**Czech banking association response to EBA Consultation Paper on Implementation of Guidelines on Security of Internet Payments**

*Considering credit transfers as mentioned in Title 1 Par. 6*

***Executive summary***

*The entry of force date of the draft guidelines will be 1 August 2015, which constitutes an extension by six months compared to the implementation date that had been set for the SecuRe Pay recommendations. The EBA is consulting in October/November 2014 and will be publishing the final guidelines including the feedback statement soon thereafter.*

**CBA comment 1:**

Concerning the complexity of Guidelines (change of authentication methods, monitoring of payments etc.) and their obligation (in comparison to SecuRe Pay recommendations), there should be a longer adoption period, minimally one year, after their coming into force.

***Page 8 question/Consultation question:***

*If the scenario were to materialize that the final text of the PSD2 includes such stronger requirements, the EBA would like to hear respondents’ views on the question whether the final EBA guidelines under PSD 1 should*

*a) 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) 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).*

**CBA comment 2:**

None of the proposed scenarios is acceptable. We suggest keeping guidelines as recommendations or intentions until PSD 2 comes into force and then elaborate guidelines respecting PSD 2 final version. Generally two-step approach is not acceptable because of extra costs and effort inefficiency. Both scenarios a) and b) shortcomings are that with high probability even in scenario b) a second step will be needed to level up additional (not anticipated) PSD2 requirements.

***Page 12 – Scope***

*Payment integrators offering payment initiation services are considered either as acquirers of internet payment services (and thus as PSPs) or as external technical service providers of the relevant schemes or PSPs. In the latter case, the payment integrators should be contractually required to comply with the guidelines.*

**CBA comment 3:**

What is exactly meant by “**Payment integrator**”? Is it “payment initiation service provider” or “account information service provider” in the meaning of PSD2? Currently these types of subjects are likely not to be subject to PSD2, what raise a number of questions and issues (security, liability, client’s protection, data protection etc.). They are not perceived as PSP what is in contradiction with the wording of these Guidelines. From our point of view these types of subjects must be subject to all relevant regulations related to payment services, data protection and information security etc. including these Guidelines.

***Page 13 – Definitions***

**CBA Comment 3**

Please explain meaning of “**sensitive payment data**” – is it any payment related information (amount, counterparty account number etc.) or *“information which when used in isolation, allow control over the payment service user’s account or can be used to carry out fraud”* (such as credit card number etc.) as described in proposal of PSD 2?

Please, align also **other definitions** with PSD 2 proposal - payment initiation service provider, account information service provider, account servicing payment service provider vs. payment integrator, PSP etc.

***Page 16 - Incident monitoring and reporting*** *(and other paragraphs requiring contract between payment initiation service provider and PSP)*

*Acquiring PSPs should contractually require e-merchants that store, process or transmit sensitive payment data to cooperate on major payment security incidents, including data breaches, both with them and the relevant law enforcement agencies. If a PSP becomes aware that an e-merchant is not cooperating as required under the contract, it should take steps to enforce this contractual obligation, or terminate the contract.*

**CBA comment 4**

According to current version of PSD 2, payment initiation service provider does not necessarily enter into contract with the account servicing PSP. In these cases, payment initiation service provider must be subject to all regulations as PSP in order ensure the same rules of security are applicable and applied during whole processing of payments.

***Page 16 - Incident monitoring and reporting***

*3. 2 PSPs should have a procedure for notifying immediately the competent authorities (i.e. supervisory, and data protection authorities), where they exist, in the event of major payment security incidents with regard to the payment services provided.*

**CBA comment 5**

Any type of payment system provider is allowed to break banking privacy only in cases and situations given and described by a law in the Czech Republic. We suppose it will be the same in other Member States. Therefore obligation given by a Guideline to inform “*data protection authorities*” is impossible to be fulfilled as these institutions are not those who could be informed according to banking secrecy legal standards.

***Page 19 - Strong customer authentication***

*The initiation of internet payments, as well as access to sensitive payment data, should be protected by strong customer authentication. PSPs should have a strong customer authentication procedure in line with the definition provided in this report.*

**CBA comment 6:**

We understand a need of protection of client funds (thus payments) by strong authentication, but it is worth considering not requiring it for an access on transactions data such as transaction history, notifications, statements etc., due to higher user convenience.

We suggest that PSP may let a client decide, whether he/she prefers **higher security** and thus protect access to payment related information by a strong authentication or prefer **higher convenience** and protection by a weaker security in the knowledge, that there is a higher risk of unauthorized access to that information. Based on our experience there are some segments (e.g. students) which definitely prefer user convenience where possible. See also next CBA comment 7.

***Page 25 - Paragraph 14.2***

*Any detailed electronic statements should be made available in a safe and trusted environment. Where PSPs inform customers about the availability of electronic statements (e.g. regularly when a periodic e-statement has been issued, or on an ad hoc basis after execution of a transaction) through an alternative channel, such as SMS, e-mail or letter, sensitive payment data should not be included in such communications or, if included, they should be masked.*

**CBA comment 7**

A)  We would like to completely **remove the notion about a letter**. Statement delivery in the paper form is the standard and widely used service and in some cases also required by law as the form of the statement delivery.

B)  Regarding **email and SMS delivery channels**.

We are offering our customers with a subscription to the service, which delivers detailed email/SMS notification about balances, transactions (realized and unrealized) and statements for an account.

In case that **some sensitive data would be masked out**, we see it as an **operational risk** that the client would not be comprehensively and fully informed about some fraudulent transaction.

The client should be provided by:

* **an accurate information** – there is no place for confusing payer account, payee account, amount, currency, or transaction details by any kind of masking. Our clients have automated solutions in place which work with the information from emails.
* **an information fully delivered by the channel of his choice** – SMS notification saying “check your internet banking for details about the transaction” is not sufficient. The client might be e.g. travelling so he would have limited or no access at all to the internet. He expects to be fully informed by the channel of his choice – SMS.

From our point of view, we would rather fully **instruct the client about risks of using unsecured channel** as means of delivery during the service subscription.

For SMS notification it is impossible to provide any widely usable solution for the message content protection – e.g. by password or encryption. SMS notifications are widely used by Retail clients.