

The Consumer Voice in Europe

## BEUC RESPONSE TO EUROPEAN BANKING AUTHORITY DISCUSSION PAPER

on future draft Regulatory Technical Standards on strong  
customer authentication and secure communication under the  
revised Payment Services Directive



**Contact:** Farid Aliyev – [Financialservices@beuc.eu](mailto: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](http://www.twitter.com/beuc) • [consumers@beuc.eu](mailto:consumers@beuc.eu) • [www.beuc.eu](http://www.beuc.eu)  
EC register for interest representatives: identification number 9505781573-45



Co-funded by the European Union

Ref: BEUC-X-2016-012 - 05/02/2016

## Summary


---

Security of payments is very important for consumers and payment service providers alike. We welcome the European Banking Authority (EBA) [discussion paper](#) on strong authentication and secure communication in payments. The way EBA's upcoming technical standards are set is very important for the consumer protection that the Payment Service Directive 2 (PSD2) aims to provide.

Security provisions are developed by providers. Consumers usually take security for granted and assume security measures are sufficient until an incident occurs. PSD2 provides individual consumers with protection from the resulting financial damage. Yet, *in fine*, all consumers bear the burden of damages through the overall costs of payments services and final prices of goods and services. Therefore, consumers and providers share an interest in putting in place state-of-the-art protection to prevent as many incidents and damages as possible.

Preventive measures are needed for all payment transactions and channels. Any exemptions from strong authentication rules must be clearly substantiated. We also acknowledge the importance of convenience, and the difficult trade-off between convenience and security checks, which must not be too cumbersome for consumers.

Finally, an adequate combination of preventive and curative measures can create a high level of protection for consumers. It would be dangerous to assume that any given payment method or channel is one hundred percent safe. Consumers should be able to receive quick and hassle-free refund in case of unauthorised transactions.



**Consumers and providers share an interest in putting in place state-of-the-art protection to prevent as many incidents and damages as possible.**

## 1. Considerations prior to developing the requirements on strong customer authentication

### Questions:

1. With respect to Article 97(1) (c), are there any additional examples of transactions or actions implying a risk of payment fraud or other abuses that would need to be considered for the RTS? If so, please give details and explain the risks involved.
2. Which examples of possession elements do you consider as appropriate to be used in the context of strong customer authentication, must these have a physical form or can they be data? If so, can you provide details on how it can be ensured that these data can only be controlled by the PSU?
3. Do you consider that in the context of "inherence" elements, behaviour-based characteristics are appropriate to be used in the context of strong customer authentication? If so, can you specify under which conditions?
4. Which challenges do you identify for fulfilling the objectives of strong customer authentication with respect to the independence of the authentication elements used (e.g. for mobile devices)?
5. Which challenges do you identify for fulfilling the objectives of strong customer authentication with respect to dynamic linking?
6. In your view, which solutions for mobile devices fulfil both the objective of independence and dynamic linking already today?

### BEUC comments

**Question 1:** In our view, there should be strong customer authentication requirements for mail orders and telephone orders. These transactions use remote channels, and, a priori, imply the same risk of payment fraud as other remote transactions, including electronic ones<sup>1</sup>. Therefore we do not see any valid reason for exempting mail and telephone orders from the scope of the Regulatory Technical Standards. Specific types of strong customer authentication could be considered for non-electronic remote transactions.

**Question 2:** BEUC considers that, physical objects such as chip cards and smartphones are appropriate to be used in the context of strong customer authentication. For example, there are already solutions on the market that allow using the smartphone as a token for multi-factor authentication. Such solutions are especially well adapted for mobile payment transactions, as the user does not have to carry an additional hardware token around while, at the same time, strong authentication requirements can be met. On the other hand, this raises the issue of security of the hardware and software i.e. currently no common EU level standards exist for mobile payments. Recent recommendations on 'Mobile and card-based contactless payments' issued by the Euro Retail Payments Board, if properly implemented, should contribute to remedy this issue.<sup>2</sup>

<sup>1</sup> <http://www.financialfraudaction.org.uk/Retailer-internet-mail-phone-advice.asp>

<sup>2</sup> [https://www.ecb.europa.eu/paym/retpaym/shared/pdf/4th-ERPB-meeting/2015-11-26\\_4th-ERPB\\_item\\_6\\_ERPB\\_CTLP\\_working\\_group\\_final\\_report.pdf?726f67769d37722de341702fe5f2387a](https://www.ecb.europa.eu/paym/retpaym/shared/pdf/4th-ERPB-meeting/2015-11-26_4th-ERPB_item_6_ERPB_CTLP_working_group_final_report.pdf?726f67769d37722de341702fe5f2387a)

Another element to take into account is the need to ensure that these new technologies fully comply with the European data protection standards, recently reviewed in the context of the General Data Protection Regulation. Connected devices must integrate the principle of privacy at an early production stage to prevent that sensitive data such as financial data is misused.

