

COMMENTS

Subject: Security of Internet Payments

I. General Comments

This document talks about the implementation of the "guidelines" of the EBA on internet payments security, prior to the transposition of the Directive on payment services (PSD2).

Before answering the question posed in the document in consultation, we would like to make a few remarks on the subject in question:

1. The protection of privacy, personal data and security of online payments, aka the Internet, are increasingly important consumer issues.

If traditional payments already pose a serious set of safety issues, the transactions in online media (internet) are even more vulnerable to potential security breaches and theft of personal data, beyond the issue of omission information, to the prior and necessary clarification consumer information.

2. The guidelines set out in the document translated into a common set of minimum requirements for measures to be implemented in payments over the internet, claiming to safeguard, at appropriate levels of security, all phases of the procedure, namely the importance of identifying risks and safeguard security as the intervention of third parties; protecting access to sensitive payment data for authentication; the implementation of protection of sensitive data mechanism (for this purpose) when they are transmitted, processed or stored; authentication procedures and transactions to provide consumers with adequate on this type of transaction information.

3. We agree with the general framework made of the main measures to be implemented and with the interests to protect, in particular security and consumer privacy, and evaluation of the risks associated with online payments to be updated regularly to keep up with the most modern and advanced technologies and mechanisms to protect the user.

However, the same document doesn't point, as possible, specific technical solutions or technical standard behaviors to adopt by operators or equipment manufacturers.

4. Perhaps our mistake, but we do not see any reference in the document about the criteria of "liability for unauthorized transactions". We have consistently argued in this regard that any regulatory system will create a system to ensure effective reimbursement to the consumer, if any incident occurring during the payment transaction, not chargeable to the consumer.

5. The "guidelines" refer the strengthening of consumer information. We totally agree with the principle that it is necessary to educate and inform consumers about which are the risks, characteristics of service, the existing defense mechanisms and rights they have.

But also understand that the duty to inform the consumer should not, or can't be turned into a weapon to his prejudice, including taking accountability for the consumer beyond what is acceptable for you information has been provided.

The consumer is not a technical expert in communications and IT, and can't be held liable beyond what should reasonably be expected of him after the information that has been provided.

6. Another point that seems important about the "incident monitoring and reporting" is not clear in the document: it is also essential to ensure customer notification in case of breach of data security (Breaches date) and not just the police.

In the remainder, we agree with the guidelines.

II. Question consulted:

b) We prefer a one-step approach, anticipating the implementation of the measures in PSD2 including them in the action to have come into force on August 1, 2015.

Knowing yourself in advance what changes will be promoted by PSD2, then the guidelines of the EBA should contemplate these changes, for the avoidance of two distinct phases of adaptation.

We believe that the banking system has a sufficient time to prepare what is necessary and, from the point of view of the consumer, it is certainly easier to assimilate.

In summary we argue that it is necessary to ensure that:

- Payments are made with the greatest possible safety for consumer's, avoiding frauds that damage consumers.
- In case of fraud, other than under the negligent use, the consumer shall not be liable for damage caused by the use of such means of payment and should be returned for any amount it has been wrongly debited.
- The protection of personal data and access to bank accounts should be a priority, so there is no possibility of third parties remain in possession of data that could potentially be used to the detriment of the consumer.