EDiMA
Shaping Internet Policy in the EU

EBA 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)

On behalf of its member companies, the European Digital Media Association[1] (EDiMA) welcomes the opportunity to respond to this consultation. We recommend the following:

- EBA should **await finalization of the PSD2 text and then review the SecuRe Pay Recommendations against these new security requirements** before issuing draft EBA Guidelines.
- **The definition of strong authentication should be flexible enough to allow for new technologies** to develop – tying this to two-factor authentication will stifle innovation in payment security. Security future proof regulations should aim at setting security benchmarks as opposed to imposing processes**.**
- EBA Guidelines should ensure **reconciliation of security with consumer convenience, as over complex security methods might lead to users' avoidance behavior with increased risk for users.**
- EBA Guidelines **should be consistent with global security practices to prevent creation of a "European fortress"**.

1. Response to the consultation question

Regarding the consultation question on the inclusion of the PSD2 requirements in the EBA Guidelines, we would like to share the following observations.

1.1 Insufficiency of the one-step approach

The benefits of the one-step approach are difficult to assess at the time of this consultation. The revised Payments Services Directive (PSD2) will not be adopted before early 2015 at best. Chapter 5 of PSD2 - on operation and security risks and authentication - will therefore continue to be amended during the next few months, making it difficult for payment service providers (PSPs) to evaluate and prepare for compliance with these requirements (see also Section 2 below on strong customer/transaction authentication).

Should the EBA Guidelines incorporate the PSD2 requirements before these are finalized, EDiMA sees a three-fold risk:

[1] EDiMA is the European trade association representing online platforms. It is an alliance of new media and Internet companies whose members include Allegro, Amazon EU, Apple, eBay, Expedia, Facebook, Google, Microsoft, Nokia, Yahoo! Europe. EDiMA's members provide Internet and new media platforms offering European consumers a wide range of online services, including e-content, media, e- commerce, communications and information/search services.

1) if the requirements eventually adopted in the PSD2 are not fully aligned with the EBA Guidelines, PSPs may have to implement and comply with requirements that have no legal basis and will become irrelevant when the PSD2 becomes enforceable;
2) the negotiations regarding the PSD2 requirements, which are still ongoing, may be impacted or influenced by the EBA Guidelines and may not take into account the input which is being provided by the relevant stakeholders during the legislative process, including from national financial regulators, trade associations, and the industry; and
3) to implement the PSD2 authentication requirements, as detailed by the secondary legislation (EBA Guidelines and Technical Standards), PSPs will need to carry out additional technical work and product changes, very likely requiring the abandonment of the product changes already undergoing to meet the SecuRe Pay Recommendations requirements.

1.2 Recommended approach

Although EDiMA strongly opposes the one-step approach, EDiMA notes that the two-step approach (i.e. the EBA Guidelines enter into force on 1 August 2015 without anticipating the PSD2 requirements) is also insufficient to ensure the necessary legal certainty for the PSPs and convenience for customers, whose transactions would be subject to disruptive authentications methods (potentially disproportionate to associated risks), which will negatively affect customers experience. ***EDiMA therefore strongly recommends that EBA awaits finalization of the PSD2 text and then review the SecuRe Pay Recommendations against these new requirements before issuing draft EBA Guidelines and/or Technical Standards.*** This approach will avoid unnecessary burden for PSPs as well as the risk of preparing to comply with two potentially diverging sets of requirements to address the very fundamental security issues.

*****

Additionally, in the spirit of EBA's commitment to stakeholders consultation, EDiMA wishes to submit the following comments concerning the EBA Guidelines but also on the PSD2 itself.

2. Comments on strong customer/transaction authentication

Best Practice (BP) 7.3 of the SecuRe Pay Recommendations refers to *"strong customer authentication"* potentially including "*elements linking the authentication to a specific amount and payee*". The latest draft of the Italian Council Presidency compromise text on the PSD2 mandates 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*".

