

The Consumer Voice in Europe

STRONG CUSTOMER AUTHENTICATION FOR PAYMENTS

BEUC suggested changes to EBA's draft RTS mandated by PSD2



Contact: Farid Aliyev – farid.aliyev@beuc.eu

Jean Allix – jean.allix@ext.beuc.eu



Introduction

As part of the revised Payment Services Directive (PSD2), the European Banking Authority (EBA) was tasked to come up with new rules on security for electronic payments. On February 23, the EBA published its [draft regulatory technical standards](#) (RTS) on security of payments, as mandated by PSD2.

The RTS is divided into two parts, one on strong customer authentication and the other on open standards for communication between banks and third-party service providers (TPPs). See below BEUC comments which only focus on strong customer authentication (chapter 3).

Overall, BEUC is dissatisfied with the EBA's proposal, as it undermines the high level principles set out in PSD2. We call on the European Commission, the Parliament and the Council to take BEUC proposals into account in order to align the RTS with PSD2 provisions and offer a high level of payment security to EU consumers.

BEUC comments

A good clarification made by EBA

Point 15: *"The liability rules as described in Art 74(2) PSD2 apply before, during and after the transitional period"*. For BEUC, this is an important point as we have criticised the restrictive interpretation by EBA in the previous version of the draft Regulatory Technical Standards (RTS).

Chapter 3. Exemptions from strong customer authentication

This chapter includes Articles 10 to 18.

General comment on the exemptions from strong customer authentication (SCA)

Based on EBA's proposal, it is impossible to know what volume of online payment transactions would fall under the derogations. What is the percentage of transactions of less than EUR 30? What is the percentage of transactions that fall outside the SCA because of Art 16 of the draft RTS?

On reading these derogations, the EBA proposal does not seem technologically neutral. It favours cards at the expense of credit transfers.

Specific comments on the draft RTS

Art 11: contactless payments at point of sale

This article is divided into 2 parts. First, it says that SCA is not necessary for contactless payments under EUR 50. It then provides the ceiling (cumulative EUR 150 or 5 consecutive transactions) beyond which the SCA will be applied.

Regarding the amount of individual transactions, EUR 50 is a high figure. In the EU, the average value of card transactions is EUR 48.8. At present, the thresholds are set in different countries at lower levels (EUR 25-30). This figure of EUR 50 is too high when looking at the risks for consumers. A thief stealing a card can, in a few minutes, make 3 purchases of EUR 50 without a PIN check. If this card were not a contactless card, the thief would not have been able to make the transactions.

BEUC demand: Lower the threshold for no-PIN contactless card transactions to EUR 30 for individual transactions, combined with a cumulative amount of EUR 100.

Art 12. Transport and parking fares

For unattended terminals, there is a general exemption to SCA. In the initial version of the draft RTS, there was no specific provision for this situation (general rules on contactless). But this new provision can be dangerous. If a card is stolen, it can be used for transport tickets and parking payments repeatedly in a short period of time. Of course, the consumer will be reimbursed after the notification of the loss but if he does not pay attention to such relatively low-value fraudulent payments, he will have to pay for all the transactions.

BEUC demand: Art 12 can be maintained if this category of transactions is clearly included in the monitoring mechanism established by Art 2.

Art 13. Trusted beneficiaries and recurring transactions

This article creates two exemptions:

The first one is about a consumer who has a list of trusted beneficiaries previously created. It could be for example the list of beneficiaries (e.g. electricity or telecom company, insurance provider) that the consumer has on his online banking account. If previous payments to this beneficiary have worked correctly, SCA is not needed. This exemption does not work when a new beneficiary is introduced for the first time in the list. This exemption is logical. The EBA should have applied the same reasoning to the other provisions, in particular regarding remote card payments.

The second exemption in this article is about a series of payment transactions with the same amount and the same payee. It should cover permanent orders.

BEUC demand: BEUC agrees with Art 13 but demands that the same reasoning is applied to Art 15 e.g. regarding remote payments.

Art 14. Same payer and payee

Credit transfers between two accounts owned by the same user in the same bank do not require SCA. We agree with the proposal.

Art 15. Low value transactions

This article introduces a general derogation for all internet payments of an amount less than EUR 30, i.e. no strong customer authentication for online card payments below EUR 30. This amount was EUR 10 in the previous version of the draft RTS.

As already explained by BEUC on various occasions, this provision is illogical. BEUC proposes that the SCA apply to the first transactions with a specific new beneficiary. If the first transaction with SCA went smoothly, a new transaction with the same beneficiary can be done without SCA

BEUC demand: Strong authentication should always be used for the first transaction with a new beneficiary. The security rules applying to different means of payment must be coherent: the logic applied to credit transfers (see Art 13) should also be applied to online card payments. After the first transaction with SCA, risk based assessment is possible if the beneficiary is the same.

Art 16. Transaction risk analysis

This article is the great novelty of the final draft version of the RTS. It introduces the possibility for the ASPSP (consumer's bank) not to ask SCA if the level of payment fraud at this ASPSP is lower than the levels indicated in the RTS.

The applicability of the system proposed by EBA raises many questions:

- Maximum fraud levels authorised without SCA are given by categories (credit transfers and cards) and by transaction amounts (EUR 100/250/500). Where do these numbers come from? Their origin is not explained in the EBA draft. Legislation sets figures, but there is no information on whether they are lower or higher than the real fraud rates.
- What percentage of transactions per bank will be excluded from the SCA? No information is available on this subject. If more than 50% transactions are exempted, the whole directive is emptied of its substance.
- These figures are different for credit transfers and cards. The rate of fraud allowed is 5 to 10 times higher for cards than for credit transfers. What is the logic of this choice? This provision gives an unjustified advantage to card payments.

If two consumers who are clients of different banks make an identical transaction of the same amount, it could be that for one the merchant requests the SCA because the bank of this consumer is above the fraud thresholds. For the second consumer, the merchant will not ask for the SCA because the consumer's bank is below the thresholds. So, for two identical transactions, different rules would be applied.

We question whether the EBA proposal complies with the criteria established by the PSD2 for derogations (Art 98.3). When two transactions are identical and the exclusion applies to only one, the Art 98.3 criteria are not applied since the level of risk is the same.

BEUC demand: BEUC considers that Art 16 should be simply deleted, as a pure circumvention of PSD2.



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

The content of this publication represents the views of the author only and it is his/her sole responsibility; it cannot be considered to reflect the views of the European Commission and/or the Consumers, Health, Agriculture and Food Executive Agency or any other body of the European Union. The European Commission and the Agency do not accept any responsibility for use that may be made of the information it contains.

BEUC would like to thank the European Environment and Health Initiative (EEHI) for providing funding for the development of this publication.