




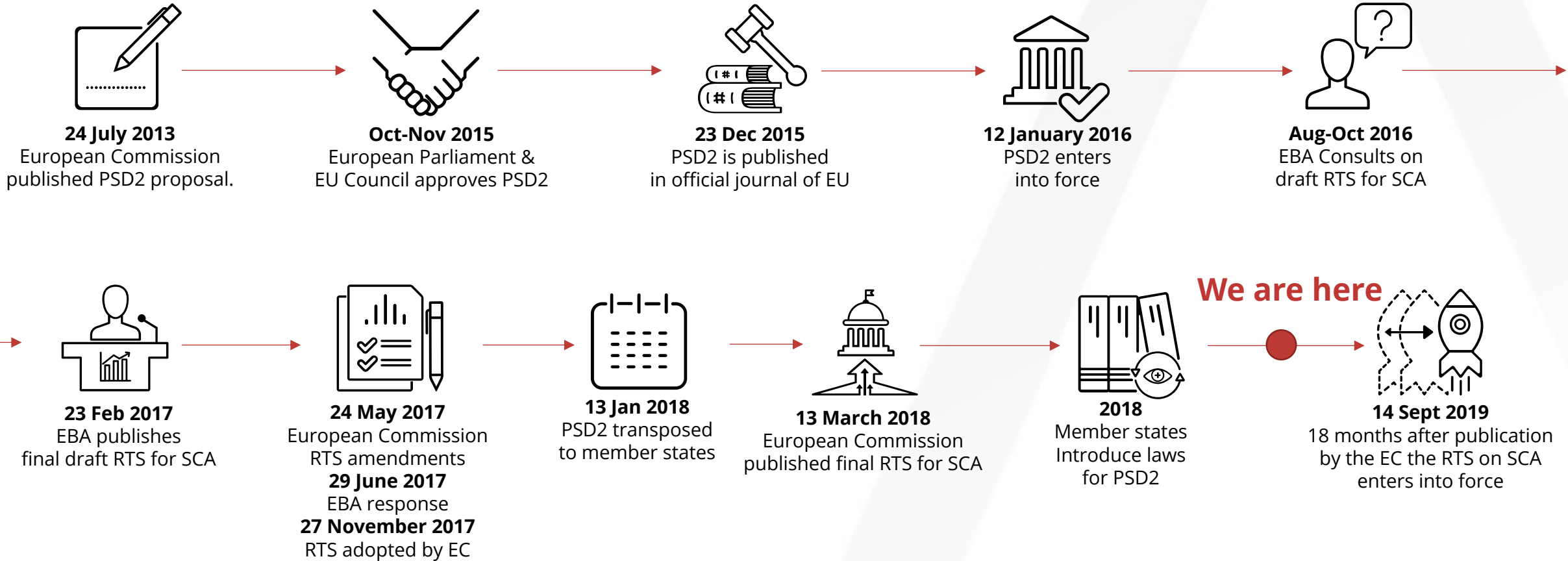
The background of the slide is an aerial photograph of a busy airport terminal. People are seen sitting on long benches, walking, and standing. A large, semi-transparent red triangle is overlaid on the right side of the image, pointing downwards.

PSD2 & 3D SECURE FRICTIONLESS FRAUD FIGHTING

Nathan Close
RSA Fraud & Risk Intelligence

 nathan.close@rsa.com  [linkedin.com/in/nclose](https://www.linkedin.com/in/nclose)  [@n8close](https://twitter.com/n8close)

PSD2 TIMELINE



WHERE DOES THIS APPLY?



■ Common Legal Framework

- Making & receiving payments whenever one party is within the EEA
- Also applies to PSPs (banks) located in the EEA even when transacting outside of the EEA
 - This will have an impact on PSPs that transact with banks inside the EEA
 - Also applies to transactions in different currencies

STRONG CUSTOMER AUTHENTICATION (SCA)

■ Need two of:

- Knowledge: "something you know" (e.g., a password)
- Possession: "something you have" (e.g., a mobile phone)
- Inherence: "something you are" (e.g., a biometric print)
(* RTS Article 4.1)

■ When:

- Accessing payment accounts online
- Initiating electronic payments
- Remote channel activities with a risk of payment fraud
(PSD2 Article 97.1)

* Regulatory technical standards for strong customer authentication and common and secure open standards of communication - 13 March 2018

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018R0389>



SCA CONSIDERATIONS

- 1. Transaction amount and payee linked to SCA**
(RTS Article 5.2)
- 2. Exemption for SCA based on the level of risk**
(RTS Article 18.1)
- 3. Transaction monitoring based on the analysis of payment transactions**
(RTS Article 18.2)
- 4. Better consumer experience:**
“User-friendly, accessible and innovative means of payment”
(PSD2 Article 98.3.a)



SCA MUST BE SECURE

1. Cannot be disclosed

- i.e., PINs/passwords need to be masked on screen [RTS Article 6.1]

2. Cannot be replicated

- i.e., Device data can't be copied to another device [7.2]

3. Must have low false positives

- i.e., Biometric methods need to perform [8.1]

4. Must be independent

- i.e., Compromise of one element doesn't compromise the others [9.1]

5. Confidentiality, Authenticity, Integrity

- Amount, payee, transmission and use of codes [5.2]

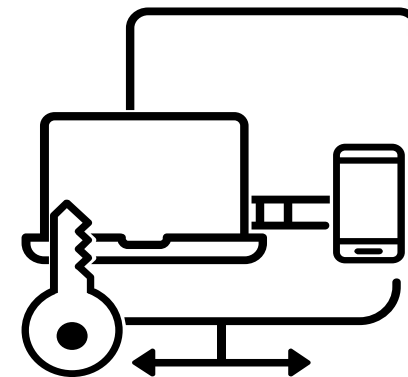


SCA PROCESS REQUIREMENTS

During the process of SCA the following requirements apply:

