



Baltic e-Commerce Forum 2020

Payment Service Directive 2 & Strong Customer Authentication



Presenters



Tomas Bromander

Director Business
Development

Mastercard

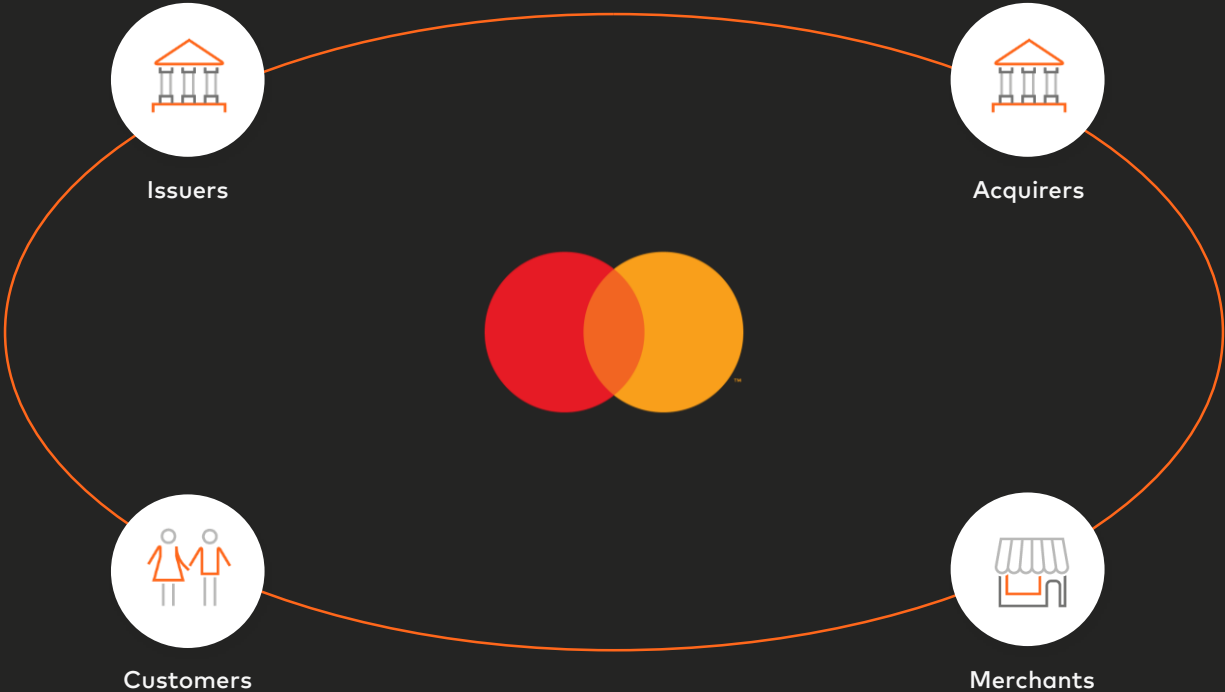


Tanja Wesén

Director Cyber &
Intelligence Solutions

Mastercard

Mastercard's operating model



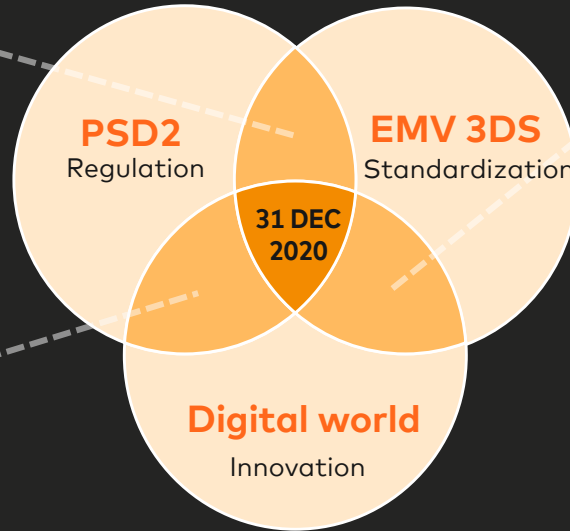
Focus Areas



A major change in an innovative landscape – PSD2 SCA



Environment & objectives



Rules & regulations

How to match & anticipate (future) use cases

Authentication guidelines

Educate & align
5000+ Issuers
~800 Acquirers & PSPs
140 ACS
And...
1.4 million merchants
or
2 billion tx

Customer journeys

Keep/Adapt EMV 3DS to be compliant with PSD2

One click experience

How is regulation impacts today multitude of digital UX

Are you ready for Dec 31st 2020 to manage your payments ?



1.

What is Strong Customer Authentication (SCA) & why did EU enforce SCA ?

What dates do we need to respect to be compliant ?

What parties in the payment ecosystem is impacted ?

