|  |  |
| --- | --- |
| 14/11/2014 |  |

**Consultation Paper on the Implementation of draft EBA Guidelines on the Security of Internet Payments prior to the Transposition of the Revised PSD2**

On 20 October 2014, the EBA published a [“Consultation Paper on the Implementation of draft EBA Guidelines on the Security of Internet Payments prior to the Transposition of the Revised PSD2”.](https://www.eba.europa.eu/-/eba-consults-on-implementation-of-guidelines-on-internet-payments-security) The EBA invites comments on all proposals put forward in this paper and in particular on the specific question detailed below. The consultation runs until **14 November 2014**.

The EBA invites comments on all proposals put forward in this paper and in particular on the specific question stated in the paper.

Comments are most helpful if they:

- respond to the question stated;

- indicate the specific point to which a comment relates;

- contain a clear rationale;

- provide evidence to support the views expressed/ rationale proposed; and

- describe any alternative regulatory choices the EBA should consider.

1. **Details Submitter:**

Your Name: Lars Rutberg

Your Organisation: Swedish Bankers’ Association

1. **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 Swedish Bankers’ Association (below “SBA”) cannot support any of the two options a) or b) in the consultation document.  SBA opposes any attempt to “anticipate stronger PSD 2 requirements” or guess what they could entail. Many parts of the PSD 2, *especially* for what concerns security, are still very much debated in the Council working group and discussionsin trilogue is anticipated. What may come out as result of the trilogue is anyone’s guess, especially since the positions of the Parliament and Council are very different  SBA prefers an option where the EBA Guidelines would be issued only *after* entry into force of the PSD2, following a consultation of the market and safeguarding an adequate timeframe for implementation (‘option c’). SBA cannot see a situation where the guidelines enter into force sooner than the PSD has been implemented and the corresponding EBA guidelines (under PSD2; i.e. articles 87 and 87 a)), as drafted in the last compromise from the Presidency, have been published. Or in other words, we cannot see that the guidelines can enter into force any sooner than *after* PSD2 *and* the EBA guidelines are finalized.  SBA also questions the legal grounds for EBA to issue guidelines incorporating demands for ‘strong customer authentication’ since this is a concept not known to the current PSD (PSD1), and it is only PSD1 which EBA can “use” as means for issuing guidelines based on EU-legislation.  The preference for ‘option c’, is based on the following arguments:   * 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 of the second step, imposing unnecessary rework costs to payment service 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 intense discussions and may change. There are currently no stable conditions for setting requirements for stronger security standards that 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. It is impossible at this late stage to demand that they 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. |

1. **Response Template**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **N°** | **Point** | **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? Moreover, how do they tie in with the second SecuRe Pay recommendation on access to bank accounts? See more below N° 3 on scope. |
| 2 | Page 7 | General | Clarification | On this page it is stated that recommendation 6.4 has been incorporated in the draft EBA guideline. However as point 6.2, which is somewhat confusing (see more below on the Annex). |
| 3 | Title I – Scope and definitions | General | Amendment/Clarification | Point 9 of Title 1 refers to “Payment Integrators” which “should be contractually required to comply with the guidelines. Point 10 however states “CTs where a third-party accesses the customer’s payment account” are excluded from the scope of the guidelines. For SBA it is unclear whether these guidelines in fact also coves payment access services and also the connection to the second recommendation from SecuRe Pay. |
| 4 | Title II – Draft guidelines on the security of internet payments | General | Amendment | Here it is referred to “this report”, which is wrong. Should be “these guidelines” rather than ‘report’, which refers back to the SecuRe Pay ‘report’. Same in page 19 as regards strong customer authentication. |
| 5 | Title II – Draft guidelines on the security of internet payments | 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 card holders 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. |
| 6 | Title II – Draft guidelines on the security of internet payments | 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. |
| 7 | Title II – Draft guidelines on the security of internet payments | 7.7 | Amendment | See point 6 above. In point 7.7 it is referred to “card payment *schemes*”. |
| 8 | Title II – Draft guidelines on the security of internet payments | 10.2 | Amendment | See point 6 above. In point 10.2 it is referred to “card payment *schemes*”. |
| 9 | Annex | General | Amendment | The Annex is unfortunately a total mess! Firstly here it refers to “the report” (which is a referral to the original SecuRe Pay “report”). What is more, it’s stated that “the numbering of the best practice ‘mirrors’ the numbering of the guidelines”. Which they don’t! Points 7.1, 7.2 and 7.3 are just a copy-and-paste from the SecuRe Pay report and has nothing to do with the guidelines. 11.1 should rather be 11.3 and there is only one paragraph in section 13 (13.1) why there cannot be a reference to 13.2 and 13.3! If anything, it should be 13.1. In short, please adjust the annex so it actually reflects what is stated as principles for it!  Moreover, it could be questioned whether the decision to move the Best practices to an Annex have improved the reading. |

|  |  |
| --- | --- |
| SWEDISH BANKERS' ASSOCIATION |  |
| Lars Rutberg |  |