IMPLEMENTATION OF DRAFT EBA GUIDELINES ON THE SECURITY OF INTERNET PAYMENTS PRIOR TO THE TRANSPOSITION OF THE REVISED PAYMENT SERVICES DIRECTIVE (PSD2)

The European Banking Authority published a Consultation Paper [1] on the 20th October 2014 inviting comments on Draft EBA Guidelines on the Security of Internet Payments (the Guidelines).

In addition to answering the specific Consultation Question regarding the entry into force of the Guidelines, the present document presents the views of Cartes Bancaires "CB" in response to the overall issues raised in the EBA paper, and where appropriate, suggests areas of improvement.

The structure of the response follows as far as possible that of the Guidelines themselves, providing general remarks on the implications and perceived objectives of the Guidelines.

It also outlines considerations related to the security issues covered by the Guidelines as well as the probable legal repercussions should the Guidelines be adopted in their present form.

Cartes Bancaires "CB" would welcome the opportunity to discuss the content of this document and provide further explanation should the EBA or the European Forum on the Security of Retail Payments so wish.

CONTACT

David Stephenson
Head of International Affairs

Groupement des Cartes Bancaires "CB"
151 bis Rue Saint Honoré
75001 Paris, France

david-stephenson@cartes-bancaires.com

+ 33 (0) 1 40 15 58 80

14 NOVEMBER 2014

[1] http://www.eba.europa.eu/documents/10180/855014/EBA-CP-2014-31+(CP+on+security+of+internet+payments).pdf

Response to the EBA Consultation Paper

1. Date of Entry into force of the Guidelines

The EBA proposes that the Guidelines should enter into force on the 1st August 2015.

This might be possible for much of the substance of the Guidelines, but great care should taken not to anticipate the exigencies which will be required due to Article 87 (Authentication) in the Payment Services Directive (PSD2) currently under revision.

Instead of the Guidelines entering into force on the 1st August 2015, a more progressive and prudent approach would be preferable since the expected date of entry into force of the PSD2 through its transposition in the different Member States will probably only be at the beginning of, or during the 1st half of 2017, and that between now and then technologies and authentication techniques will most likely evolve.

To respond to the specific question in the EBA Consultation, **it is recommended that the Guidelines be implemented in a one-step approach only after the transposition of the revised Payment Services Directive (PSD2)**.

This would avoid any transitional period and require changes to be made only once, rather than twice, and would give sufficient time to all PSPs and other entities affected by the Guidelines to do so efficiently.

2. General Remarks

2.1 CB welcomes and supports the open consultation process initiated by the EBA regarding guidelines related to the security of payments on the Internet.

It is felt important however to underline the sometimes ambiguous nature of the Guidelines as they are currently presented. For example :

- the Guidelines do not distinguish between different payment instruments making them particularly unclear and difficult to interpret with regard to cards and the role played by card schemes. **Making a clear distinction between the different payment instruments would facilitate the understanding and implementation of the Guidelines for card schemes**,

- throughout the document reference is made only to "competent authorities and financial institutions" being expected to comply with the Guidelines without mentioning card schemes. The role of card schemes must be clearly identified and described : for example the role they play with regard to the establishment of authentication measures, a task which cannot be left to PSPs alone,

- the fact that card schemes and the role of card schemes are not addressed directly in the Guidelines gives the impression that the essential role which card schemes play in internet payments has not been fully understood,

- although directly applicable with financial institutions, the Guidelines as proposed by the EBA would seem to apply indirectly to card schemes (through Central Banks with an oversight function on payment instruments). Since the measures and objects to be controlled would differ, this presents a risk of distortion of competition. Furthermore, in France for example, it should be noted that only security is overseen by the Central Bank (cf. article L141.4 of the *French Code monétaire et financier* [2])

2.2 Whilst recognising the essential need for security measures for internet payments, it is CB's view that the Guidelines should not be limited only to Internet transactions. **CB suggests that the scope of the Guidelines should be extended to cover all distance payments or "card not present (CNP)" transactions** such as Mail Order / Telephone Order (MOTO)

3. Rationale & Guiding Principles

3.1 CB is in full agreement with the first guiding principle outlined in the Guidelines that there should be a regular assessment of the relevant risks in providing internet payment services.

