Advancing secure authentication in view of regulatory, competitive and technological changes

May 2017

Where 3DS authentication is currently used, poor user experience leads to fewer completed transactions and higher cost

Poor user experience leads to authentication abandonments

- SecureCode abandonments vary by country between 7%-35% with 4% for best in class issuers

Some merchants neither attempt authentication, nor use Risk Based Decisioning

- Between 5%-50% of ecom transactions by country are authenticated

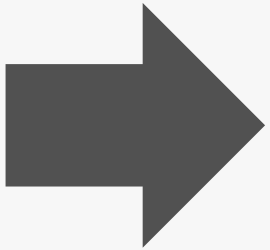
Not authenticated transactions have - lower approval rate - higher fraud rate

- Typically 10 percentage points lower approval rate
- Not authenticated transactions have 2 times higher fraud rate vs Full SecureCode

RTS Impact 1: Risk Based Authentication (RBA) will be limited, which could reduce the ecom card business due to authentication abandonments

RTS requires:

1. Strong 2 factor authentication for remote transactions > €30 (with cumulative €100 or 5 tx)
2. Risk Based Authentication (RBA) only if issuer or acquirer has low gross fraud rate:
    1. Up to €100 if max 13 bps
    2. Up to €250 if max 6 bps
    3. Up to €500 if max 1 bp



1. **Current authentication abandonments may apply to twice as many ecom transactions as today**
2. **Current abandonments may double if RBA has to be limited**

Remarks:

- Studies conclude that abandonment rate 2-4 times higher without RBA.
- Based on 2015 data.
- RTS=Regulatory Technical Standards to complement PSD2, SCA=Strong Customer Authentication, RBA=Risk Based Authentication

RTS Impact 2: Cards may become less attractive for consumers than emoney wallets and direct debits

- Probably no white listing of payees for cards (credit transfers / e-money transfers allow white listing)
- Card-on-file will probably require authentication per transaction and for setting-up
- Recurring card transactions only if same amount/merchant
- Direct debits do not require SCA (only to set-up)

1. Allows emoney wallets like Paypal to offer one-click shopping if funding via direct debit and merchants are white-listed (*)

   One-click card payments for limited amounts only if low fraud (**)

2. Makes direct debits more attractive than card-on-file

(*) RTS allows market places like Amazon to be treated as merchant; Paypal can propose consumer a list of merchants to be white listed which consumer must confirm with SCA

(**) Only 8% of ecom transactions in EEA currently have fraud levels that allow RBA without SCA up to €100

Acquirers and Issuers will also be negatively impacted by RTS

Acquirers	Issuers
Card share of ecom payments and related revenues likely to drop (due to merchant white listing ban, COF possibly requiring SCA, recurring payments only if same amount, alternative payment methods strengthened with access to account and payment initiation)	
Added value and income from fraud prevention likely to reduce if all transactions are authenticated	Investments needed to comply with RTS (currently not SCA compliant with dynamic linking, real-time transaction monitoring)
Investments needed to comply with RTS (COF possibly requires SCA, authentication decisioning logic using issuer country)	RBA requires better fraud prevention, approval from competent authorities with extensive reporting

COF=Card-on-file

Recommendation 1: Issuers must urgently improve authentication methods to reduce abandonment rates and remain competitive vs emoney wallets

1. Deploy mobile apps with biometric authentication[1], fallback method OTP SMS for cardholders without smart phone

- Lower abandonment rates (3% vs 15% OTP), lower fraud (NIST recommendation to avoid SMS OTP), full PSD2 compliance (SMS OTP requires password as 2nd factor in Germany, key fobs do not provide dynamic linking)
- Used for manual PAN entry/SecureCode and Masterpass
- Ideally integrated with mobile banking app with cardholder enrolled automatically for SecureCode

1 RTS requires real-time monitoring mechanism for all transaction to check lists of compromised or stolen authentication elements, the amount of each payment transaction, known fraud scenarios in the provision of payment services, signs of malware infection in any sessions of the authentication procedure

OTP=One Time Password

Recommendation 2: Expand Card-on-file (COF) and Masterpass acceptance (*)

Strategic Rationale	• **Make cardholders loyal with great user experience before RTS makes eMoney more attractive**

(*) COF flag in authorization and clearing messages as of October 2017 will allow us to monitor progress and to focus on markets or segments where COF penetration needs improvement.

