Payments & Strong Customer Authentication: An Update

19th September 2019

TTI Autumn Conference

Paul Rodgers: Chairman, Vendorcom

paul.rodgers@vendorcom.com +44 (0)7785 502605

Perspective

- Member: Payment Systems Regulator Panel
- Chairman: Vendorcom
- Evangelist: World Wide Web Consortium
- Mentor: Level39 Fintech Accelerator
- Investor: Dot-com
- Angel: Cotswold Whisky Distillery
- Member: Scotch Malt Whisky Society
- Founder: ProHUBition
- Trustee: Inland Waterways Association


vendorcom
Connecting Payments

Predicting the Future of Payments

The Regulation

COMMISSION DELEGATED REGULATION (EU) 2018/389

of 27 November 2017

supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication

(Text with EEA relevance)

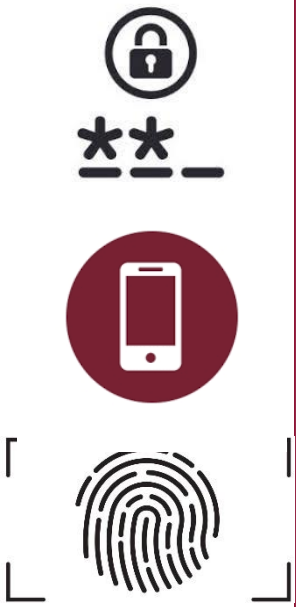
THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [1], and in particular the second subparagraph of Article 98(4) thereof,

RTS for SCA: what is it?

- Knowledge
- Possession
- Inherence



Allows a Payer PSP (issuer/bank) to:

1) verify the identity of a payment service user; or
2) Establish the validity of a specific payment instrument

SCA must be applied whenever a payment service user:

1) Accesses their payment account online
2) Initiates an electronic payment transaction
3) Any activity via a *remote channel* which may imply a risk of payment fraud or other abuses

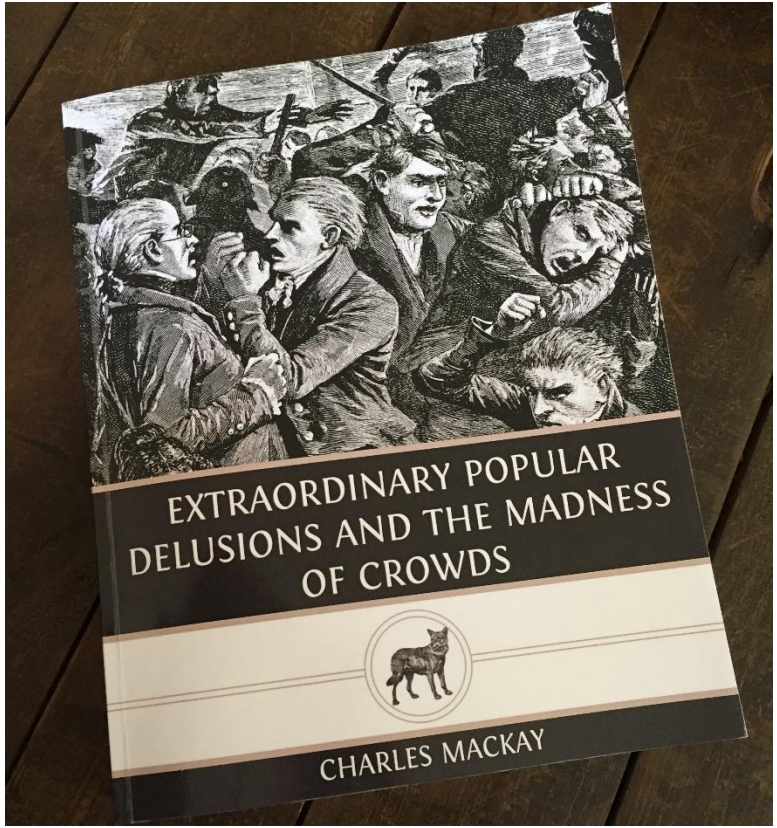
RTS for SCA: Background

- RTS for SCA is a European Regulation
- Enforced from 14th September 2019
- Applies to electronic transactions – not just card payments
- Ecommerce, mobile and remote payments will be affected
- ***Less*** impact on face to face payments
- For contactless transactions, SCA will be required after 5th transactions or when cumulative value exceeds €150
- Exemptions exist but will only apply in narrowly defined scenarios