3.2 With regard to the second principle, CB believes that it is too early to take the decision that "*Initiation of internet payments as well as access to sensitive payment data should be protected by strong customer authentication*".

This opinion is not only based on the fact that the exact wording of Article 87 in the PSD2 may still change considerably, but more importantly because the context (for example the amounts involved) of such payments should also be taken into account.

Furthermore, authentication only of the cardholder by the card issuer could be sufficient if a risk analysis of the specific case is made in advance and has established, for example, that no authentication was necessary for a given transaction.

What is more, it is inexact for the EBA to state [3] that without an authentication procedure, there can be no proof. In practice there exists a whole range of indications (video-surveillance, cardholder habits, witnesses, and so on) which can provide proof of the fraudulent behaviour of a cardholder.

---

[2] www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006072026&idArticle=LEGIARTI000027782818&dateTexte=20140221

[3] From the EBA's perspective, PSPs with no or only weak authentication procedures cannot, in the event of a disputed transaction, provide proof that the customer has authorised the transaction.

3.3 CB is in complete agreement however that there is a real need to reinforce the detection of abnormal behaviour and payment patterns of cardholders, and the need to educate users of Internet payment services, as described in Principles 3 and 4 in the Guidelines.

4. The Structure of the Guidelines

The current organisation of the Guidelines is such that they are split into :

- general control and security environment
- specific control and security measures for internet payments
- customer awareness, education, communication

Unfortunately such a structure does not take into account the principle of separation (unbundling) of the payment card scheme and processing entities as set out in Article 7 of the draft Interchange Regulation, and as such the Guidelines would not comply with the Interchange Regulation.

It is recommended that the Guidelines should be reorganised to take this into account.

5. Scope & Definitions

5.1 Scope

The wording of the Scope of the Guidelines needs to be improved, since in its current form :

- it does not provide a strong or credible legal basis to show that the Guidelines would in fact apply to card schemes, since only points 4 and 8 mention "payment schemes".

- point 9 leads the reader to believe that “acquirers” or PSPs are not necessarily members of a card scheme, and should be reworded to correct misinterpretation.

- in point 10 (negative scope) an explanation is needed to understand why "browser based payments" are not excluded from the Scope in the same way as "mobile payments".

- also in point 10, the meaning of "no ongoing relationship between the issuer and the card holder” needs to be clarified, since a relationship can be ongoing without necessarily being effective at all times.

5.2 Definitions

CB would like to suggest the following improvements to the definitions

- The definition of authentication is OK, since it conforms with the PSD2 definition

- Authorisation as it is defined in the Guidelines [4] does not however have the same meaning as authorisation as it is used in the PSD2 (where it is the agreement by a cardholder to make a payment order). This is a source of confusion which must be eliminated.

- The definition of Credentials needs to be reworded. Credentials cannot mean the physical tool containing the information, but can only be the means of identifying the payment instrument or the procedure to verify the identity of the holder.

6. General Control and Security Environment

CB is in full agreement with the principles laid down in the General Control and Security Environment, with the following exceptions.

Governance : full agreement

Risk Assessment : full agreement, except that these tasks as they are currently worded only apply to PSPs.

Under which circumstances would the tasks be the responsibility of card schemes or do the Guidelines consider that card schemes not concerned by Risk Assessment ?

Incident monitoring and reporting

The reality of the situation today is that card schemes such as CB are responsible for points 3.1, 3.2 and 3.4.

However the Guidelines stipulate that it is the PSPs who have the obligation to do the incident monitoring and reporting.

Does the EBA envisage that the PSPs can delegate these tasks to a card scheme ?

If this is the case, how would the obligations and responsibilities be shared ?

[4] In the Guidelines *Authorisation* means a procedure that checks whether a customer or PSP has the right to perform a certain action, e.g. the right to transfer funds, or to have access to sensitive data.