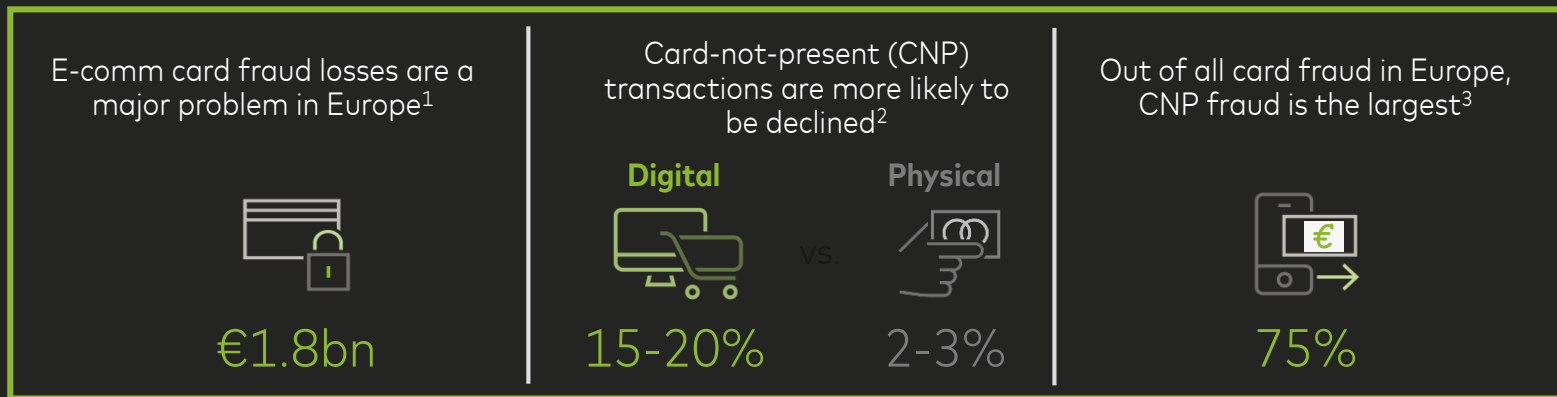
What are the opportunities with SCA ?

What do I need to do as an e-comm Merchant to be ready ?

What is Strong Customer Authentication & why did EU enforce it ?

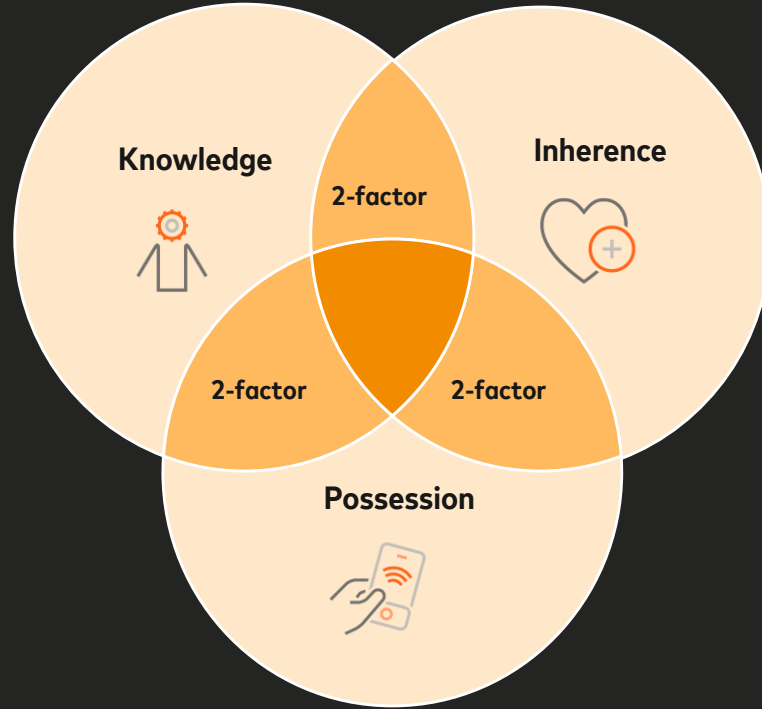


Reduce Fraud



- Global **E-COMM MARKET** is estimated at **\$1.95bn** in 2020
- Global **FRAUD** is estimated to about **\$3.1trn** in 2020

What is Strong Customer Authentication & why did EU enforce it ?



Strong 2 factor authentication

What is Strong Customer Authentication & why did EU enforce it ?



Minimise the impact on the customer experience

Static passwords & authentication methods are outdated

20-25%
online purchases
in Europe
are abandoned
before completion⁴

False declines impact cardholders' trust

1/3
after being
falsely declined consumers
either abandoned their
card or used it less⁵

Consumers prefer faster processes and show readiness for new solutions (e.g. biometrics)

58%
of interviewees
positively
evaluate biometric
solutions⁶

What is Strong Customer Authentication & why did EU enforce it ?



