BANKING STAKEHOLDER GROUP

DRAFT BSG RESPONSE TO EBA/DP/2015/03 ON FUTURE DRAFT REGULATORY TECHNICAL STANDARDS ON STRONG CUSTOMER AUTHENTICATION AND SECURE COMMUNICATION UNDER THE REVISED PAYMENT SERVICES DIRECTIVE (PSD2)

General Comments and Replies to Questions

BY THE EBA BANKING STAKEHOLDER GROUP

London, February 7, 2016

The BSG welcomes the opportunity to comment on the Discussion Paper on future Draft Regulatory Technical Standards on strong customer authentication and secure communication under the revised Payment Services Directive (PSD2).

The BSG welcomes the efforts made by authorities to define the technical procedures to improve payments security and providing a common framework for all players. These regulatory technical standards (RTS) are part of the new Payment Services Directive launched in 2015 and contribute to the clarification of open issues included in that Directive.

Main concerns

The BSG is aware that the main design of the Payment Service Directive is out of scope of this document and is not open to discussion. However, we believe that authorities must understand some key issues mentioned below as the security of consumers is one of the main concerns of PSD2.

The access to personal security credentials (PSC) in relation to customers' security. There is a concern related to sharing Payment Service User (PSU) security credentials caused by the implication of more players within the payments value chain. The new Payment Services Directive encourages competition and allows the access of third party providers (TPP) to the users' account which is held in a different entity. However, there are issues that need to be resolved such as the access to the PSC. In order to protect the consumers, reduce risk and avoid fraud, we recommend that PSC should not be accessed directly by TPP, for example a consumer entering his or her bank account password in a TPP website. However, to ease customer experience while operating with different payment services providers, once the customer grants access to the TPP following a strong customer authorization through the security systems of the account services provider, the TPP can access the customer's account for informational purposes when the customer requires it. For payment transactions, following article 97.1.b, strong customer authorization through the bank security systems is recommended on each transaction. Sharing credentials can lead to fraud, and responsibilities could be difficult to establish as customers' credentials are involved. Nevertheless, we promote the competition following PSD2 statements allowing TPPs to provide services following the same security standards as any other players.

We would like to note that sharing PSC would be against the long-standing security awareness efforts made by financial institutions to educate their customers not to share their credentials, under any circumstance, with third parties. If customers get used to the opposite when using payment initiation or account aggregation services, it could create a harmful precedent that could end up increasing risk and fraud.

Ensuring that the responsibility of the financial costs of fraud is liable to the party that performed the strong authentication would continue promoting high levels of security on electronic payments.

Given the proliferation of scenarios where users need to grant authorization to third parties in order to access their information, or to act on their behalf before their service providers become mainstream, it is fundamental that the **RTS developed by EBA do not impose any restriction on the ability of European PSPs to develop homogeneous services at global level**.

Questions for discussion

4.1 Considerations prior to developing the requirements on strong customer authentication

1. With respect to Article 97(1) (c), are there any additional examples of transactions or actions implying a risk of payment fraud or other abuses that would need to be considered for the RTS? If so, please give details and explain the risks involved.

BSG considers that the examples of Article 97(1) (c) are appropriate but would like to suggest further examples that are not included but which we judge to be important. In particular, we suggest that any interaction that implies the modification of contact details, authorization mechanisms or any element necessary for the initiation of transactions, should be exempted from the strong customer authorization (SCA) obligation such as frequent beneficiaries' lists must require strong customer authorization.

The rationale behind this issue is that the modification of this information without strong customer authorization would increase the ability of fraudsters to gain access to PSUs' personalized security credentials or to initiate transactions without their authorization (for example, creation of trusted beneficiaries by a PSU would not require strong authentication).

BSG also suggests that EBA should explicitly mention that those requirements should also apply to mail orders and telephone orders, as these are carried out through a remote channel which implies the same risk of payment fraud as other remote transactions.

2.: Which examples of possession elements do you consider as appropriate to be used in the context of strong customer authentication, must these have a physical form or can they be data? If so, can you provide details on how it can be ensured that these data can only be controlled by the PSU?

