Collis

MEMO

De Heyderweg 1
2314 XZ Leiden
The Netherlands
Tel: +31 71 581 3636
Fax: +31 71 581 3630

From	Mark Baaijens (Collis) *baaijens@collis.nl*
To	ECB *ecb.secretariat@ecb.europa.eu*
Date	16 mei 2012
Subject	Remarks on the document "Recommendations for the security of internet payments" (April 2012 version)

We believe that the concerning document is very valuable to all PSPs. However we have some remarks which are described below.

Scope and definitions

It is not clear whether pay after delivery solutions are in scope. In our opinion a somewhat different set of recommendations is required for pay after delivery solutions, so these kinds of payment solutions should be out of scope for this document. For example, recommendation 12 is not applicable to all pay after delivery solutions. On the other hand, there should be a recommendation for pay after delivery solutions to have a reasonable period of time for doing the payment before a fine should be paid.

An explicit definition of Payment Service Providers (PSPs) is needed. For the definition PSPs the document makes a reference to the Payment Service Directive (PSD), but the PSD doesn't incorporate an exact definition of a PSP. Often a PSP is referred to as the party which has a contractual relation with the merchant in order to offer different payment methods on their website and/or take over some credit risks. However, within this document, we assume, a PSP is the party offering a payment service to the payer. Different recommendations imply a contractual relationship between the payer and the PSP (i.e. Recommendations 6, 7, 8, 9 and 12).

Non-repudiation

We recommend incorporating more advice regarding the implementation of non-repudiation controls, as this security asset is often underestimated by financial service providers. In the current document, non-repudiation is limitedly covered within the recommendations. The traceability recommendation (i.e. Recommendation 5) should be extended with the notion that the transaction data should be strongly bind to the authentication data. The PSP should be able to present these pieces of data as well as their relation at the time of a dispute. Furthermore a PSP should be able to show that this data is untampered with by means of, for example, valid security procedures. Next to that, a PSP should ensure that all the details of a financial transaction are shown to the payer in a trusted manner before the authorization is done (Sign What You See).

Within the Guiding Principles it is implicitly stated that strong authentication implies good non-repudiation characteristics. However it is not strong authentication itself that provides "the proof that the customer has authorized the transaction". Only the use of a mechanism that strongly binds the transaction details to the agreement data (e.g. the authentication data) will provide this proof. Such a mechanism is, for example, provided challenge/response authentication.