**Question 3:** Behaviour-based strong customer authentication is already being performed by payment service providers such as card schemes<sup>3</sup>. Those techniques may be efficient to detect irregular transactions and prevent the risk of fraud, for example, where the transaction is initiated from an unusual place, country or IP. On the other hand, users are sometimes unfairly penalised due to automated behaviour-based techniques.

For example, many consumers complain that their credit card gets blocked by the issuer when making payments outside the EU, sometimes without any prior notice. Getting the card unblocked is usually a huge inconvenience and has a cost for the consumer, not to mention the fact that the consumer may run out of money and his holiday or business trip may be put at risk.<sup>4</sup> It can lead to major consumer detriment. Therefore, behaviour-based characteristics could be used as a complementary tool in the context of strong authentication and should in any case involve human intervention on behalf of the payment service provider. Whenever the PSP considers blocking a payment instrument upon suspicion of a fraudulent transaction:

- The PSP should immediately contact the consumer to check whether the transaction had been authorised or not;
- The responsibility on reaching the customer should lie on PSPs and there should be penalties if they do not;
- The procedure for unblocking the payment instrument should be available 24/7 and easy to reach from anywhere around the world;
- The procedure for unblocking the payment instrument should be based on advanced identification and security check, which should be easy to fulfil on the one hand from abroad but enough to ensure authenticity on the other.

**Question 4:** As regards remote card payments, currently strong authentication using 3-D Secure varies across banks and countries: in some cases the one-time security code is generated by a card reader provided by the bank, while in some other cases the security code is texted to the consumer's mobile phone number. This lack of harmonisation provides consumers with an inconsistent experience. Besides that, BEUC members raised the issue of risks related to sending the security code via SMS, which is not perceived as a secure communication channel.

In the context of authentication services it is also essential that consumers' data is secure and that in case of data breaches, there are effective redress mechanisms in place in compliance with the new data protection rules.

**Question 5:** There are possibly some scenarios in which a requirement for dynamic linking for the initiation of a transaction might be difficult to implement for various reasons. We agree that exemptions for such cases could be considered.

Referring specifically to recurring direct debits, in our view, strong authentication with dynamic linking is possible. For example, according to the e-mandate solution developed by the European Payments Council, the consumer has to log into his online banking account (using his personal security credentials and strong authentication with dynamic

---

<sup>3</sup> <https://www.visaeurope.com/media/images/sca%20position%20paper-73-31002.pdf>

<sup>4</sup> <https://communaute.indirect.fr/t5/Moyens-de-Paiement/carte-bloqu%C3%A9e-%C3%A0-l-%C3%A9tranger/td-p/13247>

linking) and then approves that the direct debit mandate was issued by a specific third party payee.<sup>5</sup>

## 2. The exemptions to the application of strong customer authentication

### Questions:

7. Do you consider the clarifications suggested regarding the potential exemptions to strong customer authentication, to be useful?
8. Are there any other factors the EBA should consider when deciding on the exemptions applicable to the forthcoming regulatory technical standards?
9. 9. Are there any other criteria or circumstances which the EBA should consider with respect to transaction risks analysis as a complement or alternative to the criteria identified in paragraph 45?

### BEUC comments

**Question 7:** The clarifications suggested by EBA regarding the potential exemptions to strong customer authentication are useful. The PSD2 aims to make sure that all electronic payment services are carried out in a secure manner. For face-to-face payments (by card), Europe adopted the Chip and PIN standard a few years ago, which considerably reduced the levels of fraud in those transactions.<sup>6</sup>

**Mobile commerce is a prime target of payment fraud, with 21% of fraud attributed to mobile transactions.**

Since then fraudsters have mostly moved to the remote space which is by definition less secure, as the payer and payee do not see each other. For example, when making an online credit card payment, the cardholder enters his card number,

expiration date and security number on the back of the card (CVV number). Fraudulent transactions using stolen cards, skimming and phishing techniques are therefore possible where security checks (strong authentication) are not performed by merchants and PSPs.

According to a recent study, mobile commerce is a prime target of payment fraud: while mobile payments account for only 14% of m-commerce merchants' transactions, this segment of merchants attributes 21% of fraud to mobile transactions.<sup>7</sup>

We consider that preventive measures are very important for all payment transactions and any possible exemptions must be duly substantiated. We also acknowledge the importance of convenience, e.g. consumers are usually not required to type their PIN code for low value face-to-face contactless payments.