BSG considers that it is appropriate the use of physical possession elements due to the current state of technology: tokens, National ID cards, payment cards and mobile devices. Regarding data elements, soft tokens and mobile numbers are also necessary elements.

We would like to include the problem related to the loss of control of those elements that the customer might suffer. To ensure security, we recommend mechanisms to limit their misuse through physical controls and validations on concession and operation restrictions afterwards. The creation of mechanisms to detect possible fraud is also important As an example the use of behaviour analytics of the customer based on machine learning and artificial intelligence that can help to detect and avoid fraud.

In the case of software elements, it is important to adopt measures regarding the software installation, the user impossibility to modify the software, and other restrictions related to the devices where the software is installed to prevent misuse and unwanted modifications. BSG also suggest the use of international standards when addressing the security related to hardware and software. In the use of mobile payments, those standards are required to allow interoperativity and provide a common field.

3. Do you consider that in the context of "inherence" elements, behaviour-based characteristics are appropriate to be used in the context of strong customer authentication? If so, can you specify under which conditions?

With the current state of technology, the behaviour-based characteristics are less reliable as an "inherent" element than are, for example, biometric elements. Nowadays, behaviour-based characteristics are a useful monitoring tool to detect irregular transactions and prevent the risk of fraud. For example, in order to detect transactions carried out in a different country or IP. However, from our point of view, behavior-based characteristics are not a strong customer authentication element. Behaviour based characteristics could only be used as a complementary tool in the context of strong authentication.

Nevertheless, provided that a precise and reliable technology becomes available in the future, we demand that the use of one or a combination of behaviour-based elements should not be restricted by the RTS.

4. Which challenges do you identify for fulfilling the objectives of strong customer authentication with respect to the independence of the authentication elements used (e.g. for mobile devices)?

There is a challenge in the externalization of the security elements: how to enable the access of TPPs to the customer account, because there must be a correct balance between user experience and security. BSG recommends EBA to consider that the ASPSP or account holder should always be in control of the authentication method of the customer. Otherwise it is difficult to justify that the risk and fraud liability is a responsibility of the ASPSP if the credentials are shared, without prejudice of the measures established at PSD2. To reinforce this, passwords should never be stored in the device.

BSG reinforces the idea that the existence and availability of mechanisms to block the use of the authentication elements in cases where PSU (Payment Service User) loses control is crucial in this issue.

BSG also recommends EBA to establish guidelines and minimum requirements to establish a strong customer authentication following international standards but allowing different value propositions to arise in the market. This will lead to different solutions in the market to achieve the same means and the customer can choose increasing competence.

5. Which challenges do you identify for fulfilling the objectives of strong customer authentication with respect to dynamic linking?

BSG invites EBA to clarify the concept of dynamic linking in the RTS, establishing some general criteria on dynamic codes to provide a common field. Nevertheless, it is fundamental to avoid the prescription of a specific solution or being too specific in the way dynamic codes are to be calculated, since meeting those requirements would be a challenge for PSPs to provide different solutions to the customer as part of their value proposition.

We must also note that the criteria to be established should not hinder the ability of European PSPs to make use of international standards that are commonly accepted.

As an alternative, we can understand the dynamic linking as a dynamic token using a cryptographic algorithm that needs to share the verification algorithm with the TPPs.

6. In your view, which solutions for mobile devices fulfil both the objective of independence and dynamic linking already today?

There are already solutions, related to SIM cards or different devices, that allow the safe storage of information that cannot be accessed by the applications. Technical solutions, such as the secure storage of authentication elements in some mobile devices, touch IDs (fingerprint recognition) and the functionality of some SIM cards, could help to achieve these objectives.

4.2 The exemptions to the application of strong customer authentication

7. Do you consider the clarifications suggested regarding the potential exemptions to strong customer authentication, to be useful?

The BSG considers that the clarifications provided by the EBA are useful as a guideline to a more detailed RTS development so as to promote a level playing field. However, the exceptions should be optional and very dynamic to countermeasure the fast industrialization of cyber-crime. If the exceptions are strictly defined, it can allow an entry door for fraud until a new regulation allows measures to be taken against it.

