RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

SecuRe Pay

The European Central Bank published a report on the 20th April 2012 presenting a set of Recommendations developed by the European Forum on the Security of Retail Payments (SecuRe Pay) [1]

The present document presents the views of Groupement des Cartes Bancaires "CB" in response to the questions raised in the report, and where appropriate, suggests areas of improvement.

The response includes general remarks on the implications and perceived objectives of the Secure Pay Recommendations. It also outlines considerations related to the security issues covered by the Recommendations as well as the probable legal repercussions should the Recommendations be adopted in their present form.

Groupement des Cartes Bancaires "CB" would welcome the opportunity to discuss the content of this document and provide further explanation should the ECB 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

20 JUNE 2012

[1] www.ecb.europa.eu/pub/pdf/other/recommendationsforthesecurityofinternetpaymentsen.pdf

Groupement des Cartes Bancaires « CB » Response to Consultation

1. **CB welcomes and supports the open consultation process initiated by the ECB** to examine issues related to the security of payments on the Internet.

   Nevertheless, whilst recognising the essential need for security measures for internet payments, **it is CB's view that the Recommendations should not be limited only to Internet transactions**.

   CB suggests that the scope of the Recommendations should be extended to cover all distance payments or "card not present (CNP)" transactions such as Mail Order / Telephone Order (MOTO)

2. **CB is concerned that the proposed Recommendations are likely to cause a distortion of competition** both within the European Union itself and also between stakeholders within the EU and those outside.

   Examples of such situations, which must be avoided, are given below

   - Firstly, within the EU, a ''level playing field'' will depend on the existence of an enforcement process for the various Recommendations and the delay permitted by the Regulators in each individual Member State for conformity to be achieved. A situation whereby the Recommendations become obligatory for regulators in certain Member States, and not for others, will not guarantee equality of treatment for those Card Schemes, PSPs and e-merchants which do, in fact, conform with the Recommendations
   - and secondly, outside the EU, where a ''level playing field'' will depend on actions by non-EU Regulators to enforce security measures, the European Regulators have an essential role to play in achieving this goal, by actively promoting and coordinating identical measures with their international counterparts.

3. **CB would like to emphasise that it is vital that any compliance process** which is implemented by National Central Banks (and in its own case, the Bank of France) to measure the conformity of Card Schemes with the Recommendations, **should be strictly limited to the provision of a minimum amount of documentation and elements of proof**.

   CB also considers that the Recommendations should :

   - **focus on an obligation to produce a result, and not the means of obtaining the result**, and
   - **be technologically independent**, and avoid prescribing specific technical solutions,

4. **CB would like to stress the importance of including measures which address the issue of "cross-contamination" in the Recommendations;**

   An example of cross-contamination is the use of only the card number and validity dates to carry out a distance payment with a card;

   Determined action is needed to prohibit such practices, and a Recommendation, or at least a Key Condition and Best Practice dedicated to this issue, should be included.

   What is more, the European Central Bank should undertake concerted action with its international counterparts to accelerate the implementation of measures to fight against cross-contamination as an item of utmost importance in the worldwide fraud prevention agenda.

5. A number of observations can be made from a legal standpoint

   5.1 A general observation is that the **content of the text of the proposed Recommendations is of a composite nature**, covering, in fact, issues of technical security, aspects related to information to be provided to users of payment instruments, as well as questions related to the protection of personal data. Because of this, and taking into account the fields of competence recognised by French legislation, the competent authorities in France are at least 3 in number : la Cnil, l'ACP and the Bank of France.

   The supervisory body under which the Recommendations will be implemented must be clearly defined.

   5.2 **The nature of the text is also composite**, since it contains recommendations, key considerations and best practices, and the mandatory nature of the three different requirements is unclear. This is further emphasized by the fact that mention is made, sometimes with, and sometimes without, reference to articles (or extracts of articles) in the Payments Services Directive (PSD) [2].

   This begs the question as to how the text is positioned with regard to existing French laws and European legislation (Directives with full or total harmonization or even a Regulation) dealing with the same subject matter.

   Introduction of the Recommendations must not create legal uncertainty,

   5.3 **The strength of enforcement of the Recommendations is unclear**, as is the interpretation of the term "recommendation".

   Should the term be interpreted as in European Constitutional Law ?

[2] Payment Services Directive : see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:01:EN:HTML

If this is the case, is a forum of Central Banks and other Supervisory Authorities and Overseers authorised to create such a text ?

And if so, when integrated into a national law, how would the Recommendations accommodate article 86 of the Payment Services Directive which describes *expressis verbis* the areas where Member states are allowed to maintain or introduce provisions other than those laid down in the PSD ?

In other words, how can members of a forum, for which the statutes are not foreseen in the European Treaties, make the proposed Recommendations binding for national or European legislators ?

5.4 In any event, **there is already a great deal of overlap between the text in the SecuRe Pay Recommendations, and existing laws and Directives.**

Following a brief analysis of the current situation in France, Key Considerations (KC), Best Practices (BP) and Recommendations which overlap with existing legislation are listed below. Similar illustrations can no doubt be found, not necessarily to the same degree, in other Member States.

