BEUC The European Consumer Organisation

The Consumer Voice in Europe

Mr. Andrea Enria
Chairperson
European Bank Authority – EBA
One Canada Square (Floor 46)
Canary Wharf
UK - London E14 5AA

Ref.: BEUC-X-2017-012/MGO/cm

14 February 2017

Re: **Security of payments under the revised Payment Services Directive**

Dear Mr. Enria,

We would like to share our concerns related to the pending Regulatory Technical Standards on strong customer authentication, which was mandated to EBA by the revised Payment Services Directive (PSD2). According to media reports and discussions with various stakeholders, the principles in PSD2 are at risk of being watered down by the draft technical standards due to be published by EBA in the coming days.

BEUC's key demands:

- **Remote card payments below EUR 30 should not be automatically exempted from strong authentication;**
- **Payment service providers should not be able to exempt themselves from strong authentication based on self-assessment of fraud levels.**

One of the overarching goals of PSD2 is to improve the security of electronic payments, and more particularly remote payments where fraud is on the rise. In the Eurozone the value of all fraudulent transactions using cards online amounted to EUR 1.44 billion in 2013, which represented an increase of 8% from 2012. In 2015, 71% of card fraud cases in the EU related to internet payments.

Recital 95 of PSD2 provides that *"Security of electronic payments is fundamental for ensuring the protection of users and the development of a sound environment for e-commerce. All payment services offered electronically should be carried out in a secure manner, adopting technologies able to guarantee the safe authentication of the user and to reduce, to the maximum extent possible, the risk of fraud."*

In order to achieve that goal, Member States will, inter alia, have to *ensure that payment service providers apply strong customer authentication where the payer accesses its payment account online, initiates an electronic payment transaction, or carries out any action through a remote channel which may imply a risk of payment fraud or other abuses* (Article 97.1). This provision implies that when making e.g. an online card payment or using online banking, the consumer should confirm the transaction using his PIN code, fingerprint, voice recognition tools, etc.

…/…

Bureau Européen des Unions de Consommateurs AISBL | Der Europäische Verbraucherverband
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • Fax +32 (0)2 740 28 02 •
consumers@beuc.eu • www.beuc.eu • www.twitter.com/beuc
TVA: BE 0422 071 051 • EC register for interest representatives: identification number 9505781573-45

The directive allows for some *exemptions from the strong authentication rule based on the level of risk involved in the service provided; the amount, the recurrence of the transaction, or both; the payment channel used for the execution of the transaction* (Article 98.3).

The high-level principles of the PSD2 are very clear: strong customer authentication is the rule, while some clearly specified exemptions are possible. However, according to media reports[1] and discussions with various stakeholders, it appears that the exemptions are turning into the rule.

First, it is unclear as to why online transactions below EUR 30 should be fully exempted from strong authentication? Does this exemption imply that the risk of fraud with transactions below EUR 30 is very low? BEUC believes such an exemption would violate the PSD2 requirement to take into account 'the level of risk involved' when considering exemptions from strong authentication. BEUC is not opposed to a risk-based assessment, provided that certain conditions are met, e.g. first remote card payment that a consumer is making with a specific online merchant should use strong authentication. Then, similar recurring transactions with the same merchant, from the same IP, device, location, delivery address could be exempted from strong authentication.[2]

Second, it seems that with regard to remote transactions above EUR 30, the application of strong authentication would be conditional on the authorised fraud thresholds. Only the PSPs that cannot keep the fraud level below a cap would have to apply strong authentication. This criteria is not in the list of the possible reasons for exemption as stated by article 98.3. In addition, a major problem is that the fraud statistics would be reported by the payment services providers, i.e. this would be a form of self-assessment by the industry. It is highly unlikely that the authorities in charge of PSD2 (European Commission, EBA, central banks) would have the resources to check the reliability of the data reported by PSPs. Therefore, we call on policy-makers to design clear rules which consumers can understand and which are relatively easy to enforce.

We hope that BEUC's concerns will be taken seriously by policy-makers. We stand ready to discuss this important file in more detail. Consumers deserve better security in electronic payments.

With best wishes,

Monique Goyens
Director General

N.B: This letter has been sent to the European Commission, the European Parliament, the European Central Bank and the Council.

[1] http://www.lesechos.fr/finance-marches/banque-assurances/0211789352218-securite-des-paiements-a-distance-leurope-cherche-le-bon-equilibre-2063854.php
http://www.sueddeutsche.de/wirtschaft/online-shopping-eu-bankenaufsicht-blockiert-strengere-regeln-bei-online-zahlungen-1.3372934

[2] BEUC's detailed position is explained in a blog published in January 2017: http://www.beuc.eu/blog/consumers-deserve-better-security-in-electronic-payments/