Regarding the possible exception of "low-risk transactions based on a risk analysis", we would like EBA to consider that the guidelines on criteria to determine low-risk transactions should provide further clarifications, including the criteria to determine what is a low risk transaction, the information to be considered, and minimum requirements of the tools used for the completion of that analysis. Convenience, for example allowing not to require the PIN code for low value transactions, and security must be taken into account and leveraged.

8. Are there any other factors the EBA should consider when deciding on the exemptions applicable to the forthcoming regulatory technical standards?

The BSG recommends EBA to consider that the exemptions could be based on transaction risk analysis taking into account RTS detailed specifications. This risk analysis can be based on internal fraud analytics or based on historical fraud figures and number of cases.

Nevertheless, as stated in answer to question 1, any interaction that implies the modification of contact details, authorization mechanisms or any element necessary for the initiation of transactions exempted from the strong customer authorization obligation (such us frequent beneficiaries') lists must require this type of authorization.

9. Are there any other criteria or circumstances which the EBA should consider with respect to transaction risks analysis as a complement or alternative to the criteria identified in paragraph 45?

BSG recommends EBA to consider in its risk analysis proposition that there are situations where a transaction is apparently executed in an environment which is different from that where it really takes place. This could undermine the dynamic risk analysis as it is taking into account that the transaction took place in a different environment. An illustrative example is that some transactions may happen in a client-present environment but, apparently, the transaction is being executed through Internet or remote-channel, such as a wallet-app payment.

Additionally, we would like EBA to consider the development of mechanisms to share information on relevant fraudulent incidents and trends. As an example, the notification of a cyberattack, how it happened and its characteristics, can avoid further attacks n other institutions.

Finally, we would like to mention again the use of the behaviour of the user and the devices used by the user in risk analysis as a complement to further authentication methods answered in question 3.

4.3 The protection of the payment service users' personalised security credentials

10 Do you consider the clarification suggested regarding the protection of users personalised security credentials to be useful?

BSG considers the clarification suggested by EBA is useful. However, we would like EBA to consider that credentials or passwords should never be stored as mentioned in answer to question 4.

11. What other risks with regard to the protection of users' personalised security credentials do you identify?

BSG considers that personalised security credentials (PSC) are a key element of security as they provide access to the payment service user (PSU) information. Although we encourage competition amongst all players,in the interests of consumers' security, we ask EBA to avoid the access to PSU's personalised security credentials by third party providers: for example, sharing the passwords that provide access to customers' accounts in a TPP website. However, to ease customer experience while operating with different payment services providers, once the customer grants access to the TPP following a strong customer authorization through the security systems of the account services provider, the TPP can access the customer's account for informational purposes when the customer requires it. For transactional services, and, following article 97.1.b, we recommend always SCA through the account provider systems for security reasons. There is a risk of using those credentials if a fraud takes place and the responsibility, will be difficult to establish as it implies the use of the password. In any case, we demand that TPPs comply with the same security standards as as any other PSP.

Finally, BSG would like to indicate to EBA that any solution should be based on international open standards.

12. Have you identified innovative solutions for the enrolment process that the EBA should consider which guarantee the confidentiality, integrity and secure transmission (e.g. physical or electronic delivery) of the users' personalised security credentials?

We have identified solutions based on customers' own biometrics as well as the biometric of the ID Cards and features embodied in devices. Open standards already in place (Open ID, OAuth, …) could also contribute to achieving a reasonable level of confidentiality, integrity and security.

13. Can you identify alternatives to certification or evaluation by third parties of technical components or devices hosting payment solutions, to ensure that communication channels and technical components hosting, providing access to or transmitting the personalised security credential are sufficiently resistant to tampering and unauthorized access?

From the BSG's point of view, as long as PSU security credentials are not accessed directly by TPPs, there will be no necessity to ensure that this information is securely protected by these third parties. Nevertheless, the protection of TPPs own security credentials should be done according to the same security standards required to ASPSPs.