Strong Customer Authentication Exemptions

Reason	Reference
White list of trusted beneficiaries No SCA for transactions to white-listed trusted beneficiaries. SCA is required when the white-list is created or amended	Article 13 RTS
Transaction Risk Analysis (TRA) No SCA for remote transactions up to EUR 500, provided (1) TRA is applied and (2) fraud rates for card transactions are within defined thresholds	Article 18 RTS
Recurring transactions No SCA for recurring payments with the same merchant and the same amount. Some debate remains over the applicability of SCA for recurring payments with variable amounts.	Article 14 RTS
Low-value remote transactions No SCA for remote transactions up to EUR 30, with a cumulative limit of EUR 100 or 5 consecutive transactions without SCA	Article 16 RTS
Contactless payments No SCA for contactless transactions up to EUR 50, with a cumulative limit of EUR 150 of total contactless transactions or 5 consecutive transactions without SCA	Article 11 RTS
Commercial transactions	Article 17 RTS
Unattended terminals for transit and parking No SCA for transactions at unattended payment terminals to pay a transport (e.g. tolls on highways, Transport for London) or parking fares	Article 12 RTS

GDPR on Steroids!



Lacks Market Understanding

Unintended Consequences

Economic Damage

Time for Collaboration

-Regulators –

- Banks -

The New Collaborative Challenge: SCA

- Ecommerce under greatest ever threat
  - £45bn hit to UK economy
  - €160bn hit to EU/EEA economy
- Avoid the #SCAcliffedge
- Transition period beyond 14th September
- All stakeholders need to be involved
- Only regulators have power to stimulate

European Banking Authority Opinion

- Issued 21st June 2019
- Reiterates the ‘application date’ of 14th September
  - …all PSPs have to comply with the requirements…’
- Acknowledges complexity
  - ..actors that are not PSPs…
- A liability shift would not alleviate PSPs obligation
- Key component is to ‘explain and make customers aware’

European Banking Authority Opinion, cont[d]

- ‘Supervisory Flexibility’
  - Exceptional basis
  - Monitor execution
  - Ensure swift compliance
  - Achieve consistency across EU
- Clarification on Two Factor ‘Compliant Elements’
  - Card details NOT 'possession’
  - OTP by SMS NOT 'knowledge’
  - 3DSecureNOT provide a biometric for 'inherence'

The Gameplan

- Two phase, whole-ecosystem collaborative initiative building on learning from Chip & PIN Programme Management Organisation:
- Phase One:
  - Lock down Regulatory Conditions and Technical Standards
  - Implement technical solution(s)
  - Comms to the citizen/consumer (cardholder) as a bank customer
- Phase Two:
  - Lock down Operational Rollout plans
  - Instigate whole ‘service user’ market rollout
  - Comms to the citizen/consumer as the merchant customer

SCA PMO

- Regulatory Stream
  - Mandate from CAs
- Technical Stream
  - Scheme and inter-bank collaboration
- Operational Stream
  - Acquirer, processor, gateway and merchant migration
- Communication Stream
  - Cardholder comms
  - Citizen/Consumer comms

