EBA consultation

The SPA position

November 11th 2014

General Comment

Smart Payments Association (SPA) thanks EBA for the opportunity given to participate in the Public Consultation of the EBA guidelines. It is however to us unclear whether comments are requested on the different clauses of the EBA Guidelines or just a response to the two Consultation Question is necessary.

**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**

**Solution a) pro's**

1. This 2-step process, suggests that (1) the final date for the publication of the PSD2 remains uncertain and (2) in between some initiative is to be undertaken to tackle down the expected increase in fraud related to online transactions. This is certainly a possible approach.

2. If we accept the EBA guidelines as they are knowing that "stronger recommendations" are coming up, this means that the comments now will not be considered but there is chance for them to be integrated in the future PSD2.

3. If the PSD2 is released long after August 2015, there will be some in-field feedback on the effectiveness of EBA Guidelines to tackle down fraud. PSD2 then might serve to upgrade the initial set of security requirements set out by the EBA Guidelines.

**Solution a) con's**

1. There is market confusion due to the apparent coexistence of different regulatory frameworks ( SecurePay recommendation for n e-commerce , m-commerce and TPP,PSD1, PSD2, EBA Guidelines, CSG Volume Book 4 + National Regulations ), their respective gaps and overlaps, which EU countries have to implement them as well as deadlines for implementation. This 2-step process makes things more complex.

2. From the Vendors prospective it is difficult to anticipate the demand and approve the product roadmap without knowing which these "stronger requirements in PSD2" will be. For our clients, the problem is similar.

3. There is little incentive to update payment systems when you know that the current set of requirements is going to evolve. Meaning this intermediate time until the publication of the PSD2 is lost … and we still ignore when the PSD2 will be published. Difficult to invest in this context.

4. A security issue is created meaning, the coexistence of (1) legacy systems,(2) systems designed to comply with SecurePay (3) systems compliant with SecurePay but featuring additional security properties with different levels of certification creates security holes …. All these systems have to be monitored and the consumer protected

**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 PS2**

**Solution b) pro's**

1. We create a robust security framework for online payments into force since August 15. The message is clear: security is paramount and must be implemented. A high level of security is required for any system.

2. New online payment solutions have to align with this strong framework. The consumer is protected. Safe innovation becomes a reality, because security is to be integrated early in the design process of any new payment product. Users will decide between solutions equivalent from the security point of view but which still differentiate by their ease of use or other personal advantages

3. From the Vendors prospective the boundaries and requirements are set. The demand can be anticipated and the solutions reengineered. Discussions on PSD2 may focus on other areas than security. The security of online systems no longer relies on the timelines for the publication and transition period to be set out by PSD2.

4. There is a strong inventive for endorsement, despite the fact that waivers for implementation not compliant with the regulation might be possible. With high-standards for security set and endorsed, hackers will focus on those online solutions perceived as weaker.

**Solution b) con's**

1. The main problem is that companies are currently reengineering their offer of online payment products to align with SecurePay ( or these EBA guidelines presumed very close). These products may be outdated before rolled-out, if the EBA Guidelines are upgraded in August 15 with stronger security requirements unknown at present.

2. There is no guarantee than in the end PSD2 will still be changing requirements. This may be felt as an inconvenient from the development and certification prospective, but also as an option to enhance security if the August 15 Guidelines give rise to implementations featuring security breaches.

**SPA Opinion**

Taking into account our analysis of pro's and con's for the two solutions submitted to comment by EBA **SPA considers that Solution b) is preferable.**

**Solution b) enables a better anticipation of the market demand for Vendors and Solution providers and helps driving online payment solutions towards good security engineering practice.**