->SCA Exemptions



LOW VALUE - Remote transactions **up to EUR 30** (for 5 consecutive transactions, or alternatively for total of EUR 100)



FRAUD RATES TRA THRESHOLDS - Remote transactions between **EUR 30** and **EUR 500** provided **RBA** is applied** by the issuer or the acquirer and **their fraud rates are under specific thresholds**

TRA
Thresholds

Issuer bps	Exempt up to:
< 13 bps	100€
< 6 bps	250€
< 1 bps	500€



WHITE LISTING - Remote transactions to **white lists of trusted beneficiaries and recurring transactions** (SCA is required for the initial 'subscription')



CONTACTLESS - transactions up to **EUR 50** (for 5 consecutive transactions, or alternatively for total of EUR 150)

What is Strong Customer Authentication & why did EU enforce it ?



SCA is required when the user



Initiates an electronic payment transaction

Applicable to F2F and remote payments (e-comm, mobile, browser-based and in-app)



Carries out an action through a remote channel which may imply a risk of payment fraud or other abuses

Applicable e.g. to card-on-file provisioning and e-mandate



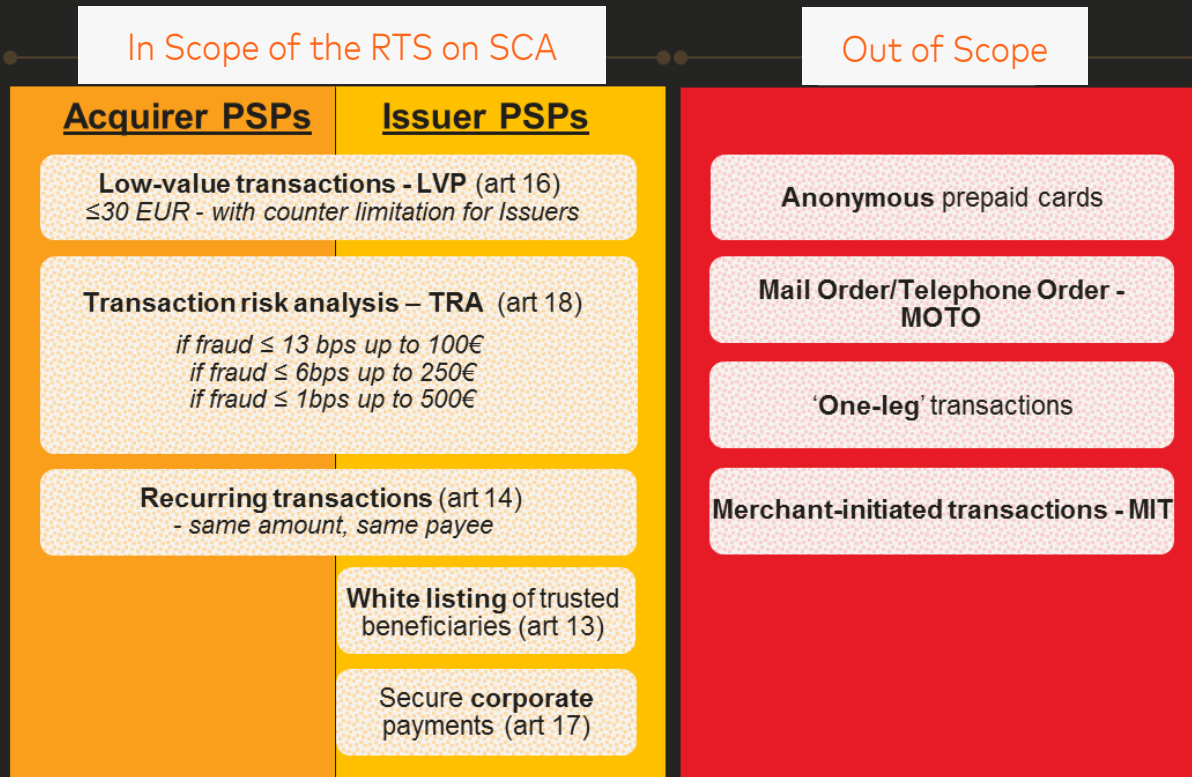
Accesses his payment account online

Includes access to B2B accounts and through AISPs

What is Strong Customer Authentication & why did EU enforce it ?