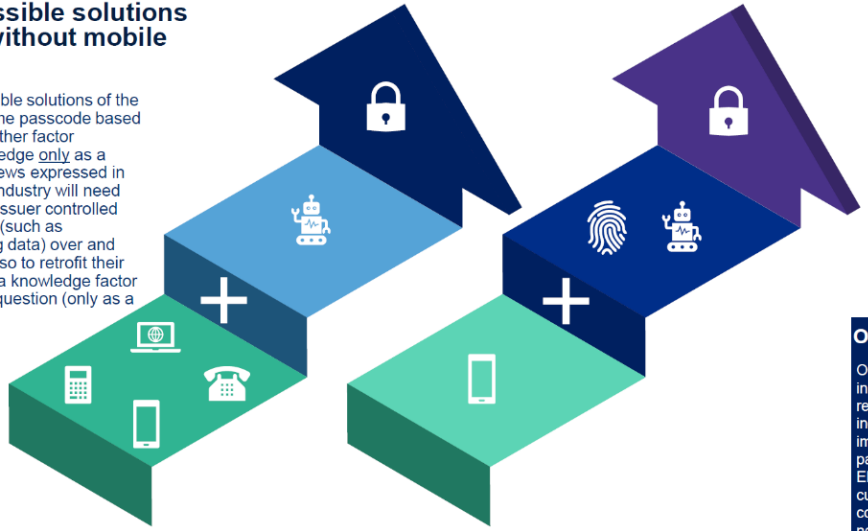
Issuers path to full compliance

UK FINANCE

Authentication: Two concurrent paths

Path 1: Accessible solutions (customers without mobile banking)

The long term accessible solutions of the industry will be one time passcode based (possession) plus another factor (inherence with knowledge only as a fallback). 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).



Path 2: Biometric and mobile app based solutions (digitally savvy customers)

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.

Medium to long term

Over time, the industry will continue to invest in the reduction of fraud through many strategic initiatives which are being actively discussed with the industry (eg tokenisation of the checkout process), with SCA seen as a short to medium term fraud reduction measure.

Knowledge factor

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 future proofed. 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.

One time passcode (OTP)

One time passcodes could be used in the form of an SMS OTP, card reader, landline call or email. The industry was prepared and ready to implement SCA through one time passcodes. Given the impact of the EBA Opinion (with card details and current 3DS data 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. With the adoption of 3DS 2.x (within 18 months) this will provide valuable risk-based data to support the authentication as an interim second factor to OTP.