- **confirm amount and payee** during the authentication [5.1a]
- authentication code/token **specific for the amount and payee** [5.1b]
 - resistant to forgery [4.2c]
 - does not disclose its source elements [4.2a]
 - used only once [4.1]
 - cannot generate a new code based on previous codes [4.2b]

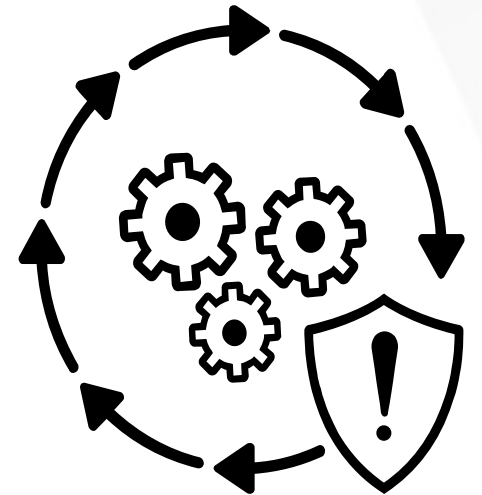
When authentication fails, cannot identify which element of knowledge, possession, or inherence was incorrect. [4.3a]



TRANSACTION MONITORING

Payment Service Providers shall have transaction monitoring mechanisms in place that enable them to detect unauthorized or fraudulent payment transactions [Article 2]

- Typical elements of the user under normal circumstances
- Lists of compromised or stolen authentication elements
- Amount of each payment transaction
- Known fraud scenarios
- Signs of malware infection



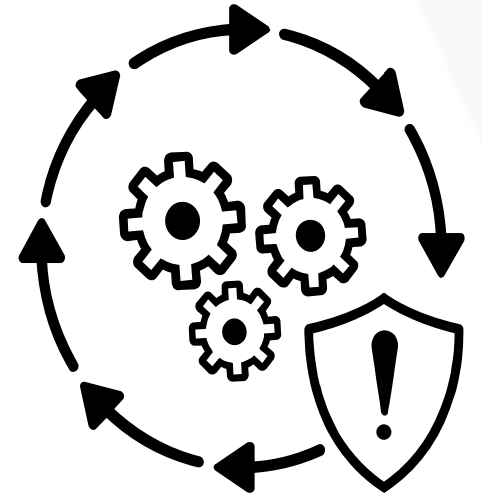
FIXED EXEMPTIONS

- **Viewing only the balance [10.1a] or last 90 days of transactions [10.1b]**
 - first time viewing the balance or transactions requires SCA [10.2a]
 - after 90 days since last SCA need to authenticate again [10,2,b]
- **Low value transactions less than €30 [16,a]**
 - SCA required when accumulated transaction value exceeds €100 or five transactions [16,b]
- **Payments from and to accounts owned by the same user [15]**
- **Payments to a previously created beneficiary [13,2]**
 - creating or changing the beneficiary requires SCA [13,1]
- **Series of payments of the same amount to the same beneficiary [14,2]**
 - the first payment, creating or changing the beneficiary requires SCA [14,1]

TRANSACTION RISK ANALYSIS

Strong Customer Authentication can also be exempted by using transaction risk analysis (risk based authentication). [Article 18]

- Abnormal spending behavioral patterns
- Payment history of the user and the user population
- Location of payer
- Location of payee account
- Lists of compromised or stolen authentication elements
- Payment amount
- Known fraud scenarios
- Unusual information about the device or software
- Signs of malware infection



SCA EXEMPTION BASED ON FRAUD RATES

- The SCA exemption applies if fraud rates are under a “Reference Fraud Rate”, based on transaction amount and type. [18,2a]
- The calculation is as follows: [19,1]

$$\text{Reference Fraud Rate \%} = \frac{\text{Total value of fraudulent successful transactions}}{\text{Total value of all successful transactions including both SCA and exempted}}$$

- The target fraud rates based on value and type are: [RTS Annex]

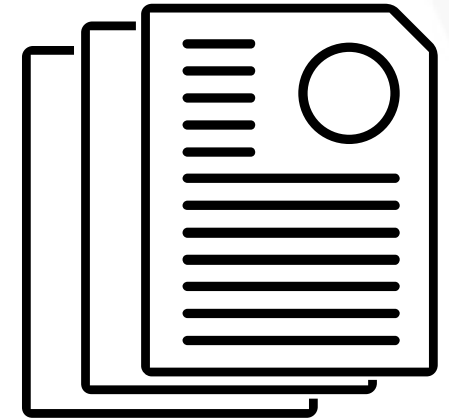
Exemption Threshold Value	Reference Fraud Rate %	
	Remote card-based payments	Credit transfers
€500	≤ 0.01	≤ 0.005
€250	0.01 - 0.06	0.005 - 0.010
€100	0.06 - 0.13	0.010 - 0.015

SCA EXEMPTION REPORTING REQUIREMENTS

SCA methods must be documented, tested and audited by an independent auditor. [Article 3]

Ongoing reporting of the fraud rates, is required for exemption compliance: [19]

- at least a 90-day basis [21,1]
- separate for each payment instrument [21,1]
- total value of fraudulent payment transactions [21,1,a]
- total value of all payment transactions [21,1,a]
- observed fraud rates [21,1,a]
- breakdown of payment totals with SCA and exempted [21,1,a]
- average transaction value with breakdown of SCA and exempted [21,1b]
- number of transactions with exemptions and percentage to total [21,1,c]



OTHER CONSIDERATIONS: TABLETS AND SMARTPHONES

Special attention is required for multipurpose smartphones and tablets to mitigate the risk of device compromise.

- Separate secure execution environments for payment and the strong customer authentication. [Article 9.3.a]
- EBA doesn't preclude a single app combining payments and authentication, or two separate apps, such as an online banking app and a separate authentication app.
- The apps need to assess whether the device has been altered or compromised (e.g., jailbreak, rooted, emulator detection capabilities). [Article 9.3.b]



OTHER CONSIDERATIONS: OPEN BANKING

PSD2 introduces open banking, requiring APIs to allow third party access.