14. Can you indicate the segment of the payment chain in which risks to the confidentiality, integrity of users' personalised security credentials are most likely to occur at present and in the foreseeable future?

BSG considers that when a TPP is acting on behalf of the customer, or a software element is initiating a payment in a device without full control by the customer, the risk of impersonation and unauthorized access to personalised security credentials increases. To reduce these risks and/or their impact, we consider that customers' identification information should only be provided by themselves and, in case security credentials are compromised, mechanisms to revoke authorization should be available and easily accessible by the PSU.

4.4 Considerations prior to developing the requirements on common and secure open standards of communication

15. For each of the topics identified under paragraph 63 above (a to f), do you consider the clarifications provided to be comprehensive and suitable? If not, why not?

BSG agrees with the clarifications provided by EBA. However, we consider that EBA should address TPPs Card Services in this RTS which are already mentioned on the new Payment Services Directive but require further development.

16. For each agreed clarification suggested above on which you agree, what should they contain in your view in order to achieve an appropriate balance between harmonisation, innovation while preventing too divergent practical implementations by ASPSPs of the future requirements?

BSG considers that an appropriate balance between those factors could be achieved referencing the RTS to commonly accepted international standards already in use.

BSG would like to encourage EBA's RTS to clearly state which services require each type of TPPs in order to provide access (for example, a personal finance information service is not the same as a service that allows to transact) and a governance model to manage liabilities and claims.

The RTS should focus more on the interchange of the information within the value chain, responsibilities and communications amongst participants in the value chain. But, in order to encourage competition, there should be more freedom in the authentication mechanisms of the customer and in the assumption of the fraud risks in the value chain.

17. In your opinion, is there any standards (existing or in development) outlining aspects that could be common and open, which would be especially suitable for the purpose of ensuring secure communications as well as for the appropriate identification of PSPs taking into consideration the privacy dimension?

BSG would like to make EBA aware of developing standards only applicable at the European level as it would increase barriers with international markets and would provoke and increase the cost and complexity for European banks.

18. How would these requirement for common and open standards need to be designed and maintained to ensure that these are able to securely integrate other innovative business models than the one explicitly mentioned under article 66 and 67 (e.g. issuing of own credentials by the AIS/PIS)?

BSG would like EBA to consider that this RTS should refer to commonly accepted international standards already in use because thereby the adoption of other standards that could potentially be developed in the future instead of only devising a European solution. BSG considers that developing standards that are only applicable at a European level would hinder the ability of European banks to compete in international markets and would increase costs and complexity.

4.5 Possible synergies with the regulation on electronic identification and trust services for electronic transactions in the internal market (e-IDAS)

19. Do you agree that the e-IDAS regulation could be considered as a possible solution for facilitating the strong customer authentication, protecting the confidentiality and the integrity of the payment service users' personalised security credentials as well as for common and secure open standards of communication for the purpose of identification, authentication, notification, and information? If yes, please explain how. If no, please explain why.

BSG considers that e-IDAS Regulation could be a solution to guarantee confidentiality and integrity in strong customer authentication, mainly for customer identification purposes. As the European Commission puts it, rolling out e-IDAS means higher security and more convenience for any online activity such as remotely opening a bank account, authenticating for internet payments, etc. Moreover, we would like EBA to consider that, in

case the PSP is required to delegate this mechanism to a public institution in charge of the e-IDAS system, the risk and liabilities should be controlled by the public institution, not by the different service providers.

Finally, we asks EBA to establish common standards but allow that the relationship protocols definition between the PSUs and PSPs are left to the market competitive forces.

20. Do you think in particular that the use of "qualified trust services" under e-IDAS regulation could address the risks related to the confidentiality, integrity and availability of PSCs between AIS, PIS providers and ASPSPs? If yes, please identify which services and explain how. If no, please explain why.

BSG considers that, as long as the qualified trust services involved are subject to the same liabilities as the rest of the participants in the value chain, their use according to the e-IDAS regulation could address those risks under a strict oversight.

Submitted on behalf of the Banking Stakeholder Group,

David T Llewellyn

Chair Person