BANKING STAKEHOLDER GROUP

CONSULTATION ON EBA/CP/2014/31 ON
GUIDELINES ON SECURITY OF INTERNET PAYMENTS

General Comments and Replies to Questions

BY THE EBA BANKING STAKEHOLDER GROUP

London, 14th November, 2014

Foreword

The EBA Banking Stakeholder Group ("BSG") welcomes the opportunity to comment on the Consultation Paper EBA/CP/2014/31 on Guidelines on Security of Internet Payments.

This response has been prepared on the basis of comments circulated and shared among the BSG members and the BSG's Technical Working Group on Consumer Issues and Financial Innovation.

As in the past, the BSG supports an initiative that aims at harmonizing supervisory rules and practices across Europe, in order to ensure fair conditions of competition between institutions and more efficiency for cross-border groups. The BSG also expects these initiatives to facilitate data sharing between European supervisors and avoid reporting duplications for banks. However, the BSG identifies a number of issues which, unless properly addressed, could lead to unintended results.

General comments

1. The BSG welcomes the plans outlined in the Consultation Paper for the EBA to address the issue of security of internet payments: it is a growing area of financial transactions, and the potential risks are not always apparent to, or understood by, consumers. For these, and those detailed in the Consultation Paper, we endorse the view that there is a need for a solid legal basis of consumer protection in this area rather than relying on the hitherto voluntary arrangements. We would emphasise the need for consumers to be able to have maximum trust and confidence in the use of internet facilities for payments.

2. However, some members of the BSG question the effectiveness of the guidelines as a basis for EU-wide implementation of high payment security standards. In some member states, guidelines or self-binding codices are not something financial institutions would follow. In this context we note in paragraph 3.2 of the Consultation Paper the reference to 'competent authorities where they exist'.

3. An effective monitoring mechanism as a part of these guidelines is of great importance. In particular, more guidance is needed for national

supervisory authorities on how to ensure compliance, as many national supervisors don't have mandates or defined procedures for action in the field of consumer protection.

4. The Consultation Paper does not make clear why certain payment services are excluded from these guidelines. The BSG would welcome statements about the rationale for exclusions particularly 1, 4 and 7. We also note that mobile phone payments and services by 3rd party providers are relatively new to consumers and are expanding quickly and possibly constitute new operating channels for fraudulent activities, so high security standards are very desirable.

5. We advocate that the Paper should promote regular joint reporting of security incidents and fraud by the PSPs to the authorities and the public. Data on consumer harm and in particular payment operations, relevant risks and instructions on security measures can be very useful for consumers, but are not available in most of the member states. Examples of good practices are in my opinion the French "l'Observatoire de la sécurité des cartes de paiement" and "Financial Fraud Action UK".

6. It is important in our view that the PSPs should make sure that clear and understandable security instructions are provided for all relevant operations by consumers. More important than general education programmes and campaigns is actionable and accessible information when the consumer is using these services. The information should be clear also for an 'average' consumer who uses such payment methods. PSPs should not expect an 'average' consumers to act similarly for example to an IT expert, by instructing them to implement measures that are complicated, time consuming or expensive. There is a danger that the PSPs expectations of consumers knowledge of payment security is of a too high level.

7. The BSG agrees strongly that PSPs should evaluate the adequacy of their internal security controls against internal and external risk scenarios. However, the Consultation Paper seems to say little about how these evaluation procedures will be monitored externally

including by supervisory authorities. The BSG would welcome more information about whether such monitoring will take place and, if so, how it is envisaged it will take place.

8. Page 15/16 General Control and Security Environment: There is a need for more clarity as to the nature of the 'review'. Under 'Governance' there is a reference to a 'regular review' and later in paragraph 2.4 there is a reference to a 'general review'. We assume the reference in paragraph 2.4 to the 'general review' taking place at least once a year relates additionally or is the same time period as the 'regular review'.

9. Page 15/16 General Control and Security Environment: There is a need for more clarity as to the nature of the 'review'. Under 'Governance' there is a reference to a 'regular review' and later in paragraph 2.4 there is a reference to a 'general review'. We assume the reference in paragraph 2.4 to the 'general review' taking place at least once a year relates additionally or is the same time period as the 'regular review'.

10. For clarity we suggest that paragraph 2.4 is amended to read: 'The PSPs should undertake a general review of the risk assessment and should be carried out at least once a year. Additionally, PSPs should undertake a review of the risk scenarios and existing security measures after major incidents…….etc.' Followed by the last sentence 'The results of the risk assessment ….etc.'

11. The Consultative Paper should make clear what information is to be provided to supervisory authorities about individual institution's security arrangements and state that supervisory agencies have power to intervene if they are judge to be inadequate.

12. We are of the opinion that para 2.3 (page 15) is vague and needs to be more explicit.

13. With reference to Point 7 above should "regularly" in para 4.5 page 17 be made more explicit?

14. Paragraph 4.6 refers to 'periodically audited'. It would be appropriate if a time period were to be given rather than the reference just to periodic.'

15. Para 4.7, page 17: should there be a requirement for PSPs to monitor and evaluate the security arrangements instituted by insourcers?

16. Para 9.3, page 22: should the GLs specify this maximum period?

17. With regard to the Consultation Question detailed on Page 27: the members of the BSG have differing views on the implementation of the EBA guidelines and therefore it is inappropriate for the BSG to state any preferences.

Submitted on behalf of the EBA Banking Stakeholder Group

David T. Llewellyn
Chairperson