This requirement can be acceptable as a best practice – as it stands in the current draft EBA guidelines – because it allows PSPs to assess how, when and in what circumstances to apply this type of authentication. However, mandating it as a 'one size fits all' approach in PSD2 would be unduly prescriptive, entailing the risk of stifling innovation. Moreover, it wouldn't allow online companies to maintain some of their current customer-friendly business practices. For instance, when a customer purchases several items that are shipped at different times, some online retailers split the transaction and charge the customer at the time each item is shipped. This would no longer be possible under Article 87(1a) of the latest Council text. Customers would either have to be charged for the full amount upfront (thus paying for items that have not yet been sent by the merchant) – which may also raise issues regarding compliance with card schemes rules – or when the last item of the order is shipped (thus impacting retailers cash flow and forcing them to wait and bear the risk of unpaid for items already delivered).

EDiMA therefore recommends that the EBA supports the online payments industry in persuading the EU Council to include the "Comply or Explain" principle and the risk-based approach – as included in the SecuRe Pay Recommendations – **in the provisions of Chapter 5 of the PSD2**. This would allow PSPs to focus on the outcome of the security measures they adopt. Unless PSD2 clearly reflects these principles and provides flexibility to PSPs regarding how they implement strong customer authentication (where justified), prescriptive requirements on how to perform strong authentication will negatively impact payment service users (by disrupting their customer experience when shopping online) as well as PSPs (by frustrating their willingness to invest in innovative authentication technologies), without any additional benefit to the security of payments.

3. Comments on the payment security approach

3.1 Need for a broader definition of strong authentication

The current definition of strong customer authentication, referencing to the traditional two-factor authentication (such as 3DS) as the only authentication method for retail payments, risks hindering innovation and technology advancement in the EU. It relies on prescribing a limited list of qualifying criteria instead of focusing on the security objective of the measure.

Strong customer authentication effectively means any method allowing for secure authentication of the legitimate user of a specific payment instrument via multiple factors (so-called Multi-Factor Authentication or 'MFA'). MFA allows for a variety of alternative security measures: investments in the area of innovative authentication in the past years have showed that MFA can be equally – or even more – efficient than 3DS to prevent fraud and protect customers. MFA methods analyze various factors to determine legitimacy of the user, including customer behavioral patterns (e.g. if online payments are executed from the usual device, IP location, use of the same physical address indication etc.), machine learning, geo-localization, real-time data analytics etc.

These factors are already used today for risk-based anti-fraud measures, with effective results, and they are becoming increasingly relevant in light of evolving technology advancements. ***EDiMA recommends that the EBA Guidelines extend the strong authentication definition to include a Multi-Factor Authentication which reflects the state of the art of authentication technologies and caters for innovation.***

3.2 Technological neutrality should underpin future-proof security policies

Technology development – especially in the digital area – happens much faster than any policy drafting or review. To avoid hindering innovation, regulation should be based on technological neutrality and define the security result to be achieved rather than mandating how to achieve the given result. As the area of payments authentication has already been proven to benefit from new technologies, EU policies should encourage innovative developments and future-proof regulation. ***EDiMA's recommendation is that the EBA Guidelines take a technology-neutral and outcome-focused approach by defining the security objectives to be achieved, while leaving PSPs the flexibility on how to achieve them.*** Strong issuer authentication and strong transactions authentication stand in stark contrast with this approach.

3.3 Consumer convenience is core to the uptake of EU digital payments

The main challenge for the digital payment security is to find the right balance between security and a user experience. Industry experience shows that customer convenience is equally important to maintaining overall security as encouraging a safe use of the product. It also prevents abandonment of transactions or attempts to avoid the security requirements. ***EDiMA's recommendation is that the EBA Guidelines ensure adequate balancing of consumer convenience with security objectives.***

3.4 Global payment security practices must be contemplated

E-commerce is a global business, so any rule enforced upon the industry must have a global perspective. For a global business such as digital payments, fragmentation of the applicable rules undermines its full potential and reduces business opportunities. EU policy-makers should ensure that security measures enforced within the EU are in line with global security practices. This will ensure the competitiveness of the EU digital market in the global marketplace. ***EDiMA's recommendation is that the EBA Guidelines ensure consistence with global security practices to avoid creation of a "European fortress" in the field of security***.