- ASPSP - Account Servicing Payment Service Providers (eg: a bank with the accounts)
 - Need to provide the APIs to access accounts and payments
- PISP - Payment Initiation Service Provider (eg: merchants, fintech apps)
- AISP - Account Information Service Provider (eg: aggregator, fintech apps)

Strong Customer Authentication requirements also apply to third party access to accounts.

OTHER CONSIDERATIONS: MANAGING RISKS AND INCIDENT REPORTING

Article 95:

- Management of Operational and Security Risks
 - Framework of mitigation measures and controls to manage operational and security risks for payment services
 - Incident management procedures, with detection classification for operational and security incidents.

Article 96:

- Incident Reporting
 - Major operational or security incidents reported to the authority without delay
 - Financial impacts to users reported to the users with mitigation measures without delay

An aerial, top-down view of a busy transit station. People are seen sitting on long grey benches, some standing, and others using escalators. The floor is a light-colored tile. A large, semi-transparent red 'A' shape is overlaid on the right side of the image.

RSA[®]

EMVCO 3DS

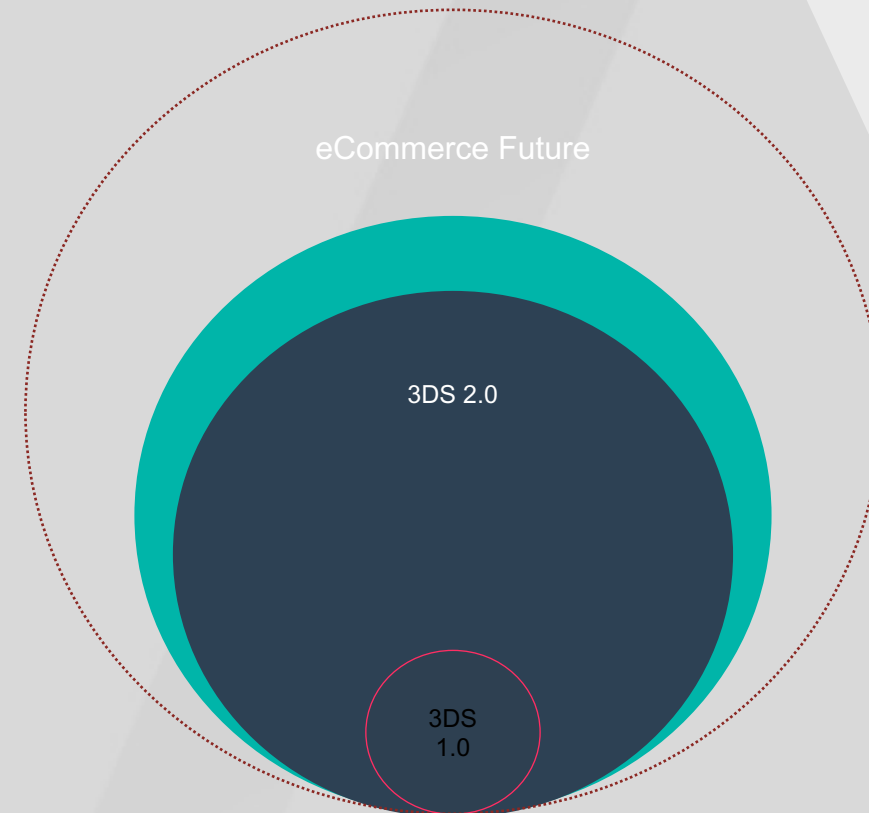
BUSINESS-DRIVEN SECURITY™

BACKGROUND

New version of 3D Secure released in Oct 2016 by EMVCo.
Name has changed from 3DS 2.0 to EMVCo 3DS.

The main changes are:

- Risk based approach
- Frictionless user experience
- Mobile application support



WHY IS A NEW VERSION REQUIRED?

- 1 Aging Current 1.0.2 version
- 2 New device types
- 3 New security threats
- 4 Higher expectations and lower patience by consumers



3D SECURE VERSION 1.X

 **ABC Bank** 

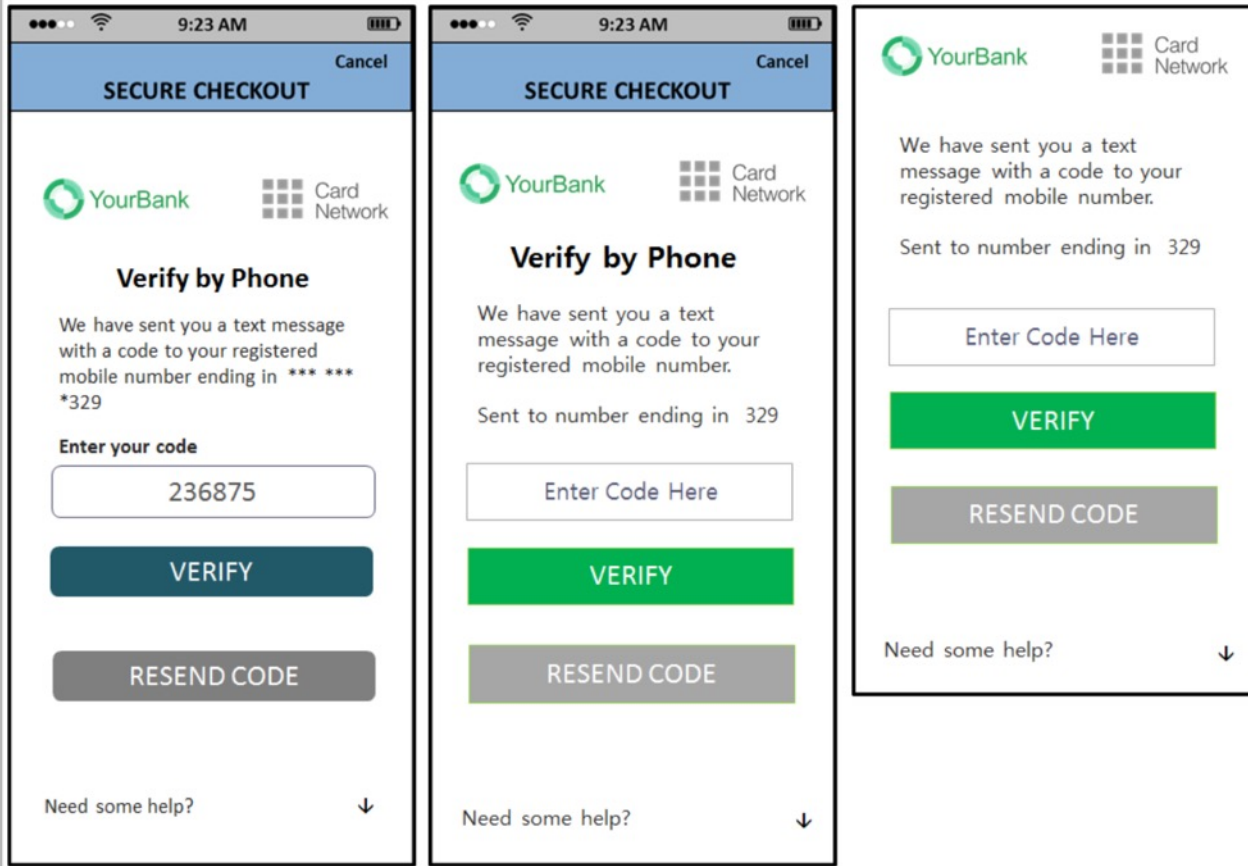
Added Protection
Please submit your Verified by Visa password.
[I am not enrolled in Verified by Visa](#)