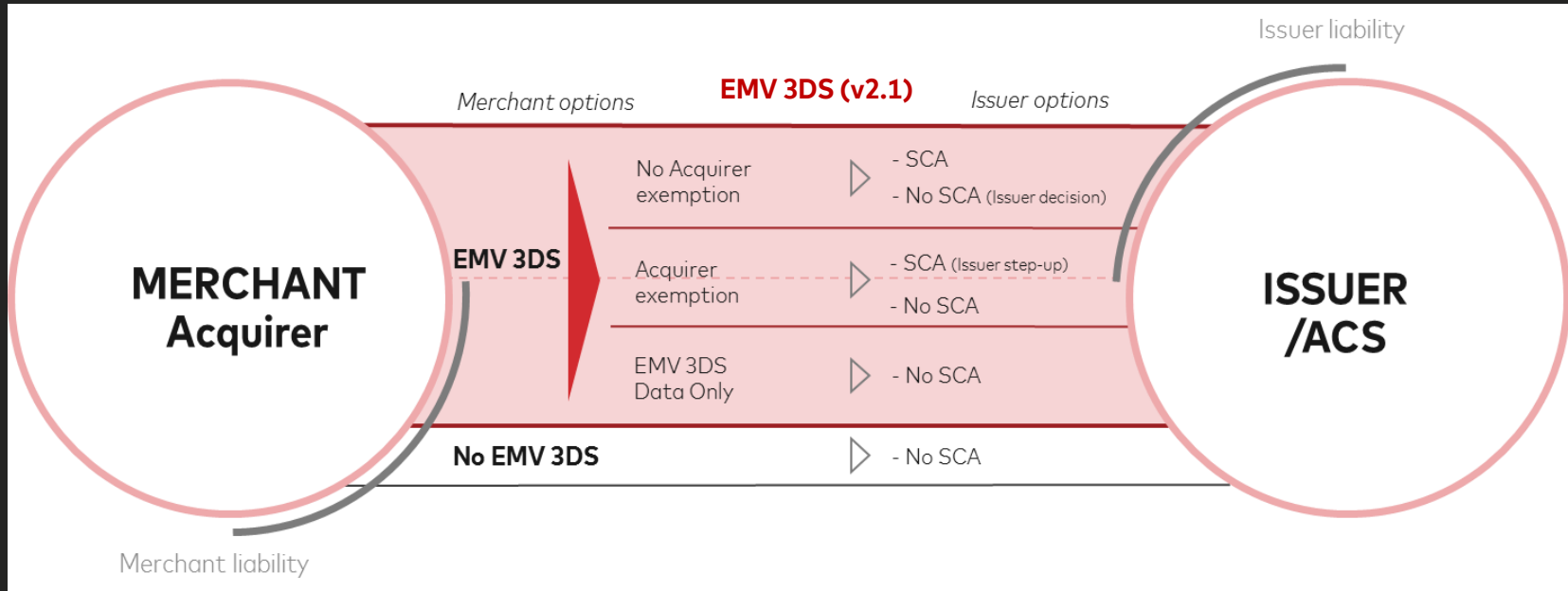
In and out of scope of the PSD 2 RTS (Regularly Technical Standards)



What is Strong Customer Authentication & why did EU enforce it ?



Key principle: Issuer always have the final say



What is Strong Customer Authentication & why did EU enforce it ?



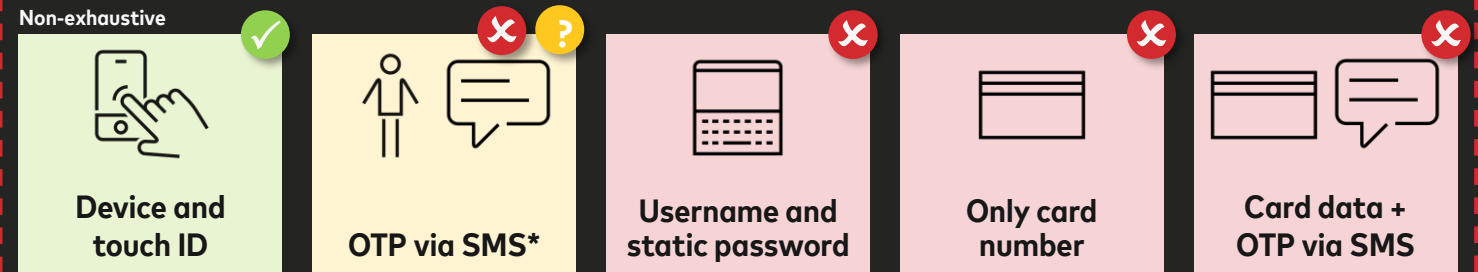
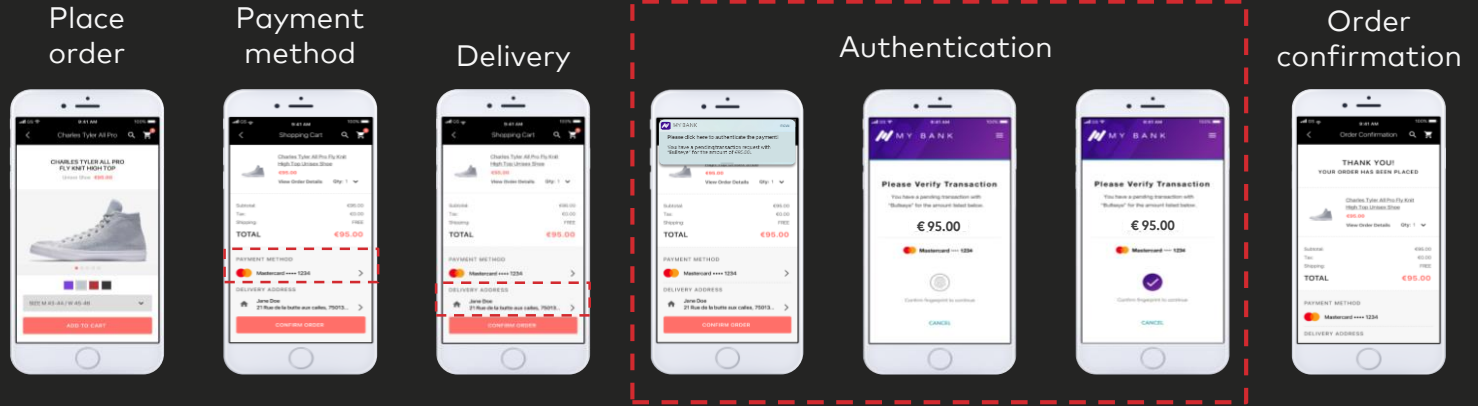
How will my customer journey change with SCA ?

