Response to the public consultation on the implementation of "Draft EBA Guidelines on the security of internet payments prior to the transposition of the revised Payment Services Directive (PSD2)"

Provided by ABI

November 2014

The EBA launched on 20th October 2014 a public consultation on "The implementation of Draft EBA Guidelines on the security of internet payments prior to the transposition of the revised PSD" (hereafter simply Guidelines).

The Guidelines have been developed on the basis of the ECB "Recommendations on the security of internet payments", as prepared by the SecuRe Pay Forum, with the aim at ensuring a more solid legal basis and a consistent implementation by financial institutions across all Member States.

As done for the SecuRe Pay Recommendations, the Associazione Bancaria Italiana (ABI) has prepared this document in response to the said public consultation after gathering comments from its Members, the ABI Lab Consortium (banking research and innovation centre), the Bancomat Consortium (manager of the Bancomat and PagoBancomat networks and owner of the related trademarks) and the Customer to Business Interaction Consortium[1].

In general, we fully agree with the decision to turn the SecuRe Pay Recommendations into EBA Guidelines, and with the aim of adapting the recommendations to the continuous evolution of the technology and importance of the security of the internet transactions.

In any cases, the adequacy of security depends also on the difference risks related to the number of parties involved: a higher number of parties involved in one specific transaction increase fraud risk, so it's really important that all actors have to implement processes and technological solutions to guarantee the same high level of security.

At the end, we believe that security is one of the most important topic in internet payments, not only for Payment Service Providers (PSP) but also for on-line merchants and customers; however, before making investments on security, we have to be sure that operational cost of implementations are justified to the results of risk analysis and proportionate to the losses stemming from fraud.

With respect to the consultation questions, we signal that **all the banks providing input on this consultation are in favour of solution a):** they prefer that **EBA Guidelines enter into force, as proposed, on 1st August 2015 with the substance set out in the consultation paper, which means they would apply during a transitional period until stronger requirements enter into force at a later date under PSD2 (i.e. a two-step approach)**. In addition, we recommend that once the PSD2 is approved, the Guidelines be revised in order to make them as much consistent and interdependent as possible with the resulting regulatory framework that will emerge.

There are three main reasons underpinning the response above.

First, at present PSPs are working to realize and implement technical structures as requested by SecuRe Pay Recommendations by February 2015 deadline, and it would be impossible for them to change the scope of their projects (and related budgets) already planned in accordance with the SecuRe Pay Recommendations.

[1] The Consortium manages a technological infrastructure for corporate banking that allows interchanges between its members in relation to payment services and document management.

Second, a lead time - well beyond 1st August 2015 – would be required to implement "strong transaction authentication" solutions or, more in general, any solution other than those already set out in the SecuRe Pay Recommendations. In fact, starting from a fragmented situation in the market the implementation of the recommendations issued by Secure Pay Forum covering a wide large range of tools, solutions and practices (such as limiting the log-in attempts to protect access, time-out rules, monitoring of transactions to prevent fraud, multiple layers of security, etc.), already require time and gradual convergence towards the best practices.

Third, there is a need to fine tune the requirements on the basis of the final text of the PSD2, which is not yet available, and thus no precise plan can be set at this stage. Indeed, there is no way whereby the requirements of the PSD2 can be "anticipated".

The fact that EBA has not incorporated any references to the Governance Authorities of payment schemes because the latter are not covered by PSD stands as an example of how important it is that as much regulatory synchronization and interdependency as possible be achieved in order to ensure a more effective and efficient regulatory framework. If the necessary degree of harmonisation is not achieved, the costs stemming from compliance and patchwork regulation would end up outweighing the intended benefits that the Authorities attach to regulatory initiatives such as the one we are commenting.

A general clarification is also required as to the exact scope of the EBA Guidelines. While it is understood that they are based, as mentioned above, on the ECB Recommendations, we wonder how they fit with the more specific and detailed guidance provided with the "Assessment guide for the security of internet payments" published by the ECB in February 2014. In other words, are PSPs obliged to comply by 1st August 2015 with the EBA Guidelines as they will be finally published after the current consultation or should also the more detailed guidance provided for in the ECB Assessment Guide be taken into consideration?