Recommendation 3: Ensure plan is met to roll-out Identity Check (*) and 3DS 2.0 (**) to enhance SecureCode

Ban bad user experience mastercard ID Check

- Ban static passwords and Knowledge Based Authentication (KBA)
- Ban Activation During Shopping (ADS)

Drive good user experience mastercard ID Check

- Risk Based Authentication (RBA)
- Auto/pre-enrollment or manual enrollment with appropriate communication
- Key performance indicators
- Provide best practices for issuers and merchants

Provide new functions with 3DS 2.0

- Support any device
- Enable in-app payments
- Provide more data to reduce fraud risk with RBA
- Simplify message flow to reduce cardholder abandonments

→ More enrolled cardholders

→ Reduced abandonments

→ More merchants requesting authentication for risky transactions

→ Reduced fraud

→ Reduced chargebacks

→ Higher approval rate

(*) Identity Check Authentication (different from Identity Check Mobile, which is our biometric authentication service) will replace SecureCode by December 2019

(**) 3DS 2.0 (launched by EMVCo) is a new protocol for handling SecureCode and Identity Check authentications which issuers have to support as of December 2018 (on top of the current protocol 3DS 1.0 which will continue to be used until merchants have migrated to 3DS 2.0 by December 2020)

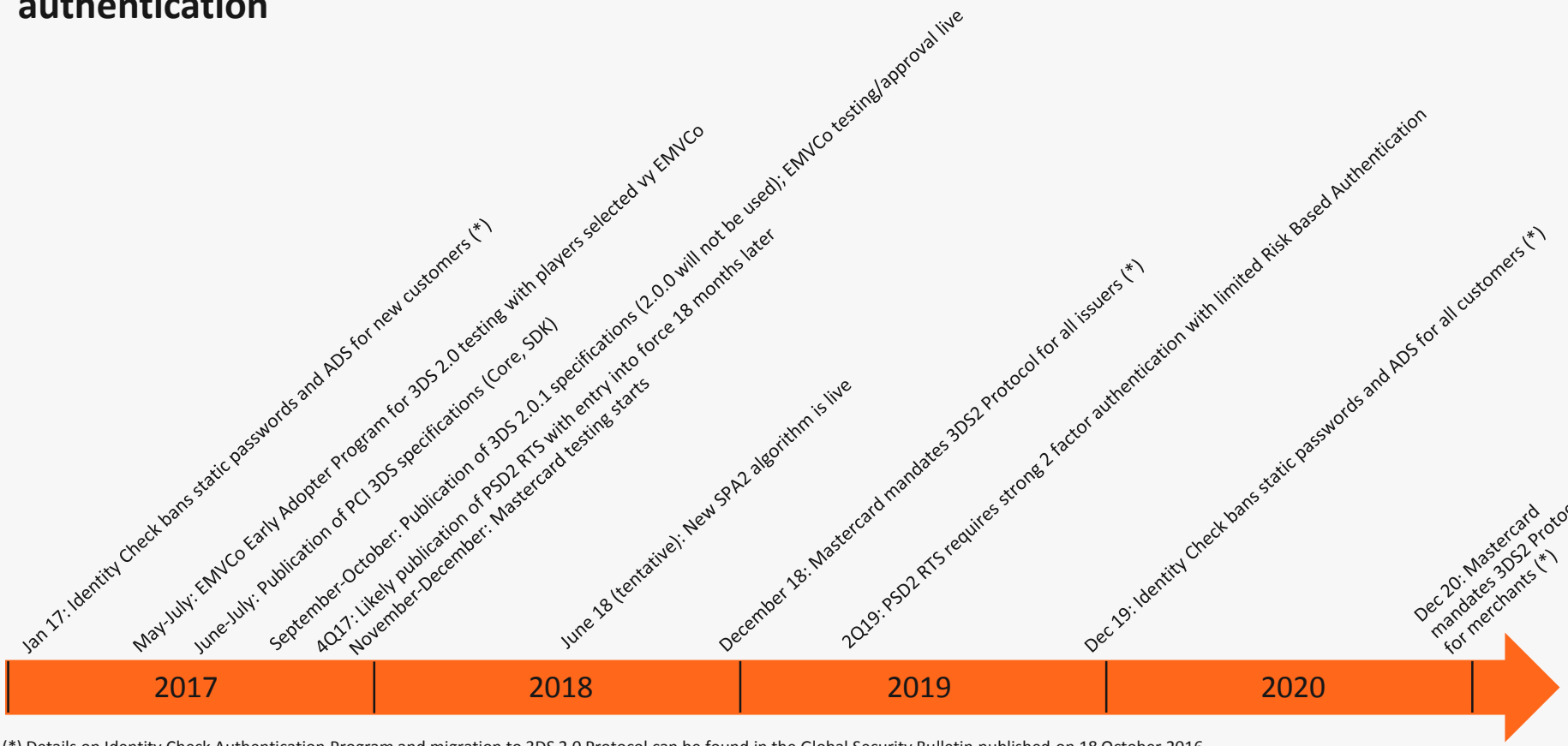
Other ideas for mitigating impact of RTS on card industry

- **Promote to shoppers the security aspect of cards (eg Zero Liability) vs other payment methods (*)**
- ?

(*) According to Ystats survey in February 2016, security is

- 2nd reason why shoppers don't buy online (27% of EU population)
- 1st reason for selecting payment method (eg 97% of Germans)

Appendix: Overview of mandates for Identity Check, 3DS 2.0, PSD2 related to ecom authentication



(*) Details on Identity Check Authentication Program and migration to 3DS 2.0 Protocol can be found in the Global Security Bulletin published on 18 October 2016