1.

SCA may lead to an increased step-up rate on the short-term

2.

SCA compliance will require specific authentication methods



✓ Compliant with SCA

? Clarified by the EBA as non-compliant** but every NCA can decide what to allow

✗ Non-compliant with SCA

What is Strong Customer Authentication & why did EU enforce it ?



KNOWLEDGE

Something only the user knows

- Static Password
- 4-Digit PIN
- Card details (PAN + Expiry + CCV)



INHEREANCE

Something the user is (Biometrics)

- Touch ID
- Facial recognition
- Iris recognition
- Voice
- **Biometric behavior / passive biometrics**



POSSESSION

Something only the user possesses

- Payment card (Chip DDA+)
- Phone (Smartphone)
- Wearable: smartwatch, smartkeys etc.
- Token (Hard/Soft)
- **OTP via SMS**
- Card data +OTP SMS



The **independence of factor does not require different devices**: the use of the phone as a factor of authentication (possession) and as a device to read/store the authentication (knowledge or inherence) is **expressly accepted**.

Are you ready for Dec 31st 2020 to manage your payments ?



What is Strong Customer Authentication (SCA) & why did EU enforce SCA ?

2.

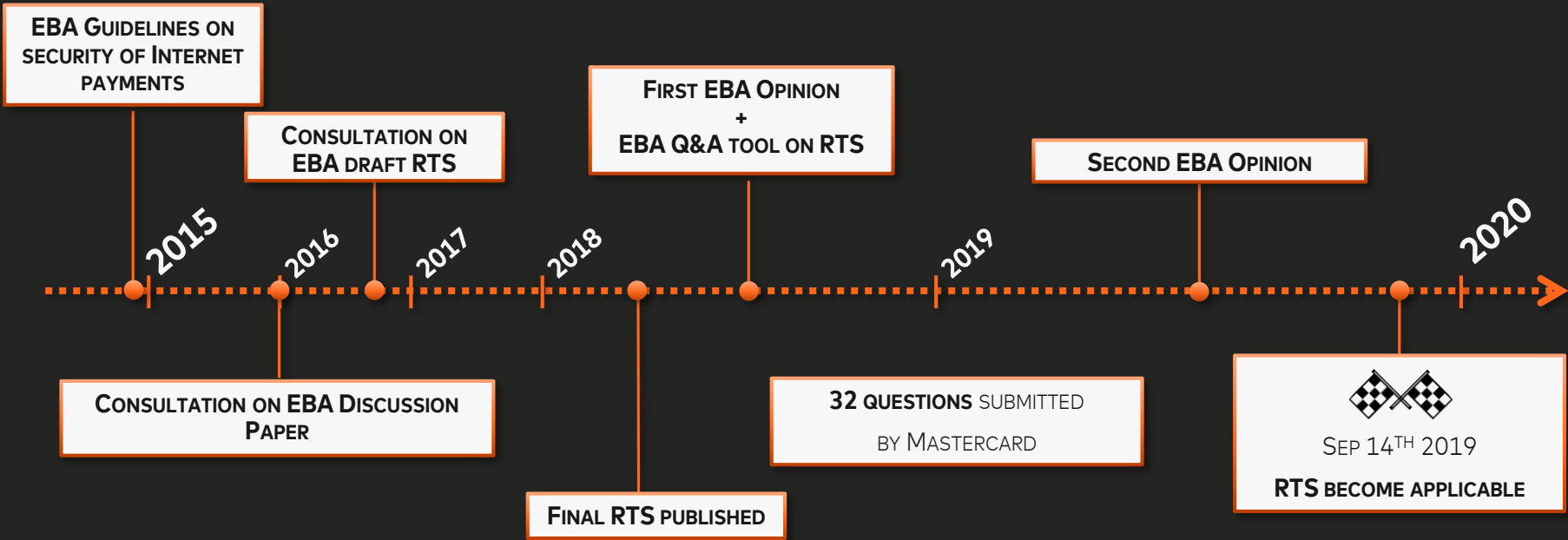
What dates do we need to respect to be compliant ?

