The Consumer Voice in Europe

DRAFT DELEGATED REGULATION ON STRONG CUSTOMER AUTHENTICATION AND SECURE COMMUNICATION

BEUC response to EBA consultation – 12/10/2016

Contact: Farid Aliyev - Jean Allix – Financialservices@beuc.eu

BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • consumers@beuc.eu • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union

Ref: BEUC-X-2016-098 - 17/10/2016

BEUC The European Consumer Organisation

Why it matters to consumers

The revised Payment Services Directive imposes new security requirements for electronic payments, the so-called Strong Customer Authentication.[1] The European Banking Authority currently develops the technical details of these new security standards that, once implemented, are expected to improve the security of payment services, but also impact the consumers' payment experience, in particular internet and mobile payments.

Summary

BEUC in general supports the draft Regulatory Technical Standards (RTS) proposed by the European Banking Authority (EBA)[2]. Security is a major issue for consumers, as is convenience, which we explained in our response to the previous EBA consultation.

The rules defined should apply to all payment instruments and not give a competitive advantage to one specific instrument.

The objective of the RTS is to apply to general rules in PSD2, and should not be used to soften these rules. In other words, PSD2 provides the objectives, the RTS indicate how to interpret them. It is very important for us that the RTS do not weaken the objectives of PSD2.

[1] PSD2 article 4.30: 'strong customer authentication' means an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data".
Knowledge can be a pin code, possession a card and inherence a biometric fingerprint.

[2] https://www.eba.europa.eu/documents/10180/1548183/Consultation+Paper+on+draft+RTS+on+SCA+and+CSC+%28EBA-CP-2016-11%29.pdf

Answer to questions

Question 1. Do you agree with the EBA's reasoning on the requirements of strong customer authentication, and the resultant provisions proposed in Chapter 1 of the draft RTS?

BEUC agrees with the EBA's reasoning regarding the requirements on strong customer authentication, while we have some questions related to authentication code and dynamic linking (see below).

Article 1 indicates that the authentication procedure shall result in an authentication code. It has to be clarified which kind of code this article refers to. It cannot be the PIN code used by the consumer for any card payment using EMV standards. Paragraphs 24 and 25 on page 11 say that no action will be required by the payer himself. It seems that the words "authentication code" are used with different meanings all over the document.

As regards article 7 it is indicated that the strong customer authentication shall be periodically tested, evaluated and audited and that a report will be elaborated indicating the level of compliance with the Regulation. That report shall be made fully available to the competent authority upon request.

First, the tests should be carried out by a designated independent third party and the frequency of the tests should be specified by EBA. Second, the reports should be automatically provided to the competent authority. Third, how will the consumer know that the competent authorities have checked that various payment service providers conform to the law? One solution should be that the conformity reports are made available to the public on the competent authority's internet site. If the report contains information which cannot be communicated for security reasons, at the very least the minimum should be that the competent authority and/or EBA indicates that the Payment Service Provider has provided its conformity report and that the authority agrees that it conforms with the Regulation. This is a basic transparency principle.

Question 2. In particular, in relation to the "dynamic linking" procedure, do you agree with the EBA's reasoning that the requirements should remain neutral as to when the "dynamic linking" should take place, under the conditions that the channel, mobile application, or device where the information about the amount and the payee of the transaction is displayed is independent or segregated from the channel, mobile application or device used for initiating the payment, as foreseen in Article 2.2 of the draft RTS.

Article 2 of the draft RTS aims to implement Article 97.2 for PDS2[3], which concerns remote payment transactions. It is unclear from the article what is the meaning of "independent or segregated" as regards channel, mobile application or device. In terms of convenience, e.g. during holidays, the consumer should not be obliged to have several devices with him to be able to initiate a remote transaction. Therefore, it should be clarified how article 2b will apply in connection with the provisions on multipurpose devices in article 6. Does article 6 covers also article 2b?

The consumer should not be obliged to have several devices with him to be able to initiate a remote transaction

As regards article 2.3, why should there be a specific rule for card transactions? The fact that a transaction is blocked for which the amount is not known in advance could also apply to other payments instruments even if it is not common practice today. Therefore, we disagree with the idea that this rule is specific to cards despite the explanation given by point 27 page 11 of the document.

Question 3. In particular, in relation to the protection of authentication elements, are you aware of other threats than the ones identified in articles 3, 4 and 5 of the draft RTS against which authentication elements should be resistant?

No

Question 4. Do you agree with the EBA's reasoning on the exemptions from the application of Article 97 on strong customer authentication and on security measures, and the resultant provisions proposed in Chapter 2 of the draft RTS?.