Merchant: TestMerchant
Amount: \$555.00
Date: 06/20/2007
Card Number: XXXX-XXXX-XXXX-0034
Personal Message: Welcome to Verified by Visa!
Login Name: MESSGOULD
Password:
[Forgot your password?](#)

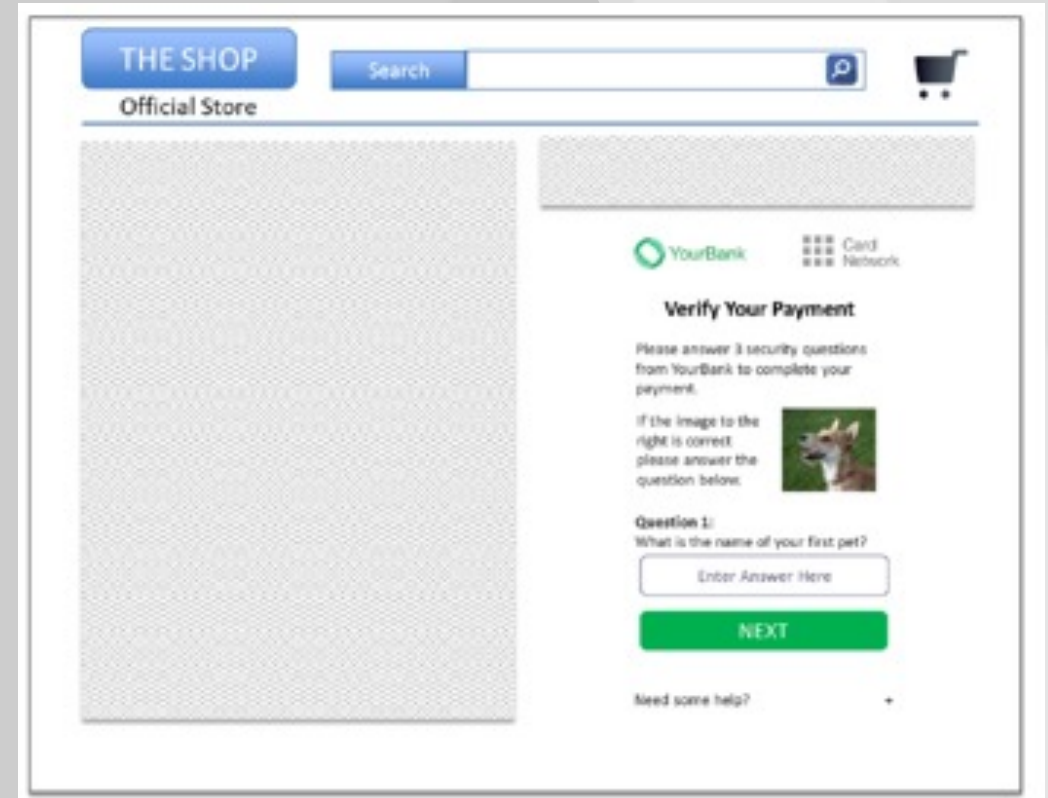
 [Help](#)

EMVCO 3D SECURE

Mobile API + Web flows



Browser Based flows



Source: EMVCo - EMV® 3-D Secure – Protocol and Core Functions Specification version 2.1.0, October 2017

MAIN DESIRED TARGETS



Payment Flows

Expand across multiple devices & apps:
mobile, tablets, smart TV's, consoles, wearables, IoT

Non-Payment Flows

Support for ID&V and digital wallets

3RI Flow

3DS Requestor Initiated - Non-Payment transaction
eg: verify subscription has a valid form of payment

