the new authorization process and communicate the additional benefits it brings to them so that they will not put online sales at risk and don't perceive SCA as a mere mandate.

A transition period will strongly help the whole industry to launch harmonized, highly secure and reliable Strong Customer Authentication processes across Europe with the necessary user-friendliness to facilitate their take up.

ii. Payment security will be fully retained during a transition period

A transition period will have no negative impact on security. In fact, fraud in internet payments has been rising in value terms due to the high growth in transaction value, but the fraud rate in the last few years has decreased due to the deployment of increasingly accurate Transaction Risk Analysis techniques that effectively assess risk of attempted transactions before they are executed. These techniques leverage high volumes of transactional and behavioral data to accurately assess transactional risk, minimizing false positives, and challenge only the higher risk attempts.

Risk Based Authentication has already delivered significant benefits in the markets where it has been deployed. Today, in a UK pre-PSD2 environment, 95% of transactions that undergo a risk-based assessment do not require customer authentication[10]. Since the introduction of a risk-based approach there has been a 70% reduction in abandonment rates. At the same time, fraud rates have fallen, indicating that risk-based assessments are an effective tool to detect and prevent fraud.

6. Insights & Recommendations

i. Evidence, insights and concerns

As mentioned throughout this paper there is widespread evidence that a lack of sufficient time to develop and appropriately test SCA solutions to offer full-feature services seems to be at the basis of several industry players not being able to deliver and appropriately test to ensure a smooth transition to new security standards.

The strong need to issue interpretation guidelines related to the published RTS is indicated by the EBA's explicit mention[2] that their opinions are addressed primarily to competent authorities, which in turn should provide local guidance to PSPs, payment schemes and technical service providers. We believe this is a further evidence that uncertainty still exists in the interpretation of the regulation, partly due to the extent of market implications and complexity as well as the variety of entities involved. This implies that industry participants that need to develop or amend their systems, hardware and software, including – in the case of banks – creating interfaces and infrastructures are in fact allowed a shorter timeframe to fully comply with the PSD2 as they need to proactively look to correct interpretations and guidance on a number of aspects well after the publication of the final RTS.

A lack of communications to consumers, businesses and merchants on the implications of the SCA requirements is leaving them largely unprepared which will result in an unsmooth transition to the new security standards.

PSD2 aims to contribute to a more integrated and efficient European payments market, ensure a level playing field for Payment Service Providers and a harmonized user experience across the

[10] *Visa Risk based authentication case study*

EU. That will be achieved only if all – or at least the overwhelming majority of – industry players enjoy the same level of readiness that will enable them to fully implement the new requirements, embracing and staying on top of the new regulatory framework, not suffering it.

We are concerned that if the industry approaches the September deadline with fragmented, non-harmonized solutions it will negatively impact the e-commerce and payment ecosystems and consumer and businesses will suffer the consequences. Also, we believe that unreadiness will result in questionable reliability and negative market impacts as well as higher costs to fix the systems than it would take to complete the necessary developments and appropriate tests during a managed transition period.

ii. Recommendations for a managed transition period in the application of the RTS on SCA and CSC

The PSD2 aims at increasing payments security but also have a large impact on the way customers authenticate their payment transactions and finalize online purchases and on the merchant's business model.

In 2018 60% of Europeans completed online purchases and e-commerce sales have grown at 15% YoY over the last 5 years, making online shopping a common practice throughout the EU[11]. As such the RTS on SCA and CSC should be regarded as a regulatory framework with significantly higher market impact than others had in the past, so allowing a longer timeframe to implement the mandate than the standard 18 months it is not unreasonable and would allow the industry as a whole to fill the unreadiness gap and offer comprehensive and harmonized user experience across Europe resulting in long-lasting benefits for everyone.

All players in the industry are moving forward with the intent to be fully ready, but the complexity and the extent of the requirements set out in the PSD2 are so profound that they need more time to complete all developments required and conduct appropriate testing to offer reliable solutions and optimize the customer experience.

In order to ensure a harmonized and smooth transition to SCA and appropriate awareness of consumers and merchants we recommend regulators to consider allowing an 18-month managed transition period starting from September 2019.

We recommend structuring the transition period in a few soft-enforced milestones to facilitate meeting all the requirements set out in the RTS on SCA and CSC and testing the solutions before their roll out. This would provide all industry players – issuers, acquirers, card networks, processors and merchants – with an opportunity to properly upgrade their payment systems, implementing all mandated and optional regulatory requirements, develop in-app authentication capabilities and carry-out appropriate testing for a sufficient time to achieve high service reliability levels under most business circumstances and an opportunity to amend/fine-tune their platforms according to the tests run, which will also ensure they stay on top of PSD2 for the years to come.

Issuers will also need time to update contact information of their customers, collect mobile numbers whenever possible and push their customer to download their banking apps to facilitate secure and user-friendly transaction authorizations via SCA, improving customer experience.