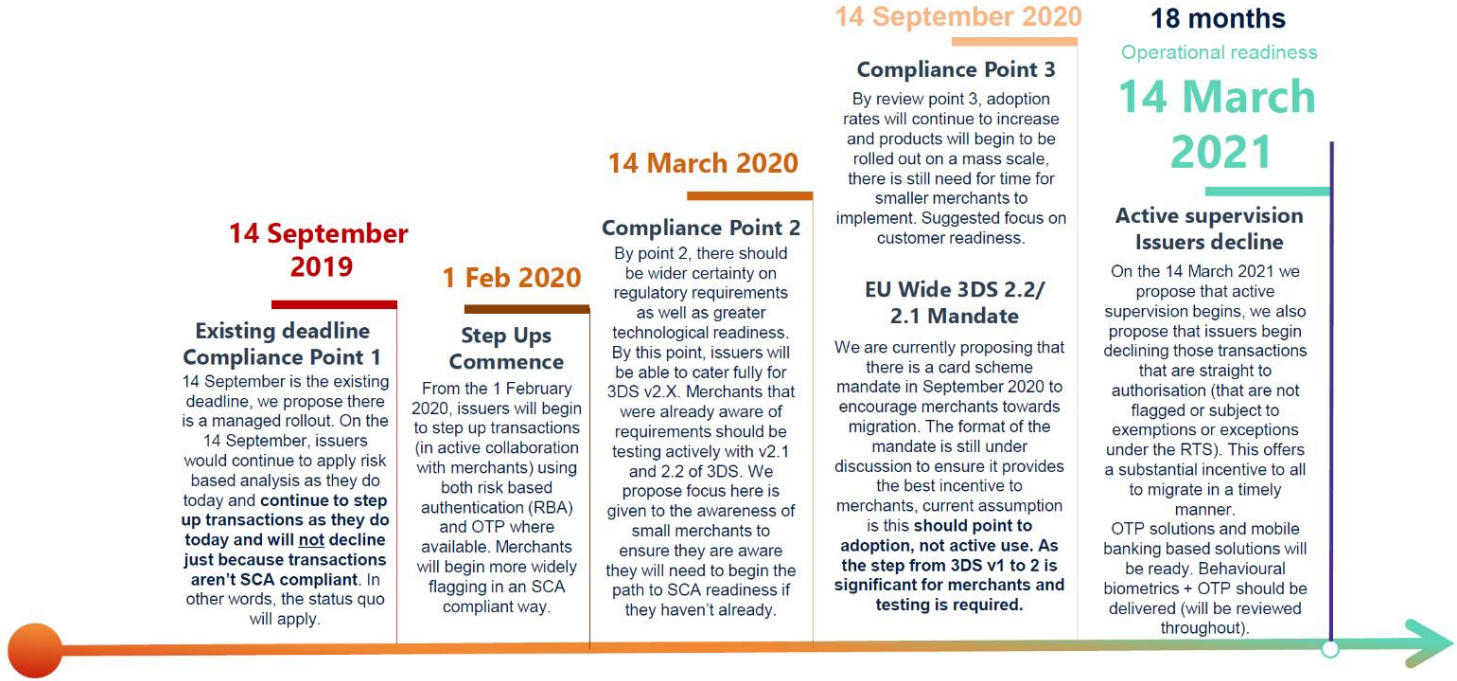
Exemptions

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 18 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



NCA (un)readiness (BRAG Status)

- Austria - FMA Finanzmarktaufsicht Österreich
- Belgium - National Bank of Belgium
- Bulgaria - Bulgarian National Bank
- Croatia - Croatian National Bank
- Cyprus - Central Bank of Cyprus
- Czech Republic - Czech National Bank
- Denmark - Finanstilsynet
- ECB (SSM) - European Central Bank
- Estonia - Estonian Financial Supervision Authority

NCA (un)readiness (BRAG Status)

- Finland - Finanssivalvonta - Finnish Financial Supervisory Authority
- France - Autorité de contrôle prudentiel et de Resolution
- Germany - BaFin and Bundesbank
- Greece - Bank of Greece
- Hungary - Central Bank of Hungary
- Iceland (EEA) - Financial Supervisory Authority
- Ireland - Central Bank of Ireland
- Italy - Banca d'Italia

NCA (un)readiness (BRAG Status)

- Latvia - Financial and Capital Market Commission
- Liechtenstein (EEA) - Financial Services Authority
- Lithuania - Bank of Lithuania
- Luxembourg - Commission de Surveillance du Secteur Financier
- Malta - Malta Financial Services Authority
- Netherlands - De Nederlandsche Bank
- Norway (EEA) – Not on EU list of Competent Authorities
- Poland - Polish Financial Supervision Authority

NCA (un)readiness (BRAG Status)

- Portugal - Banco de Portugal
- Romania - National Bank of Romania
- Slovakia - National Bank of Slovakia
- Slovenia - Bank of Slovenia
- Spain - Banco de España
- Sweden – Finansinspektionen
- United Kingdom – Financial Conduct Authority

Perspective

• 12th Aug 2016	EBA Consultation	1133 days ago
• 13th Mar 2018	SCA in law	555 days ago
• 21st Jun 2019	EBA Opinion	90 days ago
• 14th Sept 2019	Application date	5 days ago
• Today		
• 1st Feb 2020	Step ups commence	135 days
• 14th Mar 2020	Compliance point 2	177 days
• 14th Sept 2020	EU-wide 3DSv2 mandate	361 days
• 14th March 2021	Operational readiness	542 days

Questions For Your Payments Providers

- Acquirer(s) - waiver with NCAs; 3DSv2 testing; gateway testing programme; TRA thresholds;
- Processor - plans for 3DSv2;
- Gateway - accreditation path with acquirer(s)
- Web/app developer – availability to provide updates
- Fraud tools – support with exemptions
- Trade body - representation in rollout plan development
- UK Finance - route to participate in PMO
- Customers – familiarity with banks' requirements

Follow #SCAday tag on LinkedIn

Strong Customer Authentication

paul.rodgers@vendorcom.com

@paul_vendorcom

+44 (0)7785 502605