User Experience

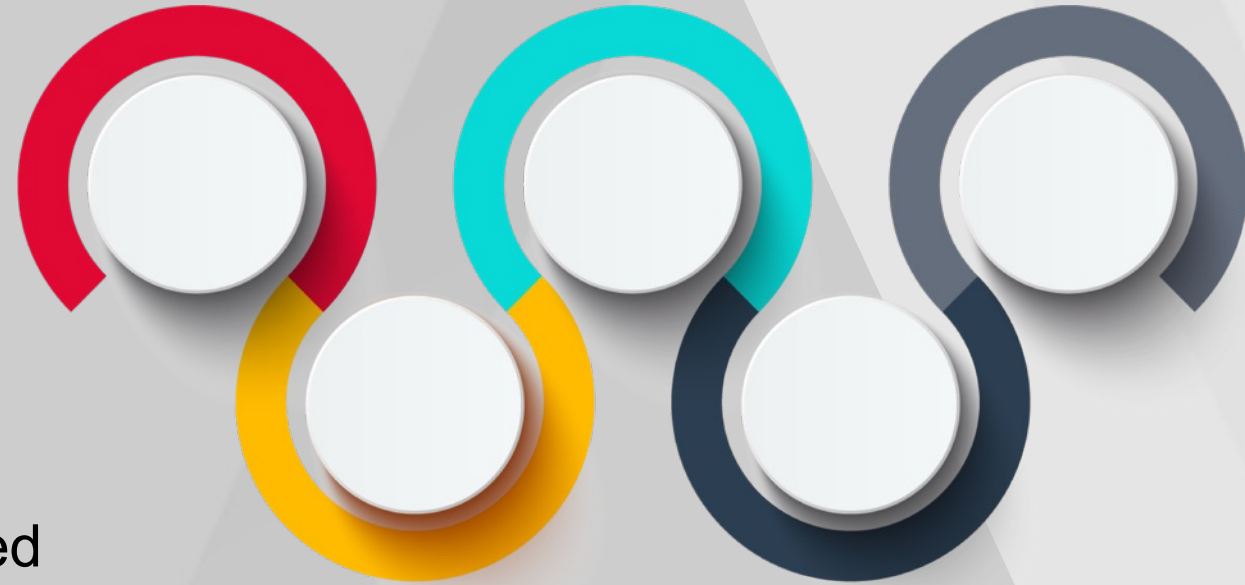
Frictionless checkout experience where possible
User experience aligns with the consumer device and logical flows

CONCEPT

- Priority #1 is Frictionless User Experience

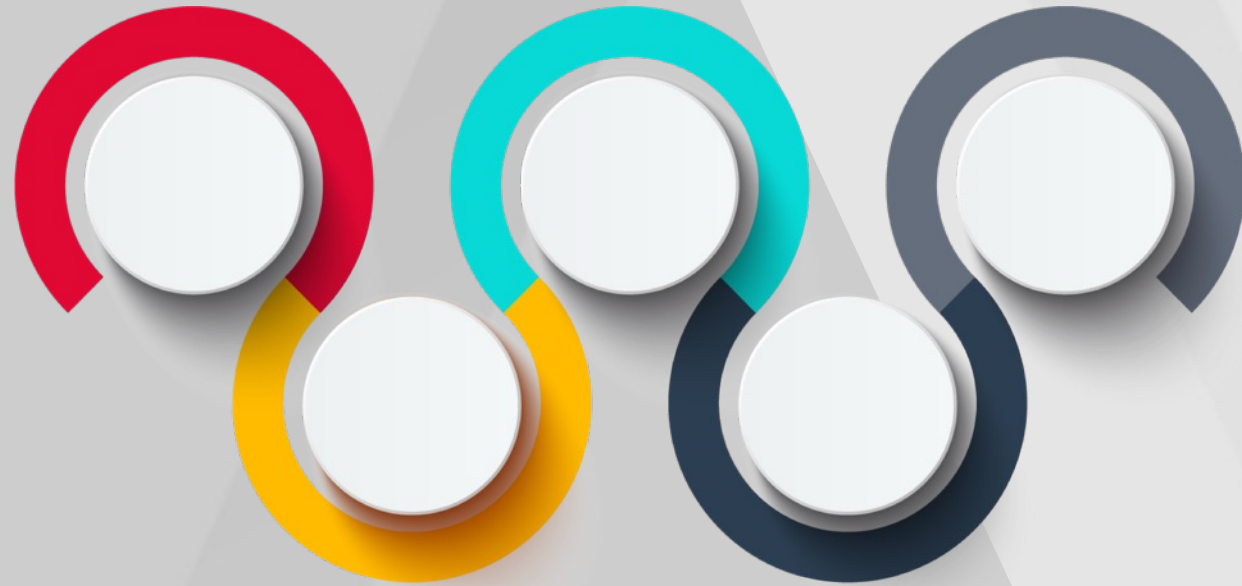
The best user experience is no experience

- Enriched protocol for better risk analysis
- Designed to increase trust between all parties
- Enables risk based authentication (transaction risk analysis)
- Intervention with the consumer is minimized



