centro de cooperación interbancaria

20 de junio de 2012

Content analysis of the entitled ECB document

Recommendations for the security of internet payments, vers. April 2012

Prepared by the computer security group of CCI

Location and content	**Comments and Observations**
Guiding principles *... strong customer authentication is a procedure ...*	It would be advisable to define, depending on the type of payment, as precisely as possible the taxonomy of the combined factors that would meet the customer requirements for strong authentication procedure.
Guiding principles *... the internet payment services ... should be initiated by means of strong customer authentication.*	The CCI working gruop considers necessary to keep in mind, as stated by SEPA legislation (principle of the four corners), that the intervention of the PSP may not occur at the beginning of the transaction or at the verification of the customer´s payment.
Recommendations 2.3 *The assessment of risks should address the need to protect and secure sensitive payment data, ...*	It would be advisable to define, depending on the type of payment, in a concrete way the data to protect and the methods used for such protection and securing
Recommedations 4.5 *The PSP's security measures for internet payment services should be periodically audited to ensure ... The implementation and functioning of the internet services should also be audited.*	It would be advisable to define the conditions to be met by experts as well as the scope and frequency of the audits.
Recommendations 5 *Traceability*	To ensure proper traceability, recommendations at EU level should harmonize, and recommendations about the specific data that must be saved should incorporate to this document (Identification, Authorization, Approval or Signature, Confirmation), as well as conservation condition, and a timeframe.
Recommendations 7.2 *Obtaining access to or amending sensitive payment data requires strong authentication*	A more specific definition of "sensitive payment data" would help to implement the recommendations of this document.

centro de cooperación interbancaria

20 de junio de 2012

Content analysis of the entitled ECB document

Recommendations for the security of internet payments, vers. April 2012

Prepared by the computer security group of CCI

Location and content	**Comments and Observations**
Recommendations 6 *Customers should ... confirm their willingness to conduct internet payment transactions before being granted access to such services.*	The CCI working group considers that the purpose of this recommendation will be developed in the clauses of the contract which confer the means of payment. Without prejudice that further action could be defined in a more specific way.
Recommendations 10.1 *PSPs should use real-time fraud detection and prevention systems to identify suspicious transactions, for example based on parameterised rules ..., abnormal behaviour patterns of the customer ..., sometimes identified (... geolocalisation ...) and known fraud scenarios.*	It is necessary to carefully analyze the implementation of these measures on knowledge refered to the customer activities and the consequences that result from the relationship with him, the impact on the respect of the privacy policy, and all the safeguards required by the law. So that the use for these purposes must be legitimized (by the legislation itself).
Recommendation 12.4 *PSPs ... should initiate customer education and awareness programmes designed to ensure customers understand, ...*	It is necessary to define the scope of the "customer education" and "awareness programmes", and how to ensure that they take place.
Recommendations 3.2 *PSPs and card payment schemes should ... notifying the competent authorities ... immediately in the event of major incidents ...*	It is necessary to define what is considered "a serious incident".
Annex I, paragraph II *THE LEGAL FRAMEWORK FOR REPUDIATION AND RELATED LIABILITIES WITH RESPECT TO TRANSACTIONS VIA THE INTERNET SHOULD PROVIDE SUFFICIENT CLARITY TO ENHANCE TRUST IN THESE PAYMENT*	The CCI working group highlights the importance of harmonizing the EU legal framework with respect to the "burden of proof" and "liability limits" related to each of the participants in an operation. An arbitration service would facilitate the resolution of disputes.

NOTE: With respect to card payments, the information contained in the document is covered in more detail by the PCI-DSS regulations, except for what related to: double-factor authentication, customer education and awareness programmes and the verification of the implementation of customer payments.

--- 00000 ---