EPC285-14
Version 1.1
14 November 2014
EPC

EPC Response to the EBA Consultation Paper on the Implementation of EBA Draft Guidelines on the Security of Internet Payments

Circulation to: **EBA**
Restricted: **No**

1. Details Submitter:

Organisation: **European Payments Council**

Contact: **Christophe.godefroi@epc-cep.eu**

2. Consultation Question

Question: Do you prefer for the EBA Guidelines
a) to enter into force, as consulted, on 1 August 2015 with the substance set out in this consultation paper, which means they would apply during a transitional period until stronger requirements enter into force at a later date under PSD 2 (i.e. a two-step approach); or

b) to anticipate these stronger PSD2 requirements and include them in the final Guidelines under PSD 1 that enter into force on 1 August 2015, the substance of which would then continue to apply under PSD 2 (i.e. a one-step approach).

Answer (a or b including justification):

The EPC recommends a scenario whereby the EBA Guidelines would be issued only after entry into force of PSD2 (according to Article 103 of the draft PSD2) and publication of the regulatory technical standards as may be mandated of EBA in accordance with PSD2, following a consultation of the market and safeguarding an adequate timeframe for implementation ('option c').

The preference for the aforementioned 'option c', is based on the following arguments:

- The legal enforceability of options a) & b) is uncertain. Indeed, according to Article 16 of Regulation 1093/2010 EBA shall in order to ensure common, uniform and consistent application of Union law issue Guidelines and recommendations. Article 1.2 of the same Regulation lists the EU legal texts (e.g. PSD) forming the scope within which EBA shall exercise its powers. EBA in its consultation paper refers to the current PSD as a legal basis while seeking to 'ensure common, uniform and consistent application of Union law'. However, the consultation paper is about implementation of draft Guidelines on the security of internet payments - prior to the transposition of the revised Payments Services Directive (PSD2). An essential element for the draft EBA Guidelines is the reliance on the concept of strong customer authentication. It is important to note that this concept does not yet exist under the current PSD and will only be incorporated in 'Union law' once PSD2 (new Article 87 PSD2) enters into force. Based on current Union law PSPs are not yet (legally) required to apply 'strong customer authentication'. As a result, the EBA Guidelines – as currently drafted - would appear unenforceable until PSD2 enters into force.

- Shortcomings related to option a) include:
  - The 2-step approach creates a risk of implementations in the first step not being compliant with future Guidelines related to the second step, imposing unnecessary rework costs to payment service providers and other technical providers, and confusion/inconvenience to merchants and consumers.
  - The security Guidelines would not be enforced on all payment service providers as payment initiation services providers will only be regulated under PSD2 at a later stage.

- Shortcomings related to option b) include:
  - It does not provide a guarantee of a one-step approach, because the stronger PSD2 requirements are at this time still under discussion and may change until the publication date which is likely going to be too close to 1 August 2015. We therefore believe that there are no stable conditions for setting requirements for stronger security standards which will ultimately exist under PSD2.

- At present PSPs are working to develop and implement technical structures as requested by SecuRe Pay Recommendations by the February 2015 deadline, and it would at this late stage be impossible for them to change the scope of their projects (and related budgets) already planned in accordance with the SecuRe Pay Recommendations.
- A lead time - well beyond 1st August 2015 – would be required to implement “strong transaction authentication” solutions or, more generally, any solution other than those already set out in the SecuRe Pay Recommendations.
- The security Guidelines would not be enforced on all payment service providers as payment initiation services providers will only be regulated under PSD2 at a later stage.

If the EBA were not to accept the recommended ‘option c’, the EPC would have a preference for option a) (i.e. the 2 steps approach) subject to the EBA Guidelines remaining based on the SecuRe Pay Recommendations published in 2013 which was the basis for the ongoing implementation efforts. However, the EPC’s concerns regarding the legal enforceability of strong customer authentication and the uncertainty around the final stipulation of PSD2 in this regard remain.