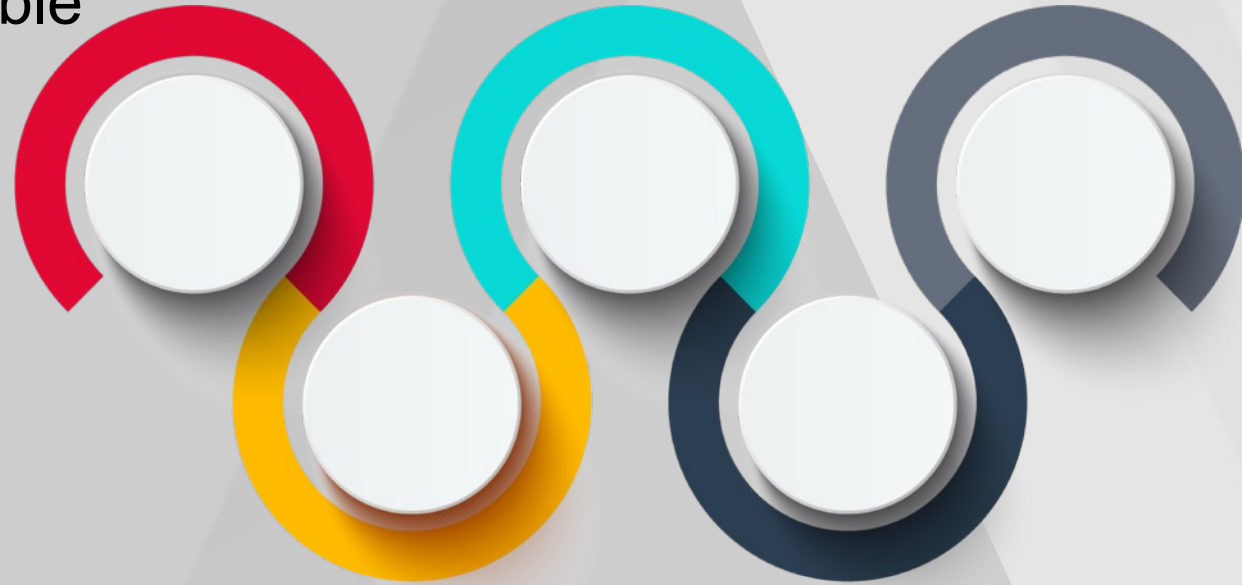
CONCEPT

- If intervention is required, streamline authentication:
 - Native look & feel integration with merchant apps via API
 - Browser based adjusts to consumer devices
 - Issuer owns the content, merchants control the flow

