Association of Latvian Commercial Banks
Pērses street 9/11, Riga, V-1011, Latvia
Phone +371 67284528, fax +371 67828170
E-mail: asoc@bankasoc.lv
www. bankasoc.lv

RIGA

20 June, 2012 No. 1-27/133_e

European Central Bank
Secretariat Division
Kaiserstrasse 29
D-60311 Frankfurt am Main
Germany
E-mail: ecb.secretariat@ecb.europa.eu

ALCB RESPONSE TO THE EUROPEAN CENTRAL BANK CONSULTATION

THE "RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS"

This submission is made on behalf of the Association of Latvian Commercial Banks. The Association of Latvian Commercial Banks (ALCB) is a public organization, uniting on voluntary principle the banks registered in Latvia and branches of foreign banks. It was founded on July 23, 1992. The purpose of the Association is to contribute to strengthening and developing the banking system of Latvia.

- **Recommendation 4**
  4.7 KC PSPs offering acquiring services should require e-merchants to implement security measures on their website as described in this recommendation.

  ALCB: PSPs should not take the responsibility of the level of security provided by the other process stakeholders including e-merchants. PSPs currently don't have a legal right to require and check the fulfilment of such security requirements.

- **Recommendation 7**
  Internet payment services should be initiated by strong customer authentication.
  7.1. KC Strong customer authentication is a procedure that enables the PSP to verify the identity of a customer. The use of two or more of the following elements – categorised as knowledge, ownership and inherence – is required:
  – something only the user knows, e.g. password, personal identification number;

– something only the user possesses, e.g. token, smart card, mobile phone;

ALCB: It seems that it will be not possible to use code cards with rotating (repeatedly used) codes. If yes, then such requirement is overstated because it does not intend to take into account additional risk mitigating solutions and factors (as limits) being used together with such code cards.

- **Recommendation 8**
  The PSP should ensure that the enrolment for and the initial provision of strong authentication tools required for the internet payment service is carried out in a secure manner.
  Personalised security credentials and all internet payment-related devices and software enabling the customer to perform internet payments should be delivered securely. Where tools need to be physically distributed, they should be sent by post or delivered with acknowledgement of receipt signed by the customer. Software should also be digitally signed by the PSP to allow the customer to verify its authenticity and that it has not been ampered with. Moreover, personalised security credentials should not be communicated to the customer via e-mail or website.

  ALCB: It is not fully clear from the recommendation text, if the ordinary letter sent by post can be still used for the distribution of authentication tools.
  The recommendation states that personalised security credentials, such as one-time password, can't be delivered to the customer via e-mail, does that mean that it can be communicated via mobile phone or sms?
  If the personalised security credentials should not be communicated to the customer via website, will it still be possible to offer password change via website?

- **Recommendation 9**
  9.3 KC PSPs should set down the maximum period after which inactive payment sessions are automatically terminated, e.g. after ten minutes.

  ALCB: Our experience has proven that very detailed and particular requirements are not effective, because each risk and threat evaluation should be done based on the specific individual situation, taking into account additional risk mitigating factors and used technological solutions.

- **Recommendation 10**
  10.1 KC PSPs should use real-time fraud detection and prevention systems to identify suspicious transactions, for example based on parameterised rules (such as black lists of compromised or stolen card data), abnormal behaviour patterns of the customer or the customer's access device (change of Internet Protocol (IP) address or IP range during the internet payment session, sometimes identified by geolocation IP checks, abnormal transaction data or e-merchant categories, etc.) and known fraud scenarios. The extent, complexity and adaptability of the monitoring solutions should be commensurate with the outcome of the fraud risk assessment.

ALCB: Current regulation doesn't set this as a requirement for PSPs, therefore such security systems, that allow to identify and block suspicious transactions according to the defined complicated criteria of fraud are not in use. Such systems, expensive and requiring particular resources, are being used for monitoring cards transactions, but not the i-payments. We have a serious concern about ability to fulfil the requirement about the use of such systems by the July 2014.

- **Recommendation 14**
  14.1 KC PSPs should provide customers with a facility to check transactions and account balances at any time in a secure environment.

  ALCB: PSPs already comply with the recommendation, however the requirement isn't set in any rules or regulation. Facility to check transactions and account balances is one of basic services on the market that customers require. Therefore such requirement seems to be self-evident and there is no need to include it in the market regulation.