Ref.:EBF_011402
Brussels, 14 November 2014

EUROPEAN BANKING FEDERATION[1] ANSWER TO EBA CONSULTATION PAPER ON THE IMPLEMENTATION OF ITS GUIDELINES ON THE SECURITY OF INTERNET PAYMENTS (EBA/CP/2014/31)

1. Consultation Question: Entry into force of the Guidelines:

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 PSD 2 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).

The EBF cannot support any of the 2 options presented by the EBA (options a. or b.)
The EBF presents a third option: a one-step approach **but with an entry into force at a date later than 1 August 2015** (in reality what can be considered as an option c).

We strongly oppose any attempt "to anticipate stronger PSD 2 requirements". Some parts of the PSD 2, especially for what concerns security, are still hotly debated within the Council and still need to be discussed in trilogue. It is impossible to "anticipate" or second-guess what will be the result of the debate.
Therefore, it is most probable that the definitive and final text of the PSD 2 will only be adopted in the best case shortly before 1 August 2015. PSPs will need at least 1 year to implement the Guidelines which will have to be implemented following stronger PSD2 requirements and which will therefore be new with respect to the SecuRe Pay recommendations.
There is a strong likelihood that in order to accommodate for the needs of some TPPs, PSD 2 will require PSPs to review and make further (possibly significant) technical changes to their online banking platforms and customer and payment systems interfaces. Any technical changes will require time to develop, test and implement.

The one-step approach can only be based on the definitive and final text of the PSD 2 as well as the EBA technical regulatory standards which will be established following a precise mandate of the PSD2. The implementation date of the Guidelines on the security of internet payments should take into account an appropriate time frame starting from the effective date of adoption of these texts.

Option c is the only feasible scenario which ensures legal certainty for all stakeholders.

[1] Launched in 1960, the European Banking Federation is the voice of the European banking sector from the European Union and European Free Trade Association countries. The EBF represents the interests of some 4,500 banks, large and small, wholesale and retail, local and cross-border financial institutions. Together, these banks account for over 80% of the total assets and deposits and some 80% of all bank loans in the EU alone.

If however the EBA did decide that the Guidelines were to enter into force on August 1, 2015, the EBF would prefer that it be under option a. (the 2 step approach). This two-step scenario (option a) is expected to enable better management and planning of the compliance effort and related investments vis-à-vis the one-step approach (option b).

Option a. however presents several shortcomings, namely:

- The 2 step approach creates a risk of implementations of the first step not being compliant with future guidelines of the second step, imposing unnecessary rework costs to payment service providers, and confusion/inconvenience to the consumers.
- The security guidelines should be enforceable to all payment service providers, including payment initiation services providers (which will only be regulated under PSD 2).

2. General Comments or questions:

2.1 Need for regular review of the Guidelines

In the last two decades many security solutions were implemented, only to have been rendered obsolete as technology evolves and to 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.

Since the first consultation on the security requirements for internet payments, new solutions have appeared in this highly dynamic field of digital security such as risk based authentication. The Guidelines will need to be reviewed regularly to avoid that innovation in this area is seriously hindered by the current requirements.

2.2 **Scope**: *Do these guidelines apply to Payment Initiation Service Providers and Account Information Service Providers in the meaning of the PSD 2 draft?*

We believe they should.
Point 9 of Title 1 talks about “Payment Integrators” which “should be contractually required to comply with the guidelines “;
Point 10 however says that:” CTs where a third-party accesses the customer’s payment account” are excluded from the scope of the guidelines.
Clarity is required regarding payment account access services.

2.3 Comparison between the draft EBA guidelines and the SecuRe Pay recommendations:

We regret that Recommendation 6.4 of the SecuRe Pay report, which requires “payment service providers (PSPs) to ensure that customers are provided with instructions explaining their responsibilities regarding the secure use of payment services, has been incorporated in the draft EBA guidelines only as a best practice”. This downgrade constitutes in our opinion a lowering of customer awareness and education measures which goes against the principle of better customer education and is not helpful for what concerns fraud mitigation.

3. Title II General Control and Security Environment

Guideline 2.1:

Customers should be responsible for the security and use of their own (internet) payment environment. In order to secure the whole value chain, the security measures proposed by the Guidelines should also apply to customers and e-merchants through proper legal and contractual arrangements.

Guideline 2.3:

Not only sensitive data (including credentials), but also all payment transaction related data should be secured in terms of its integrity and origin.

4. Strong Customer Authentication

Guideline 7.1:

Customers should only be allowed to enter their credentials and authentication codes by themselves in a secure environment as indicated and approved by the issuing PSP.
With respect to authentication, protection against for example a "Man in the Middle" attack should also be effective. Here it is impossible for the issuing PSP to distinguish between the actual fraudulent and (supposedly) non-fraudulent use of authentication codes not initiated by PSP customers and/or in the secure banking environment. PSPs are not able to inform their customers whether or not these services are genuine and trustworthy. Customers themselves are also not able to recognise the difference between genuine and fraudulent services.

Guideline 7.6:

This guideline is addressed to Payment Schemes.
Payment schemes are however excluded from the EBA guidelines according to the Comparison between the draft EBA guidelines and the SecuRe Pay recommendations.
Clarity is sought on this issue.

5. Transaction monitoring

Guideline 10.2:

This guideline is addressed to Card Payment Schemes.
Payment schemes are however excluded from the EBA guidelines according to the Comparison between the draft EBA guidelines and the SecuRe Pay recommendations.
Clarity is sought on this issue.

6. Customer awareness, education and communication

Guideline 12.4

How does the possible handing-over of customers' secret personal credentials to a third-party, as allowed by the draft PSD 2, fit with this guideline: "PSPs should initiate customer education and awareness programmes designed to ensure customers understand, at a minimum, the need to protect their passwords, security tokens, personal details and other confidential data".

More particularly, in the context of this consultation, it is difficult to reconcile the very differing requirements set by guideline 12.4 with what may be allowed under PSD 2. The consequence is likely to be very conflicting anti-fraud messages for users, leading to confusion and ultimately providing a loop-hole for criminals to exploit.

Clarification is sought here.

7. Best Practice 7.3: Strong customer authentication linked to a specific amount and payee

It is very important that this practice remains as such, a best practice, and does not become a mandatory rule. The draft PSD 2 appears to be going further by mandating this approach in Article 87(1a) by requiring PSPs to *"apply strong customer authentication that shall include elements dynamically linking the transaction to a specific amount and a specific payee"*. It should be left to PSPs to determine when and in what circumstances to apply such a mechanism. Mandating it as a 'one size fits all' approach via PSD 2 would, in our view, be too prescriptive, running the risk of the unintended consequence of stifling innovation.

8. Annex 1: Best Practice Examples

This annex should be adjusted to reflect what is stated in the Guidelines paper. There are some inconsistencies e.g. reference to "the report"; numbering not corresponding.

Contact: Patrick Poncelet: p.poncelet@ebf-fbe.eu and Séverine Anciberro: s.anciberro@ebf-fbe.eu