3. Additional Comments

N°	Issue	Comment	Reasoning
1	General	Clarification	How do the EBA Guidelines relate to the SecuRe Pay assessment guide for the security on internet payments, which was published by the ECB in February 2014? Would it not be appropriate to merge both into one single document or at least to have the assessment guide referenced in the Guidelines? Should the more detailed guidance provided in the ECB assessment guide also be taken into consideration by PSPs?
2	General	Amendment	The regrouping of the best practices into an annex does not improve the reading. Also, the fact that the Guidelines are not numbered is not very user friendly. The lay-out of the original SecuRe Pay document is preferred.
3	General	Amendment	In the last two decades many security solutions were implemented, only to have been rendered obsolete as technology evolves and be replaced by safer solutions. Stakeholders are permanently in search of solutions that master the subtle balance between security and user convenience. In the last five years,

			new threats have appeared, authentication solutions have evolved, and the preferred platform for internet payments has changed from PCs to mobile devices. This field of expertise is highly dynamic. As an example since the issuance of the SecurePay Recommendations, tokenization has been picked up as one of the prevalent security solutions in any future e-payments system (understandably, at the time of publication, the Recommendations did not take tokenization into much consideration). Another very promising area of evolution in digital security is risk based authentication, and innovation in this area can be seriously hindered by the current requirements. We therefore suggest that these new developments be taken into account when finalising the Guidelines. Finally, the effectiveness of the requirements on card payments restricted to the European markets will not be effective in reducing fraud rates: they will only push fraud to regions that do not enforce the same security standards. Regardless of the level of authentication used by the cardholder when paying, the attackers will use the card numbers of European citizens at e- merchants that do not require strong authentication. This effect is clearly demonstrated by the EMV adoption in Europe, where fraud with European cards simply migrated to non-EMV markets. We therefore suggest a global effort through coordination with non-European authorities and central banks.
4	Background (p.6) Paragraph with reference to 1 February 2015 deadline	Amendment	“Competent authorities and financial institutions that are already on track with implementing the SecuRe Pay recommendations to the original date of 1 February 2015 are not affected by the extension and should continue with their plans.” The above would create a non-level playing field as PSPs would be subject to different deadlines depending on the jurisdiction where they are established.
5	Background (p.8) and Title I – Scope and definitions (p.14)	Amendment	The PSD2 discussions have shown the importance of having accurate definitions. As such with the publication of these Guidelines, the opportunity should be taken to improve some terms. Moreover on page 8 the new term “strong transaction authorisation” has been introduced (which does not appear at all in the current version of PSD2) and which refers to including a specific amount and payee into the authentication data, which is in fact “transaction data authentication”. Therefore a “clean” approach with different definitions for the below terms would be required: • Customer authentication

			• Transaction (data) authentication • Transaction authorisation by the payer Also, a distinction should be made between customer and transaction credentials (page 14: definition credentials). Furthermore, the definitions used in the EBA Guidelines should be consistent with the definitions in PSD2.
6	7.3	Clarification	The following statement is unclear: “[cards] For card transactions, all card issuing PSPs should support strong authentication of the cardholder. All cards issued must be technically ready (registered) to be used with strong authentication”. Should we interpret this that cards need to be technically ready but that strong authentication of the cardholders is not required? Furthermore, the word “registered” should be deleted in the following sentence: “All cards issued must be technically ready ~~(registered)~~ to be used with strong authentication.” This due to the fact that the issuer should only have to register cards (e.g. for 3D Secure) if they can indeed be used for internet payments.
7	7.6	Clarification	There seems to be an inconsistency in item 7.6 as reference is made to ‘payment schemes’ whereas on page 7 it is stated that “References to payments schemes, their Governance Authorities (GAs), and the oversight thereof have not been incorporated in the draft EBA Guidelines, as payment schemes are not covered by PSD1”. The reference to the current PSD and the non-incorporation of the reference to ‘payment schemes’ on page 7 illustrates that there is a problem with the legal basis under the current PSD for concepts which do not exist under the current PSD.