**Question 8:** A good level of protection for consumers of payment services is provided through an adequate combination of preventive and curative measures. Providing a hassle-free and unconditional refund in case of unauthorised, fraudulent and disputed payment transactions is a precondition necessary to help reassure consumers in retail

<sup>5</sup> [http://www.europeanpaymentscouncil.eu/pdf/EPC\\_Article\\_17.pdf](http://www.europeanpaymentscouncil.eu/pdf/EPC_Article_17.pdf)

<sup>6</sup> <http://www.smartcardalliance.org/publications-emv-faq/>

<sup>7</sup> True cost of fraud mCommerce, LexisNexis, January 2015:  
<http://lexisnexis.com/risk/downloads/whitepaper/true-cost-fraud-mobile-2014.pdf>

payments and contribute to innovation, convenience, and smooth payment experience. EBA should consider this crucial aspect when drafting the Regulatory Technical Standards.

**Providing a hassle-free and unconditional refund in case of unauthorised, fraudulent and disputed payment transactions is a precondition necessary to help reassure consumers in retail payments.**

The PSD2 aims to better protect consumers against fraudulent transactions where the consumer has not acted fraudulently or has not committed gross negligence<sup>8</sup>. Yet in reality consumers often face difficulties in obtaining quick redress, as some PSPs tend to shift the liability to the consumer.

For example, a French bank that repeatedly rejected consumers' refund claims for fraudulent transactions was recently ordered by a court to fully refund their money<sup>9</sup>. In Germany, a *prima facie* approach ('Anscheinsbeweis' in German) has been used by courts to merely assume gross negligence behaviour even if no proof of such behaviour has been provided<sup>10</sup>.

**Question 9:** Paragraph 45 refers to behaviour-based risk analyses, which is not always reliable in practice and can cause detriment to the consumer. See our response to Q3.

### 3. The protection of the payment service users' personalised security credentials

#### Questions:

10. Do you consider the clarification suggested regarding the protection of users personalised security credentials to be useful?
11. What other risks with regard to the protection of users' personalised security credentials do you identify?
12. Have you identified innovative solutions for the enrolment process that the EBA should consider which guarantee the confidentiality, integrity and secure transmission (e.g. physical or electronic delivery) of the users' personalised security credentials?
13. Can you identify alternatives to certification or evaluation by third parties of technical components or devices hosting payment solutions, to ensure that communication channels and technical components hosting, providing access to or transmitting the personalised security credential are sufficiently resistant to tampering and unauthorized access?
14. Can you indicate the segment of the payment chain in which risks to the confidentiality, integrity of users' personalised security credentials are most likely to occur at present and in the foreseeable future?

<sup>8</sup> The consumer's liability will be limited to EUR 50 compared to EUR 150 currently.

<sup>9</sup> Fraude à la carte bancaire: Le Crédit mutuel condamné, 22 Mai 2015 : <http://www.quechoisir.org/argent-assurance/banque-credit/service-bancaire/actualite-fraude-a-la-carte-bancaire-le-credit-mutuel-condamne>

<sup>10</sup> Though Art 59 of PSD1 and Art. 72 of PSD2 discourage the mere assumption of proof, the Bundesgerichtshof, Germany's highest court of Justice in Civil Law cases, still found in 2011 that gross negligence may further be assumed in a case of loss and misappropriation of a payment card with an ATM if the use of the original payment card had been recorded. (Urteil vom 29.11.2011 - XI ZR 370/10) Only last month though this court set a new decision on the abuse of PIN and TAN with online banking stating that the recording of the use of those credentials was not enough to assume liability of the account holder (BGH Urteil vom. 26.01.2016 – Az. XI ZR 91/14).

## BEUC comments

**Question 10:** The clarifications suggested by EBA regarding the protection of users' personal security credentials are useful.

**Question 11:** BEUC welcomes the fact that the previously unregulated third-party payment initiation service and account information service providers (PIS and AIS) have been brought under the scope of the PSD2. PIS will have to comply with a number of requirements as regards their registration and licensing, strong customer authentication, authentication vis-à-vis the consumer's bank, and liability in case of payment incidents. The liability requirements related to PIS under the PSD2 are very consumer friendly: in case of an unauthorised transaction, the consumer will be entitled to get the refund from his bank; the ultimate liability for the fraudulent transaction will be addressed between the consumer's bank and the PIS.