Risk control and mitigation

Once again, nothing is said in this section concerning card schemes, and how they are positioned in relation to the PSPs

In points 4.1, 4.2, 4.3, 4.4, 4.5 and 4.6 nothing is mentioned regarding 4-Party systems and the exchange of sensitive data needed to execute a payment order.

The recommendation to terminate the contract in point 4.8 is somewhat drastic. Today's best practices would provide the merchant with a reasonable delay to rectify the situation before termination of the contract.

Traceability

It is necessary to define what is meant by e-mandate data before being able to measure the impact of obligations 5.1, 5.2 and 5.3.

Since these obligations are unclear as they relate to cards, it is recommended that a clear distinction be made between different types of payment instruments and to attribute the relevant and pertinent obligations to each one.

7. Specific Control and Security Measures for Internet Payments

CB is in full agreement with the principles laid down in the Specific Control and Security Measures for Internet Payments, with the following exceptions.

Initial customer identification, information

- Point 6.2 lists the specific details relating to internet services to be provided to the customer.

  Care must be taken that this list (in the form of guidelines with no immediate legal effect) should not affect existing legal obligations of the customer under DSP1. In particular, under PSD1 (and PSD2), the customer has an obligation to keep their personalised security device safe.

  It is recommended therefore that this list be reviewed and that a statement be made to explain how it fits in with PSD1 and PSD2.

- It should be noted that blocking a transaction for security reasons as it is described in Point 6.3 will need to take into account the resulting consequences according to the applicable regime concerning data protection. Since the Guidelines propose / support a refusal of a service (and therefore the exclusion of customer rights) it will be necessary to obtain an authorization from the competent authorities (such as the CNIL in France) before doing so.

Strong customer authentication

CB wholeheartedly supports the use of strong customer authentication as described in points 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9 and 7.10

It should be noted however that reference to card payment schemes is only made in points 7.6 and 7.7. This begs the question as to why card schemes are mentioned as prescribers of authentication measures only in those two points and not in the others ?

Furthermore **it is important that the Guidelines indicate that the card scheme must be able to approve the authentication measures and procedures which are applied to cards bearing the brand of that card scheme**.

Enrolment for and provision of authentication tools and/or software delivered to the customer

CB supports point 8.1 and with regard to point 8.2, feels that reference should be made to the PSP rather than the card issuer.

Log in attempts, session time out, validity of authentication

CB supports points 9.1, 9.2 and 9.3.

Transaction monitoring

CB supports points 10.1 to 10.5

Protection of sensitive payment data

No comment on points 11.1 to 11.3 except that as mentioned earlier under Risk Control and Mitigation, a reasonable delay should be given for the merchant to rectify the situation to avoid abusive termination of the contract.

8. **Customer awareness - education - communication**

Customer education and communication

No comments on points 12.1 to 12.5

Notifications – setting of limits

No comments

Customer access to information on the status of payment initiation and execution

No comments on points 14.1 and 14.2

About Groupement des Cartes Bancaires CB

Established in 1984 to provide a universal and interoperable card payment and ATM cash withdrawal scheme in France, Groupement des Cartes Bancaires CB is a non-profit organization acting as the governing body of the CB payment scheme.

As of November 2014, CB has 129 members, comprising both banks and payment institutions worldwide.

CB is responsible for the system's overall architecture, inter-member rules & procedures and risk management. CB also defines technical and security standards, and ensures that manufacturers and vendors whose products and services are used in the CB system comply with these standards.

Furthermore, CB operates an information system, providing its members with high performance data mining tools and countermeasures in the fight against fraud.

CB is one of the largest card payment schemes in the European Union (2013 figures) :

- 61.7 million cards
- 1.3 million merchant acceptance points and more than 58,600 ATMs
- a very significant activity, both in terms of transaction volumes and value
- 8.6 billion CB payment transactions + 1.5 billion CB ATM operations for a total value of 524.3 billion €uros

For further information

visit www.cartes-bancaires.com

✉: information@cartes-bancaires.com

☎ + 33 (0) 1 40 15 58 00