What parties in the payment ecosystem is impacted ?

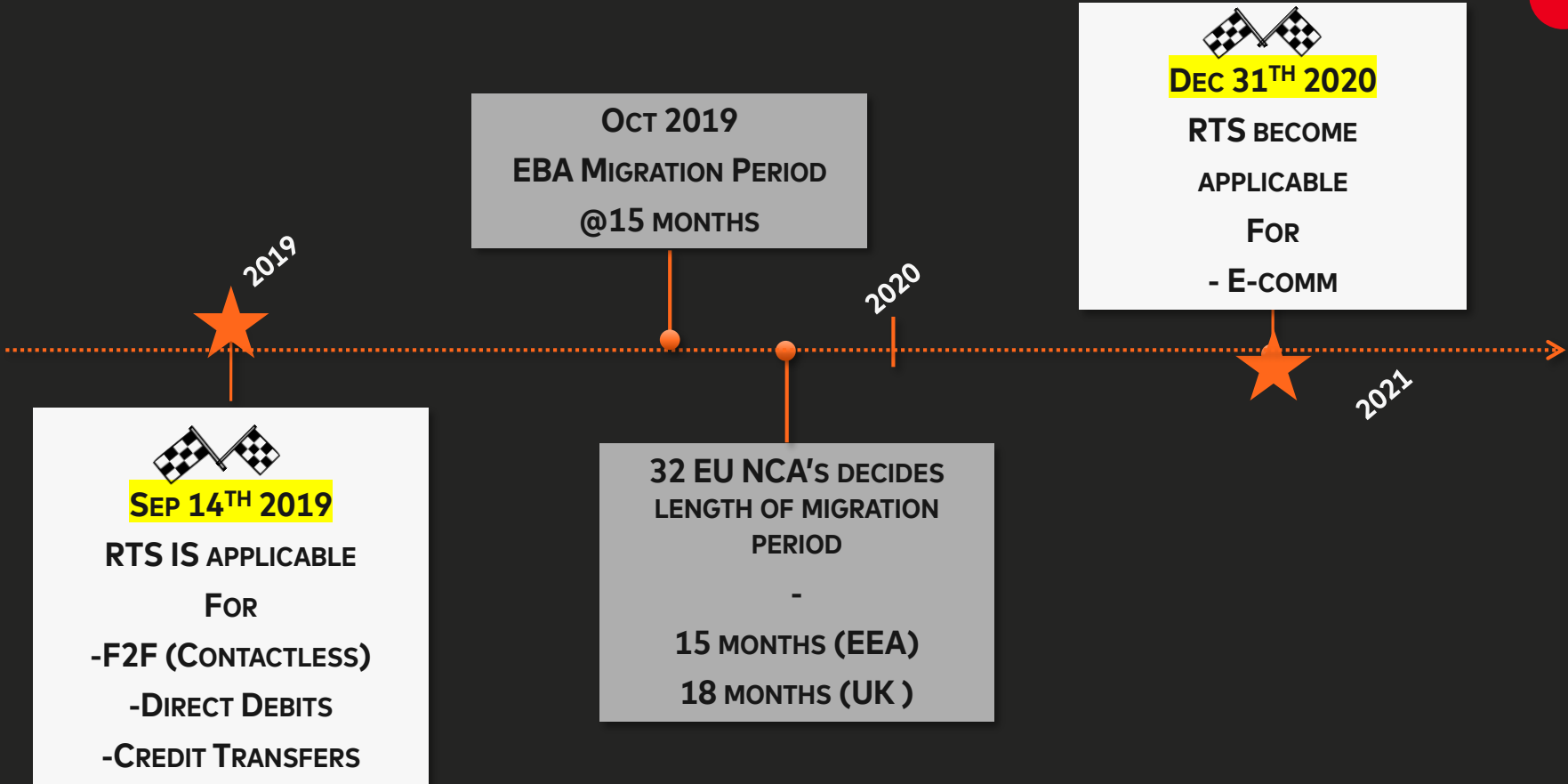
What are the opportunities with SCA ?