A major security concern relates to the operating model where PIS come into possession of the consumer's personalised security credentials to access his bank account. This threatens consumer security and privacy and by far exceeds the objective, which is to receive payment authorisation and payment guarantee for a specific payment transaction. In some countries, like Denmark, consumers use single sets of personalised security credentials (digital signature) for accessing various services online, e.g. doing online banking or viewing their tax file<sup>11</sup>. BEUC considers that the consumer's personalised security credentials should not be accessed by any third party, including PIS/AIS.

In spring 2014, the European Commission organised two technical workshops on access to payment accounts by third-party payment service providers. The workshops brought together the representatives of banks, PIS, EBA, the European Commission, the European Central Bank, and consumers (BEUC). The participants discussed different possible payment account access models by PIS. Most importantly there was a unanimous agreement on the need for the consumer not to share his reusable personal credentials but sharing one-time dynamic transaction codes would be acceptable.<sup>12</sup> We invite EBA to take those conclusions into account when drafting the Regulatory Technical Standards.

**Questions 12, 13 and 14** are for product developers.

---

<sup>11</sup> <https://www.nemid.nu/dk-en/>

<sup>12</sup> See conclusions of the 2<sup>nd</sup> technical workshop on access to payment accounts by third-party payment service providers, Brussels, 29 April 2014

#### 4. Considerations prior to developing the requirements on common and secure open standards of communication

##### Questions:

15. For each of the topics identified under paragraph 63 above (a to f), do you consider the clarifications provided to be comprehensive and suitable? If not, why not?
16. For each agreed clarification suggested above on which you agree, what should they contain in your view in order to achieve an appropriate balance between harmonisation, innovation while preventing too divergent practical implementations by ASPSPs of the future requirements?
17. In your opinion, is there any standards (existing or in development) outlining aspects that could be common and open, which would be especially suitable for the purpose of ensuring secure communications as well as for the appropriate identification of PSPs taking into consideration the privacy dimension?
18. How would these requirement for common and open standards need to be designed and maintained to ensure that these are able to securely integrate other innovative business models than the one explicitly mentioned under article 66 and 67 (e.g. issuing of own credentials by the AIS/PIS)?

#### BEUC comments

**Question 15:** BEUC supports the approach proposed by EBA with respect to common and secure open standards of communication between account servicing payment service providers (banks), AIS and PIS providers, payers, payees and other service providers. See also our response to Q11.

In addition, we would not be in favour of PIS/AIS developing new sets of personalised security credentials, identification and authorisation procedures. That would add more confusion for consumers.

**Questions 16, 17 and 18** are for product developers.

#### 5. Possible synergies with the regulation on electronic identification and trust services for electronic transactions in the internal market (e-IDAS)

##### Questions:

19. Do you agree that the e-IDAS regulation could be considered as a possible solution for facilitating the strong customer authentication, protecting the confidentiality and the integrity of the payment service users' personalised security credentials as well as for common and secure open standards of communication for the purpose of identification, authentication, notification, and information? If yes, please explain how. If no, please explain why.
20. Do you think in particular that the use of "qualified trust services" under e-IDAS regulation could address the risks related to the confidentiality, integrity and availability of PSCs between AIS, PIS providers and ASPSPs? If yes, please identify which services and explain how. If no, please explain why.



## BEUC comments

**Question 19:** We agree that the e-IDAS regulation could be considered as a possible solution for facilitating strong customer authentication, protecting the confidentiality and the integrity of the payment service users' personalised security credentials as well as for common and secure open standards of communication for the purpose of identification, authentication, notification, and information. As the European Commission puts it, rolling out e-IDAS means higher security and more convenience for any online activity such as remotely opening a bank account or authenticating for internet payments.<sup>13</sup>

For example, the ERPB report on 'The pan-European use of electronic mandates for SEPA direct debit' already explored the possibility of using qualified electronic signatures as an EU-wide and interoperable means of electronically signing mandates. The report refers to best practices in some Nordic and Baltic Member States.<sup>14</sup>

**Question 20:** Qualified trust services may well be a solution to the issue of confidentiality, integrity and availability of personal security credentials between AIS, PIS and banks (see our response to Q19). These services must be subject to strict oversight by relevant supervisory authorities.

END

---

<sup>13</sup> <http://ec.europa.eu/digital-agenda/en/trust-services-and-eid>

<sup>14</sup> ERPB report on "The pan-European use of electronic mandates for SEPA direct debits – Issues and the way forward", 7 November 2014:  
[https://www.ecb.europa.eu/paym/retpaym/shared/pdf/2nd\\_eprb\\_meeting\\_item4.pdf?27ef4897696839d1e7d0918f6b2dae48](https://www.ecb.europa.eu/paym/retpaym/shared/pdf/2nd_eprb_meeting_item4.pdf?27ef4897696839d1e7d0918f6b2dae48)



*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.*