European Payment Institutions Federation aisbl

13 JUNE 2017

EPIF COMMENTS ON THE REVISED DRAFT RTS ON STRONG CUSTOMER AUTHENTICATION AND SECURE COMMUNICATION

ABOUT EPIF (EUROPEAN PAYMENT INSTITUTIONS FEDERATION)

EPIF, founded in 2011, represents the interests of the non-bank payment sector at the European level. We currently have over 190 authorised Payment Institutions (PIs) and other non-bank payment providers as our members offering services in every part of Europe. EPIF thus represents roughly one third of all authorized Payment Institutions in Europe. Our diverse membership includes a broad range of business models, including:

- Three-party Card Network Schemes
- Acquirers
- Money Transfer Operators
- FX Payment Providers
- Mobile Payments
- Payment Processing Service Providers
- Card Issuers
- Third Party Providers
- Digital Wallets

EPIF seeks to represent the voice of the PI industry and the non-bank payment sector with EU institutions, policy-makers and stakeholders. We aim to play a constructive role in shaping and developing market conditions for payments in a modern and constantly evolving environment. It is our desire to promote a single EU payments market via the removal of excessive regulatory obstacles.

We wish to be seen as providers for efficient payments in that single market and it is our aim to increase payment product diversification and innovation tailored to the needs of payment users (e.g. via mobile and internet).

EPIF's COMMENTS

Please find below some comments on specific articles which we hope you will find useful at this stage of the process.

- **Article 5**

  Our understanding is that the intent of dynamic linking is to prevent man-in-the-middle attacks whereby the amount or payee can be intercepted by a fraudster and funds can be redirected. The likelihood of such an outcome for remote card transactions is very low if not nil, particularly if an authentication tool is used, so it is difficult to see how the introduction of dynamic linking for remote card transactions will reduce fraud.

  Furthermore, there are well-established merchant processes where the merchant identification and amount associated with the transaction can change (e.g. online supermarket orders and delayed shipment) and our current reading of the requirements suggest that such transactions would need to be declined, which would have a significant impact to merchants and consumers, with little or no equivalent reduction in fraud.

  On this basis, we propose that card based transactions are exempt from the dynamic linking requirements provided they are protected from man-in-the-middle attacks.

- **Article 11**

  The challenge with the current contactless exemption is the prescriptive nature of the requirement for SCA after a set cumulative amount and number of transactions, which cannot be achieved without significant technology changes such as point of sale upgrades and card re-issuance, which is impossible to change prior to the RTS coming into effect . While issuing PSP's already use offline counters and online authorisation to effectively mitigate risk and customer harm, they do not trigger authentication. The article of the RTS needs to reflect that it is not systematically possible to do. Furthermore the requirement is unnecessary, as the existing and planned controls to safeguard lost/stolen fraud are more than adequate.

  We suggest relaxing the requirements to keep the maximum transaction amount to 50 euros but not introduce prescriptive thresholds.

- **Article 12**

  This article currently only applies to transport fares and parking fees, and should be extended to cover all type of other unattended terminals such as vending machines.

  Suggested changes: Unattended terminals

Payment service providers shall be allowed not to apply SCA subject to compliance with the requirements laid down in Article 2 where the payer initiates an electronic payment transaction at an unattended payment terminal.

- **Article 13**

Under article 13 of the EBA's February RTS, SCA was exempted for transactions to payees included in a list of trusted beneficiaries previously created by the payer, or confirmed by the payer through its ASPSP. In the Commission's redrafted RTS, the option to have a list of trusted beneficiaries confirmed through the ASPSP seems to have disappeared.

We recommend to go back to the EBA's version. ASPSPs should be able to generate their own whitelists to reflect ongoing customer behaviour, the risk-profile of the payee, the frequency of such payments etc. This would allow for the ASPSP to apply its risk management practices to the benefit of customers' convenience, thereby mitigating the negative impact of SCA on the customer and merchant experience.

- **Article 14**

The exemption for recurring transactions only covers transactions for the same amount, yet there are recurring transaction which vary (e.g. phone bills) that should benefit from this SCA exemption.

Suggested changes

Payments service providers shall apply strong customer authentication when a payer creates, amend, or initiates for the first time, a series of recurring transactions with ~~***the same amounts and***~~ *the same payee.*

- **Article 16**

Article 16 on low value transactions provides prescriptive and cumulative conditions for the exemption, i.e. a transaction amount of 30 EUR, a cumulative amount of 100 EUR and a set number of consecutive transactions (5). This is highly prescriptive and does not offer additional security benefits to the consumer. From a security perspective, the value of the transaction, the cumulative value or even the number of transactions are only one of many factors that describe the actual level of risk posed by the transaction: other elements are also taken into account, such as location, the device used or the user's usual pattern of behaviour, the IP address, etc. These elements are included in existing and future controls contained in the risk-based approach. There is therefore no need to set out such prescriptive conditions under article 16. We suggest relaxing the requirements to what the EBA originally intended to either/or threshold requirements.

We suggest relaxing the requirements to what the EBA originally intended to either/or threshold requirements, but not both and keep the maximum transaction amount to 50 euros.

- **Article 17**

We welcome the addition of Article 17 on corporate payments exemption and would like to suggest a slightly different wording to improve the requirement.

Suggested changes

> *Payments services providers shall be allowed not to apply strong customer authentication in respect of payment service user not being a consumer of* ~~***legal persons***~~ *initiating electronic payment transactions through the use of dedicated corporate payment processes or protocols where the competent authorities are satisfied the those processes or protocols* ~~***guarantee***~~ *achieve at least equivalent levels of securities to those aimed for by Directive 2015/2366.*

- **Article 18**

Article of the RTS on SCA introduces the transaction risk analysis exemption and Article 19 of the RTS on SCA details the calculation of fraud rates. While PSPs can make an effort to interpret the words and calculate the fraud rates, clear guidelines are missing. The statutory auditor will also require clear guidelines to be able to perform the required yearly audit accurately. We understand that the SecurePay Forum is working on guidance on this subject. We would like to see a formal reference in the RTS on SCA that will make sure guidelines for the fraud rates calculation will be created.

- **Article 31**

The Commission amendments and introduction of a fallback-option is a substantial improvement. The existence of such fallback-option is the only thing that ensures that TPPs and fintechs can survive also if a dedicated interface provided by an ASPSP does not work the way it should. It is self-regulating; if the API works it will be used and if not the fallback option will be used.

It is essential for innovation and competition for the entire industry that banks will not be able limit the development of Fintechs by offering "limited" APIs. The fallback solution ensures future innovation as new services can be created on the basis of the data available on the PSU's online account – without the risk that banks might withhold data that the consumer has agreed to transmit to authorised third parties.

It has to be ensured however that in particular Article 33 (3b) is not misinterpreted and/or abused in the sense that ASPSP can somehow prevent the usage of a fallback solution by means of not

enabling the TPP to rely on the authentication procedure provided by the ASPSP. Such approach would be in violation of inter alia Recital 30 and Article 97 PSD2.