What do I need to do as an e-comm Merchant to be ready ?

What dates do we need to respect to be compliant ?



What dates do we need to respect to be compliant ?



Are you ready for Dec 31st 2020 to manage your payments ?



What is Strong Customer Authentication (SCA) & why did EU enforce SCA ?

What dates do we need to respect to be compliant ?

3.

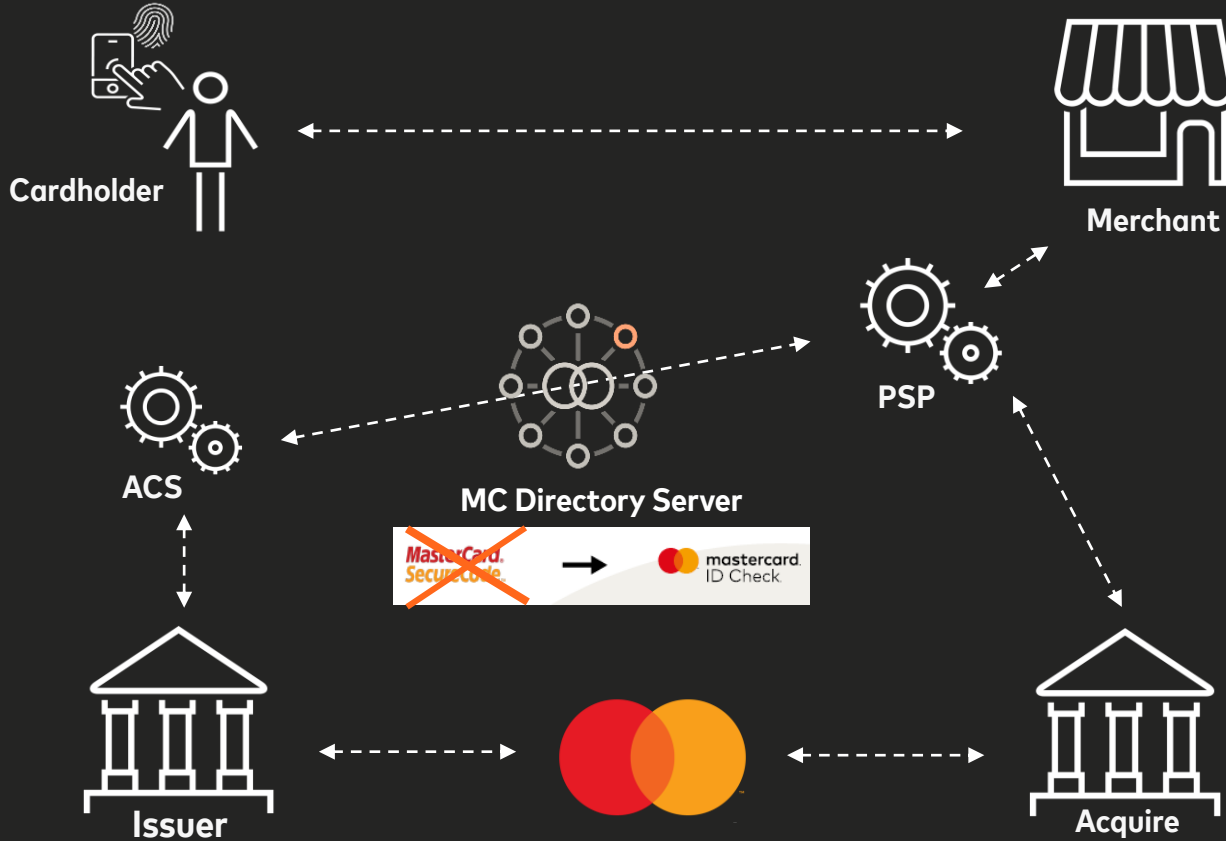
What parties in the payment ecosystem is impacted ?

What are the opportunities with SCA ?

What do I need to do as an e-comm Merchant to be ready ?

What parties in the payment ecosystem is impacted ?

**EMV
3DS
flow**



What parties in the payment ecosystem is impacted ?



RTS Key Principal: Dynamic linking

The authentication code has to be linked to the Merchant name and Authentication amount

- Unique Merchant ID
+
- Total Amount
+
- 2 Factor Authentication (SCA)

Are you ready for Dec 31st 2020 to manage your payments ?



What is Strong Customer Authentication (SCA) & why did EU enforce SCA ?

What dates do we need to respect to be compliant ?

What parties in the payment ecosystem is impacted ?

4.

What are the opportunities with SCA ?

