To the Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Germany

Consultation Reply

on the 'Konsultation 02/2015 - Rundschreiben zu den Mindestanforderungen an die Sicherheit von Internetzahlungen' (GZ: BA 57-K 3142-2013/0017)

(To the planned BaFin circular on minimum requirements for the security of internet payments)

by e-mail to: konsultation-02-15@bafin.de

18th March 2015

Contact:

EPSM e.V.
board@epsm.eu

This reply was written by the EPSM consultant Lars Tebrügge, having received input from the members of the EPSM and approval from the EPSM board.

About the EPSM

The "European Association of Payment Service Providers for Merchants (EPSM)" is an interest representation and information platform of European payment network operators, acquirers and other payment service providers for merchants. Among the non-voting members are terminal manufacturers, processing and acquiring providers as well as payment schemes. It is based in Munich, Germany.

The 68 EPSM members have their headquarters in 15 European countries (AU, BE, CH, CZ, DE, DK, FR, GR, IR, LU, LV, NL, SE, SK, UK).

1. Achievement of a 'European Level Playing Field' is unclear

a) Transpositions in Other Member States

The EPSM would appreciate clarification on how the 'Guidelines on the Security of Internet Payments' (guidelines) from the European Banking Authority (EBA) will be implemented in other member states. EPSM members from other European countries, e.g. the Scandinavians and the U.K. reported that there is no corresponding initiative known from the respective competent authorities.

EPSM is very much in favour of a consistent approach in all European countries and would welcome clarification on how this will be achieved.

b) Bindingness

In the English guidelines of EBA most of the requirements contain the formulation 'should'. Also, the official German translation of the EBA Guidelines matches this formulation with the German word 'sollte/n'. The consultation tabled from BaFin uses the words 'muss' or 'hat zu' which translates to the English expressions 'must' or 'have to'.

This raises the question, why BaFin changed this wording in such a significant way. How can it be ensured that the bindingness will be the same in all Member States? In order to maintain a European level playing field, the EPSM suggests that BaFin will support the original form of the EBA guidelines.

c) Comply-or-Explain Principle

The previous version issued from the SecuRe Pay Forum contained a fundamental principle called 'comply-or-explain'. This means that an organisation should either comply or needs to explain, why it does not follow the guidelines.

In our experience, all major organisations providing internet payments services should have their own fundamental business interest in providing the best appropriate security level.

Consequently, service providers should be granted the possibility to deviate from the regulatory approach and be allowed to install market driven solutions with the same or even better results.

2. Scope needs to be clarified

a) Online Banking

In the letter accompanying the consultation it is mentioned that payments, which can be initiated via 'Online-Banking', are covered. This explanation does not correspond to the

definition of the scope in the text of the consultation. According to this definition, all payment services (§ 1 Abs 2 ZAG) provided from payment institutions (§ 1 Abs 1 ZAG) are covered.

b) Acquiring

The consultation document obliges ‘acquirers’ to perform a number of tasks, without defining what an acquirer is. The EBA guidelines are always referring to ‘acquiring payment service providers’. It is understood, that only such acquirers are regulated, which are covered by the Payment Service Directive (respectively by the ZAG).

It would be welcomed, if this could be clarified in the consultation of BaFin.

c) App and Wallet Payments

Payment procedures have developed significantly in the last years. In the current consultation document it is unclear, whether new forms of payments are inside the scope. It remains open, to what extend for example so called ‘in-app-payments’ are covered. To our understanding there is also room for interpretation, if wallet solutions that are not based on card payments, are regulated – e.g. if a payment wallet handles only SDD payments.

d) Extra-territorial institutions and transactions from outside SEPA

From our understanding the drafted ‘Mindestanforderungen an die Sicherheit von Internetzahlungen‘ is applicable to payment service providers that are supervised from BaFin. A clarification would be appreciated to what extend extra-territorial institutions are covered – e.g. companies registered outside Germany and providing services in Germany and companies registered in Germany providing services abroad.

The EPSM also believes that more guidance is needed regarding transactions which origin from outside Germany and/or outside SEPA. Assuming that in other countries, the requirements for strong customer authentication as defined in the present consultation are unknown and the consumers are not supplied with the respective credentials. The EPSM would be interested to learn how an authentication process should look like in these cases. The EPSM believes that certain requirements should be waived for this kind of transactions.

e) Telephone Banking and Telephone Order

It is understood that BaFin intends to apply the rules on internet payment also on ‘telephone banking’ in an analogous manner. The EPSM questions to what extend the principles on strong customer authentication can be applied for telephone banking. Furthermore, it is unclear, how ‘telephone orders’ have to be handled. This payment method is characterised by a consumer providing payment authentication data to a merchant who may enter the credentials into a web-browser.

3. Coordination with NIS Directive is pending

The objective of the proposed Directive on 'Network and Information Security' (NIS) is to ensure a high common level of network and information security across the EU. According to the NIS directive, entities providing critical infrastructures are required to report to the competent authorities incidents with a significant impact on core services. These reporting requirements are similar, but not identical with the requirements from the present consultation.

Consequently, it should be ensured that the NIS Directive, currently being transposed in the Member States, and the Guidelines from EBA correspond with each other and do not contain contradicting requirements.

4. Details on 'Strong Customer Authentication' compliance are missing

a) Provider of strong customer authentication solutions seem not to be ready

The EPSM, representing service providers for merchants, has difficulties to understand, which organisations are in charge providing solutions for strong customer authentication.

It needs to be noticed that acquiring service providers are only able to offer services, respectively payment methods including authentication solutions that are available in the market. From the perspective of EPSM it seems unlikely that in the next five month comprehensive solutions that are in line with the strong customer authentication requirements will be available.

As it is believed that stopping the majority of internet payments and jeopardising the business models of a whole industry cannot be the intention of the BaFin, a clarification from BaFin, how a switch to strong customer authentication is envisaged in practice, is needed.

b) Consistent certification and approval of solutions are needed for SEPA

Presently, guidance is needed to clarify which solutions are in line with the requirements of strong customer authentication. Consequently, EPSM strongly urges BaFin to clarify which organisations, institutions and or authorities are in charge of providing information which solutions comply with the requirements.

5. Closing Note

The goal of the EPSM with this paper is to help in the creation of a workable, secure and appropriate “European Level Playing Field” for payment providers and merchants.

Please do not hesitate to contact Mr. Lars Tebrügge or the EPSM board for any remaining questions or comments.