5.4.1 Overlap with the Loi Informatique et Libertés [3]

- KC 1.2, KC 2.3,
- Recommendation 3 and the planned European Regulation on the protection of personal data which includes an article requiring that authorities which are responsible for the protection of personal data be notified of major incidents concerning personal data (an example of which is a card number),
- KC 3.2, KC 3.3, KC 4.2 , KC 4.3 KC 5.1, KC 5.2 KC 5.3, KC 7.2,
- Recommendation 10 seems to be contrary to a requirement (in the Loi Informatique et Libertés) never to take a decision based on a single data processing process
- KC 11.1 , KC 11.2, KC 11.3, BP 11.1

5.4.2 Overlap with the Code Monétaire et Financier [4]

- Recommendation 6 (Customer Identification)
- KC 6.1 adds a condition to articles L133-6 1 and L 314-12 II of the Code Monétaire et Financier

[3] Loi Informatique et Libertés : see www.cnil.fr/en-savoir-plus/textes-fondateurs/loi78-17/

[4] Code Monétaire et Financier : see www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006072026

- KC 6.2 also adds to article L314-12 II
- KC 6.3 appears to add a new condition which would bring about the application of article L 133-10 (i.e. the need to inform the user before blocking his/her card)
- KC 6.4 is different to existing article L 314-12
- BP 6.1 (identification of user before granting access to internet payment services) is totally new, and would add an unforeseen obligation
- KC 7.3 adds a necessary consent by the user concerning the authentication procedure
- BP 10.2 is different from the existing article L133-10
- Recommendation 12 : KC 12.1, KC 12.2 , KC 12.3 and KC 12.4 drastically increase the burden on PSP's and their obligations to provide information to users.

5.4.3 **Overlap with the Payment Services Directive**

- KC 6.1 adds to article 42 of the PSD by requiring that a user must identify themselves before being able to access a service
- KC 6.2 provides an additional list of documents to be provided to users of payment instruments
- KC 6.3 adds a new condition which would bring about the application of article 55.3 of the PSD,
- KC 6.4 describes "instructions" and not "information" (which appears to be different : cf. article 42.5a)
- BP 10.2 is not exactly identical to the obligation which figures in article 55.3
- Recommendation 12, KC 12.1, KC 12.2, KC 12.3 and KC 12.4 increase the burden and obligation to provide information which figures in article 42 of the PSD.
- KC 13.1 and BP 13.1 modify the finality of the spending limit as described in articles 42.2 and 55.1

5.5 Definitions

5.5.1 It is recommended that the definitions in the Payment Services Directive be used in future versions of the Recommendations (to avoid incoherence, examples of which are given below).

- For example what is the meaning and impact of the notion of **"strong customer authentication "** compared with **"personalized security features of a payment instrument"**

This may lead to a different **interpretation of article 61 .3 of the PSD** which provides for Member States to be able to limit the liability of the Payer, by taking into account, in particular, the nature of the personalized security features of the payment instrument

- In the same way, **article L 133-4 of the French Code Monétaire et Financier defines "** le dispositif de sécurité personnalisé (i.e. **personalized security feature**) " as including **"any technical measure carried out by a Payment Service Provider (PSP) for the use of a payment instrument by a given user "**

  The purpose of this feature / device, which is specific to a given user of a payment service, and under the user's safekeeping, is to attempt to authenticate the user.

  It appears however that there is a difference between these dispositions, and the principle of strong authentication in 3D Secure does not correspond to this terminology.

5.5.2 The terminology used (such as Key Considerations, Best Practices, ...) must be appropriate and avoid introducing uncertainty and room for misinterpretation.

Are Key Considerations and Best Practices interchangeable or are they complementary?

6. **Scope of the Recommendations**

Even if it is understandable that certain payment instruments are excluded from the scope of the Recommendations since they are governed by other Supervisory Authorities, the document should be more precise. Many of the statements referring to card schemes may also be valid for other schemes used for payment on the Internet, in which case the other schemes should be included.

In any event, concerted effort should be made to guarantee that payment instruments and payment organisations which are excluded from the scope of the Recommendations will be subject to identical or similar obligations in terms of security as those which fall within the scope.

7. **An implementation date of 1 July 2014 appears, at this stage, to be rather ambitious**.

8. and finally, since security in the payment value chain depends on its weakest link, **CB trusts that the Authorities will be vigilant and make sure that each and every player in the European payments market applies and complies with the Recommendations when finally established**.

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 January 2012, CB has 128 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 (2011 figures) :

- 60 million cards
- 1.2 million merchants and more than 58,000 ATMs
- a very significant activity, both in terms of transaction volumes and value
- 7 billion CB payment transactions + 1.6 billion CB ATM operations for a total value of 482 billion €uros

For further information

visit www.cartes-bancaires.com

✉: information@cartes-bancaires.com

☎ + 33 (0) 1 40 15 58 00