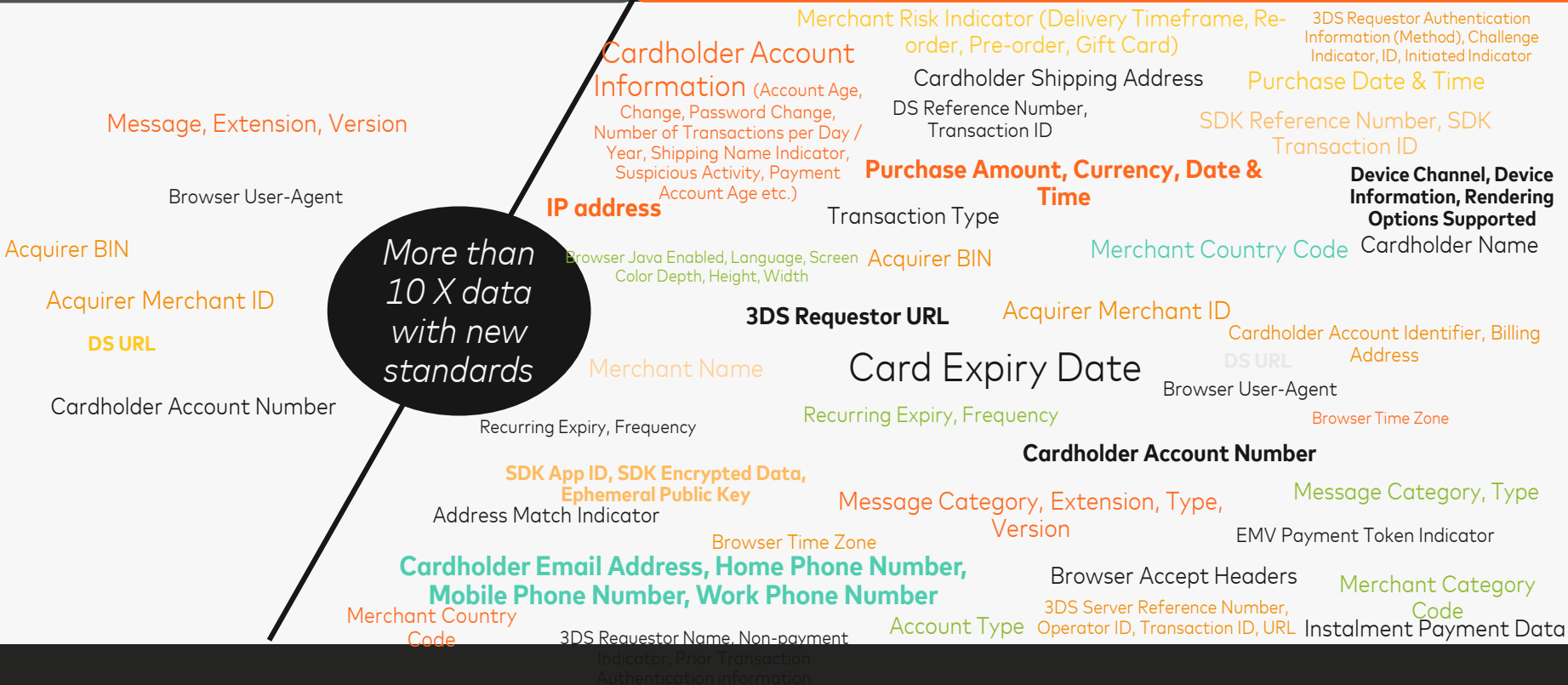
What do I need to do as an e-comm Merchant to be ready ?

What are the opportunities with SCA ?



3DS 1.0 Data (Initial Message – VEReq)

EMV 3DS Data (Initial Message – AReq)



What are the opportunities with SCA ?

Transaction impact

Short term impact

- **Increased abandonment rate** in eCom due to higher transaction friction
- **Increased decline rate** in eCom when authorization or exemptions not supported
- **Decreased CNP fraud rate** thanks to more robust authentication process

Long term impact

- **Long term threat:** potential of eCom volume moving away from card to alternative (ACH based) payment methods offering superior UX
- **Decreased decline/abandonment¹ & lower CNP fraud rates** thanks to a more robust authentication process

1. Includes decrease in "false declines"



Are you ready for Dec 31st 2020 to manage your payments ?



What is Strong Customer Authentication (SCA) & why did EU enforce SCA ?

What dates do we need to respect to be compliant ?

What parties in the payment ecosystem is impacted ?

What are the opportunities with SCA ?

5.

What do I need to do as an e-comm Merchant to be ready ?

What do I need to do as an e-comm Merchant to be ready?



Don't wait - contact your
Acquirer & PSP today to ensure
that you will be able to complete
payments by Jan 1st 2021!



"The only way to make sense out of change is to plunge into it , move with it, and join the dance."

Alan Watts



Thank you



tanja.wesen@mastercard.com

tomas.bromander@mastercard.com