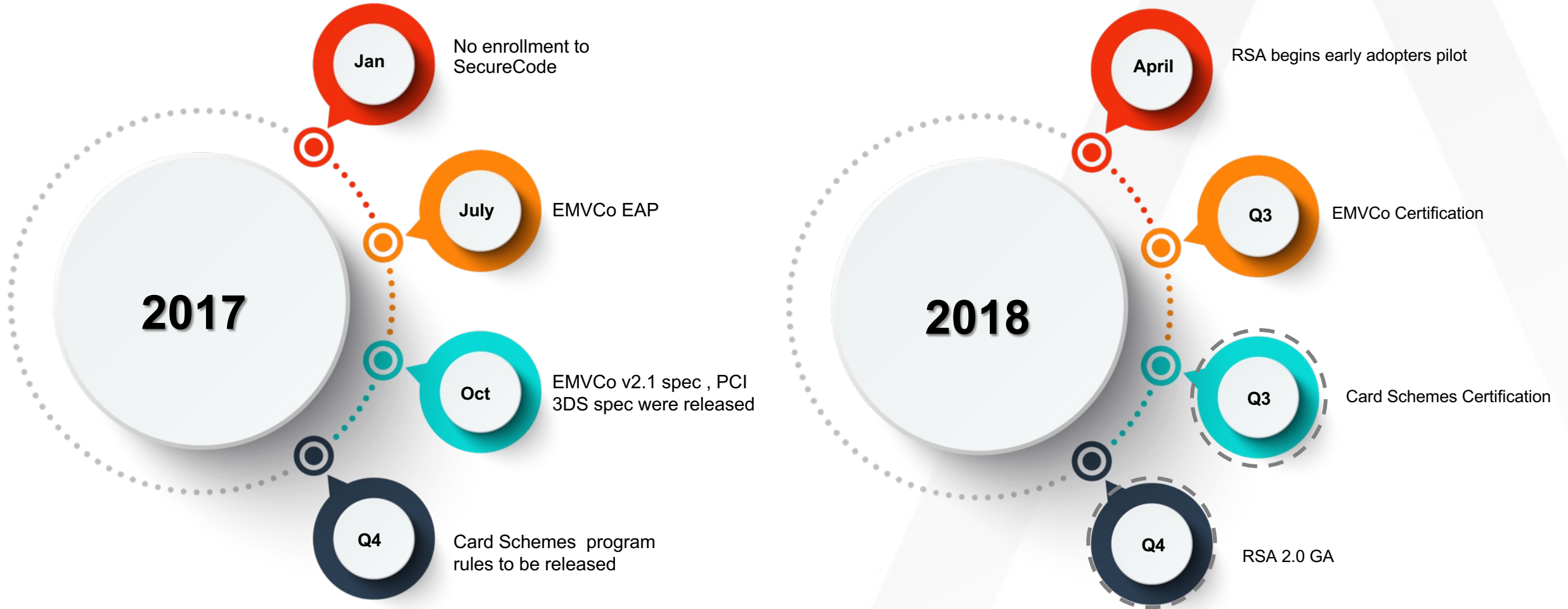


CONCEPT

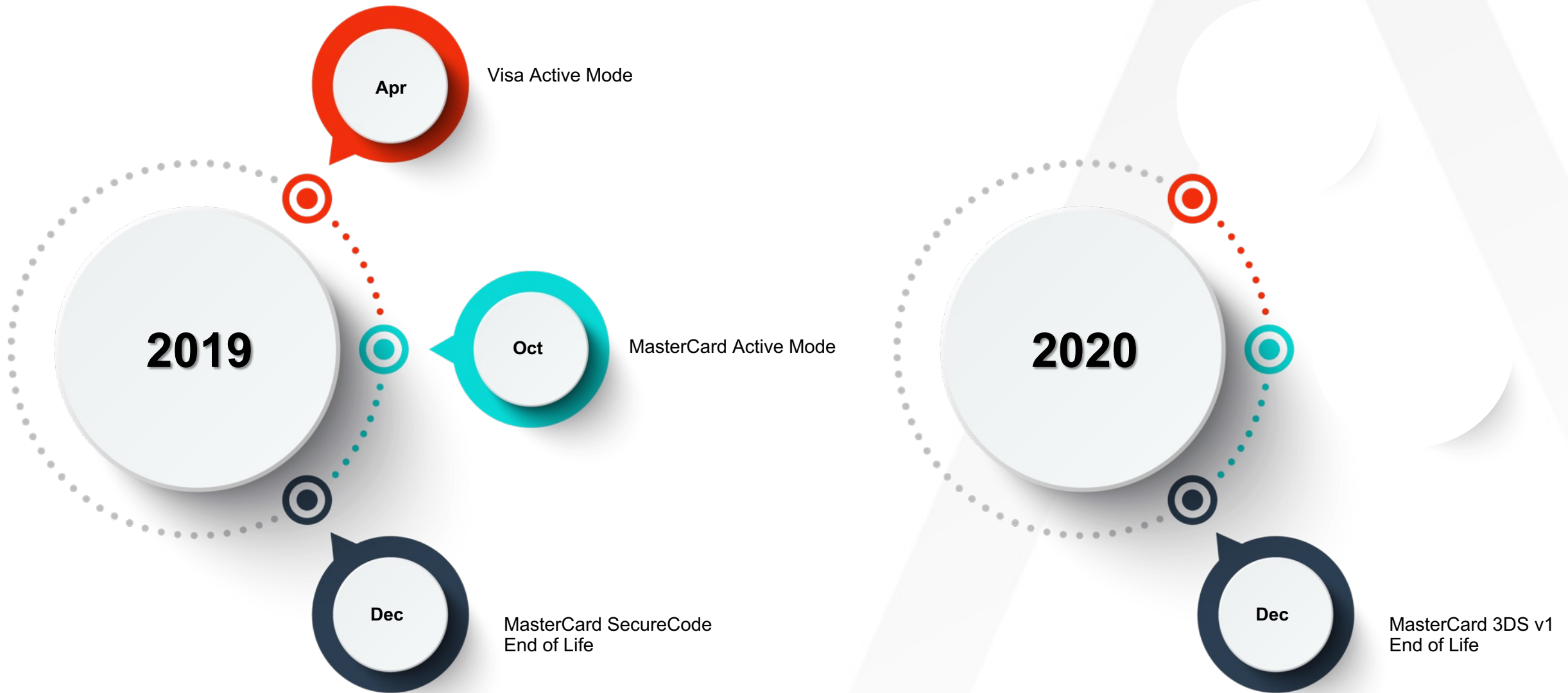
- Consumer active enrollment is excluded
- Static passwords are no longer acceptable
- Risk based authentication is required



EMV 3DS TIMELINE



EMV 3-D SECURE (3DS2.0) TIMELINE



Mastercard® Biometric Authentication in the Europe Region

Standards Specification v1.0

11 January 2018



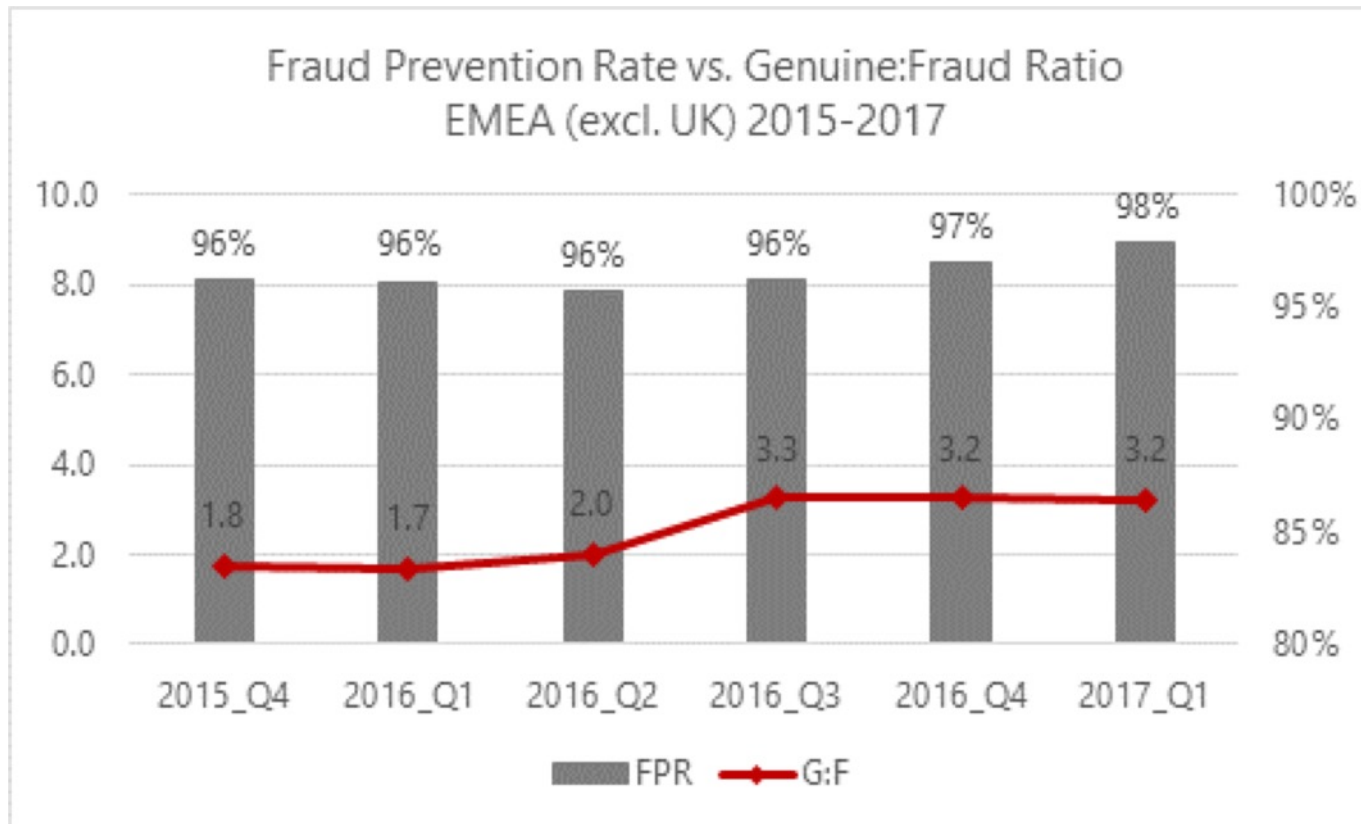
**1 Sept 2019
for CEE**

As of 01 April 2019 (unless specified differently in your markets, please refer to the announcements published in your country), organizations are required to offer their customers biometric authentication for Masterpass and SecureCode/Identity Check transactions.