[3] *PSD2, Article 97 – Authentication*

1. Member States shall ensure that a payment service provider applies strong customer authentication where the payer:
   a) accesses its payment account online;
   b) initiates an electronic payment transaction;
   c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.
2. With regard to the initiation of electronic payment transactions as referred to in point (b) of paragraph 1, Member States shall ensure that, for electronic remote payment transactions, payment service providers apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee.
3. With regard to paragraph 1, Member States shall ensure that payment service providers have in place adequate security measures to protect the confidentiality and integrity of payment service users' personalised security credentials.

4. Paragraphs 2 and 3 shall also apply where payments are initiated through a payment initiation service provider. Paragraphs 1 and 3 shall also apply when the information is requested through an account information service provider.

5. Member States shall ensure that the account servicing payment service provider allows the payment initiation service provider and the account information service provider to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user in accordance with paragraphs 1 and 3 and, where the payment initiation service provider is involved, in accordance with paragraphs 1, 2 and 3.

From the consumer perspective, it is very important that the same derogations apply in the same situations. As explained by paragraph 53 of the document, the consistent application of Strong Customer authentication (SCA) has for effect that the exemptions are applied in exactly the same way. This paragraph justifies these common rules by competition dimension. It could be added that it is also important for a consistent consumer experience. Creating different rules for identical situations would make no sense to consumers.

Article 74.2 of PSD2 states: *Where the payer's payment service provider does not require strong customer authentication, the payer shall not bear any financial losses unless the payer has acted fraudulently. Where the payee or the payment service provider of the payee fails to accept strong customer authentication, it shall refund the financial damage caused to the payer's payment service provider.*

The RTS do not indicate if this article applies even if the Strong Customer Authentication is not applied in conformity with the exemptions. In point 19 it is indicated that this article should not apply after the publication of the RTS. BEUC disagrees with this interpretation which is contrary to PSD2. BEUC considers that the EBA goes beyond its mandate and misinterprets the PSD2 provision. It must be made clear that Art 74.2 will always apply in cases where the Strong Customer Authentication is not used.

It must be made clear that Art 74.2 will always apply in cases where the Strong Customer Authentication is not used.

In its previous answer BEUC has insisted on the fact that the consumer could, in some circumstances, share his non reusable one-time dynamic transaction code but never share his reusable personal credential. Therefore, BEUC supports the position expressed by our German member VZBV regarding the risk of fraud.

Question 5. Do you have any concern with the list of exemptions contained in Chapter 2 of the draft RTS for the scenario that PSPs are prevented from implementing SCA on transactions that meet the criteria for exemption?

BEUC agrees with the various exemptions, in particular with the idea developed in paragraph 52 on the need to maintain the high level of security provided by the Chip and PIN technology.

Question 6. Do you agree with the EBA's reasoning on the protection of the confidentiality and the integrity of the payment service users' personalised security credentials, and the resultant provisions proposed in Chapter 3 of the draft RTS?

Article 10 on the protection of confidentiality creates a specific obligation when the transaction is initiated by, or through, the payee. This is logical. But the restriction to card-based payment transactions is incoherent. First, there is no logic in having a specific right regarding cards. Second direct debits are also transactions initiated by, or through, the payee. In several countries some kinds of transactions initiated face-to-face or at a distance are classified technically as a direct debit if a card is used. These transactions are not considered as card-based by EU legislation. Why should the article not cover this situation? Therefore, the sentence *"in the context of a card based transaction"* should be deleted.

The sentence *"in the context of a card based transaction"* should be deleted.

In addition, EBA should clarify that any electronic mandate setting up series of direct debits should also be covered by Strong Customer Authentication.

Question 7. Do you agree with the EBA's reasoning on the requirements for common and secure open standards of communication for the purpose of identification, authentication, notification, and information, and the resultant provisions proposed in Chapter 4 of the draft RTS?

For BEUC the issue is about full interoperability. A consumer using any Payment Service Provider should be able to connect to his bank account. The technicalities of a network involving only PSPs are not a consumer issue.

BEUC has a concern regarding accessing the market of various non-Account Servicing Payment Services Providers (ASPSP). In recitals 10 to 13 the ASPSP can have their own dedicated communication interface and the use of this interface is described as mandatory. Article 19 provides a long list of information on the dedicated interface allowing the user to access it. The situation will be that any PSP will have to know the specificities of all ASPSPs, which is technically impossible due to the huge number of ASPSPs. This obligation can be assimilated to a contract. This is confirmed by paragraph 19a on page 9 which states: *"this would however require a prior contractual agreement between the PIS and the ASPSP".* This statement is in contradiction with article 66.5 of PSD2 which states *"The provision of payment initiation services shall not be dependent on the existence of a contractual relationship between the payment initiation services providers and the account servicing payment services providers for that purpose".* This provision on a dedicated interface would be a major obstacle to interoperability.

There is also a broader issue related to a common Application Programming Interface (API) as currently discussed in several countries and in particular the UK. EBA must make sure that the limited network as described by this Regulation will be compatible with a much broader network accessible to consumers.

END

BEUC The European Consumer Organisation

This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2014-2020).