In addition, the managed transition period will be used to properly raise market awareness and provide consistent guidance on SCA. Acquirers, payment schemes and trade associations will have sufficient time to inform merchants on a range of outstanding issues including how SCA will impact their businesses and provide them with guidelines on how to educate their customers. Issuers, merchants, payment schemes and consumer associations will be able to

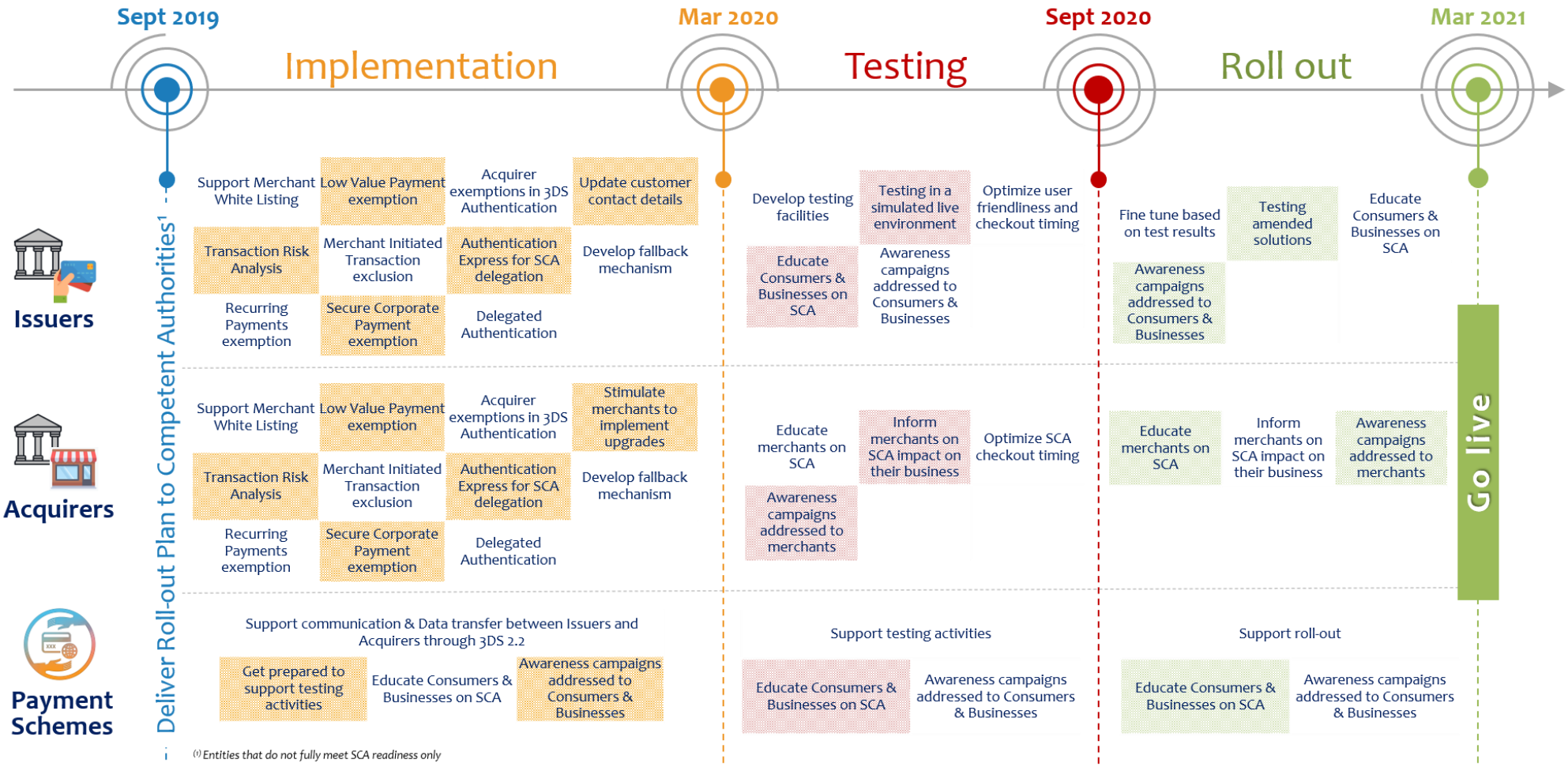
[11] *Eurostat 2019*

create relevant material to communicate the benefits of SCA and how to deal with the new authentication standard.

We recommend that by September 2019 PSPs and payment schemes provide the competent authorities with a roadmap of activities they plan to deploy during the 18-month managed transition period along with easily audited milestones.

A managed transition period will greatly contribute to a smoother transition to the new security standard, in alignment with the EBA and European Commission objectives of ensuring higher payments security, uniform procedures and consistent approaches throughout the EU and will result in higher confidence in e-commerce and broader trust in online payments.

Proposed Managed Transition period – SCA Roadmap



(1) *Entities that do not fully meet SCA readiness only*

CleverAdvice
Via Ferrante Aporti 34
20125 Milano, Italy

T +39 02 39660672
F +39 02 2870768

e postmaster@cleveradvice.eu
w cleveradvice.eu

CleverAdvice