These standards apply to all Mastercard® and Maestro brand cards (including consumer, commercial, prepaid, and debit cards) enabled for electronic remote transactions, and to near-field communication (NFC) transactions at terminals with mobile devices.

FRictionless?

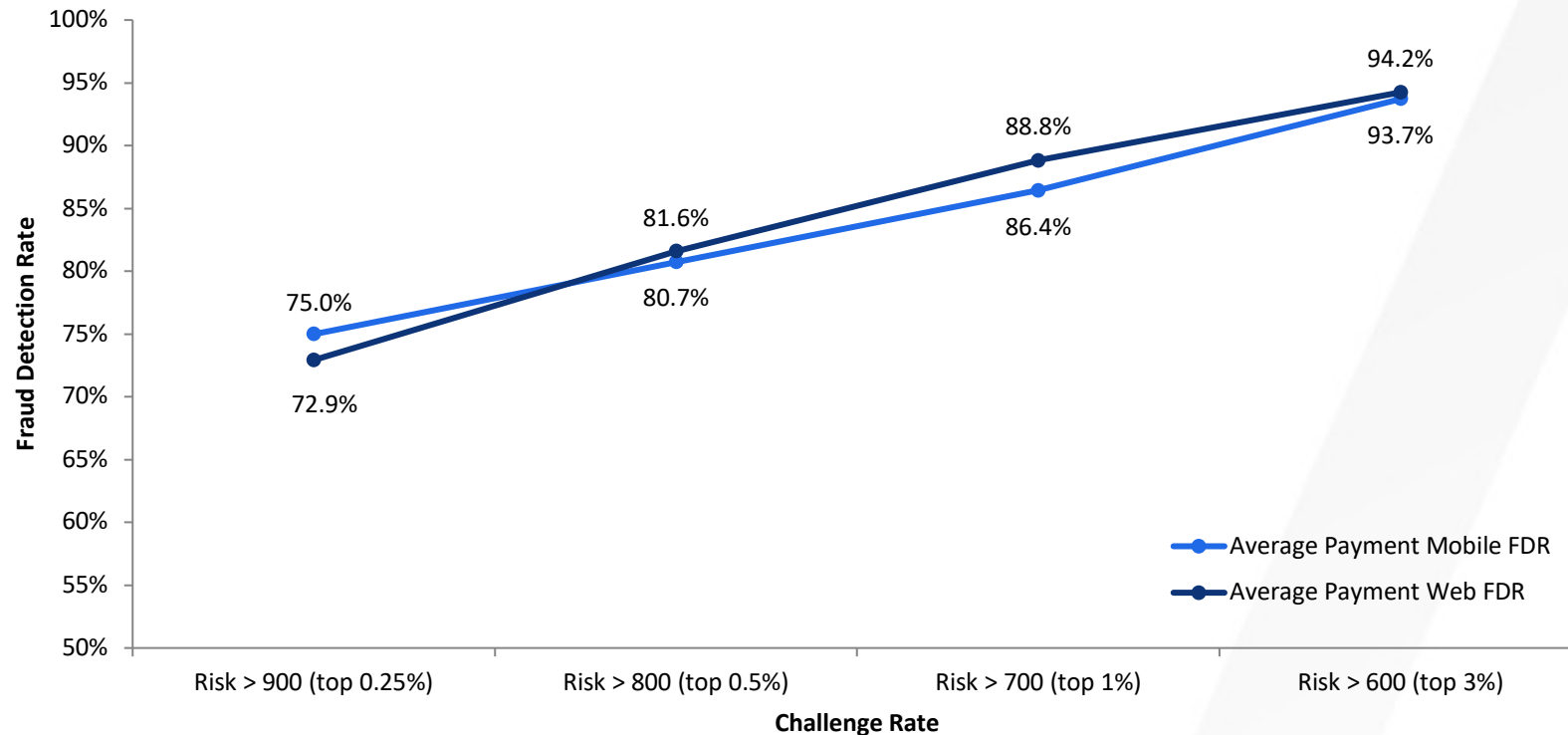
- PSD2 Transaction Risk Analysis and PSD2 exemptions reduce intervention.



3DS: 98% fraud prevention
@
3.2:1 Genuine:Fraud
intervention rate

FRICITIONLESS?

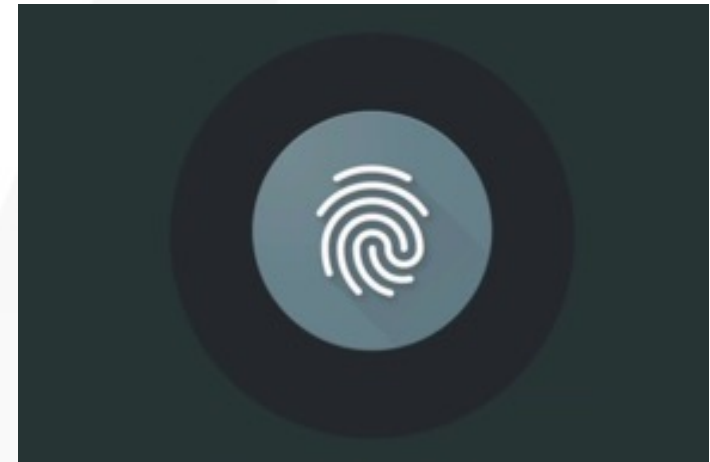
- Transaction Risk Analysis exemption thresholds require using risk engines with proven results of very high fraud detection with very low challenge rate.



Payments Mobile + Web:
94% fraud prevention
@
3% intervention rate


FRICITIONLESS?

- Authentication methods need to be frictionless as possible
- Consumers demand using what is fast and familiar: mobile apps & biometrics
- Need to accommodate all consumer types and banking products.



THANK YOU

Nathan Close

 nathan.close@rsa.com  [linkedin.com/in/nclose](https://www.linkedin.com/in/nclose)  [@n&close](https://twitter.com/n&close)