BANKA SLOVENIJE
EUROSYSTEM

BANK OF SLOVENIA
Slovenska 35
1505 Ljubljana
Slovenija
Tel.: +386 1 47 19 000
Telex: 31214 BS LJB SI
Fax: +386 1 25 15 516

EUROPEAN CENTRAL BANK
Secretariat Division
Kaiserstrasse 29
D-60311 Frankfurt am Main
Germany

Via e-mail: ecb.secretariat@ecb.europa.eu

Ref : 29.50-0207/12-JK
Date: 20 June 2012

Subject: **Response to public consultation on the Recommendations for the security of internet payments**

Dear Sirs,

On 24 April 2012 Banka Slovenije informed all relevant national stakeholders and their associations on the launch of the public consultation on the respective recommendations.

With respect to that, one entity (Chamber of Commerce and Industry of Slovenia) provided opinion on the recommendations directly to Banka Slovenije. Therefore we would like to hand over the received response to the ECB (as attached).

Best regards

mag. Peter Centrih [signed]
mag. Simon Anko [signed]
Payment and Settlement Systems

Annex 1: Opinion of Chamber of Commerce and Industry of Slovenia (*English version*)
Annex 2: Opinion of Chamber of Commerce and Industry of Slovenia (*Slovenian version*)

Annex 1:

CHAMBER OF COMMERCE AND INDUSTRY OF SLOVENIA
Response to the ECB public consultation on the Recommendations for the security of internet payments

Recommendations for the security of internet payments have been examined closely by the Section for information security management, acting within the Chamber of Commerce and Industry of Slovenia (Central Slovenian region).

During the review of the document with the Recommendations for the security of internet payments (April 2012), we found that in the respective recommendations all adequate controls are covered and existing best practices in that field are considered.

However, we would like to stress the following issues:

- in our opinion, it would be good to define in detail the "major incident" from chapters 2.4 or 3.2, since both chapters represent obligation of payment service provider (PSP). That would as well prevent the PSPs from avoiding responsibilities;
- we support PSP's obligation to ensure the procedure for authorisation of transaction, which includes unusual (out of subsistent, so far existing, regular business) behaviour of the service user – as stated in basic principles on the page 6. Provision from chapter 13.3 providing for protection of individual's privacy, according to which the user "can" specify personalised rules for behaviour with regard to internet payments, should be changed into "has to" (if PSP already ensures that sort of tracking of behaviour). Respectively, PSP should not perform that kind of monitoring without the user's permission;
- in our opinion, dissemination of sensitive data on a user is sufficiently determined (referred to in chapter 14.2), as non-anonymized data should not be included in turnover and account statements of a user.

Annex 2:

GOSPODARSKA ZBORNICA SLOVENIJE
Odziv na javno posvetovanje ECB o priporočilih za varnost spletnih plačil

V Sekciji za upravljanje varovanja informacij (SUVI), katera deluje znotraj GZS-Zbornice osrednjeslovenske regije smo pazljivo preučili priporočila za varnost spletnih plačil.

Ob pregledu materiala Recommendations for the security of internet payments (april 2012) smo ugotovili, da so navedena priporočila zajela vse primerne kontrole oz. da so upoštevane dosedanje dobre prakse tega področja.

Opozorili pa bi na naslednje:

- menimo, da bi bilo dobro, če bi se v dokumentu podrobneje opredelilo, kaj pomeni "večji" incident (major incident) - zapisano v poglavju 2.4 ali 3.2, saj oba poglavja predstavljata obvezo za PSP (Payment Service Provider) in tako ne bi bilo možno "izogibanje" z njegove strani;
- nič ni slabega, če je določeno, da je PSP dolžan zagotoviti procedure za avtorizacijo transakcije vključujoč tudi "nenavadno" (izven obstoječega, dosedanjega, rednega poslovanja) obnašanje uporabnika storitve - osnovni principi na strani 6. Varovalka, ki preprečuje, da bi tako določilo vodilo k zlorabi zasebnosti posameznika je vgrajena v 13.3, kjer je določeno, da uporabnik lahko (predlagamo, da se ta varovalka spremeni v MORA, če PSP že zagotavlja tako sledenje obnašanja) opredeli osebna pravila svojega "obnašanja" oziroma plačevanja po internetu - oziroma, da PSP brez njegove privolitve takega spremljanja ne sme uporabljati;
- tudi izkazovanje občutljivih podatkov uporabnika je dovolj dobro opredeljeno, saj v poglavju 14.2 določa, da taki podatki (neanonimizirani) ne smejo biti prikazani v izpisku prometa in stanja za uporabnika.