To:

European Central Bank
Secretariat Division
Kaiserstrasse 29
D-60311 Frankfurt am Main
Germany
Fax: +49 69 1344 6170
E-mail: ecb.secretariat@ecb.europa.eu

Sent via E-mail to: ecb.secretariat@ecb.europa.eu

Comment on the draft

"Recommendations for the security of internet payments"

Svenska Handelsbanken welcomes the initiative to give guidance on security within the area of internet payments.

These recommendations should apply to all stakeholders involved in the internet payment chain not only to PSPs. Also other involved parties like e-merchants and parties labeled as "third-party access" should be covered. The suggested limitation of the scope would reduce the value of the recommendations since important parties and businesses securing vital parts of the value chain in practice would be excluded, such as:

- transfers of electronic money between two e-money accounts;
- credit transfers where a third-party accesses the customer's payment account;
- redirections, i.e. where the payer is redirected to the PSP by a third party in the context of a credit transfer and/or direct debit, the redirection itself is excluded. "redirections" must be clearly defined and understood by all involved parties including the consumer, so that they not behave similar to Trojans, attempting to compromise the customer. E.g different types of overlay services.

These recommendations should include all players and means of payments in the internet payment area. By excluding non regulated participants in the payment process, the suggested recommendations would introduce risk for regulated payment service providers. The general reference to the PSD legal framework adds limitation of scope when it by definition excludes non-regulated participants in the payment process and value chain. The consequence of excluding some participants leads to an informed decision of adding a weak link to the value chain and thereby adding risk to the regulated part of the value chain. From a business perspective it will not lead to a level playing field and sound competition amongst payment service providers to compete. On the contrary it leads to an ability to compete by offering lower security levels. In our view, competition between different means of payments should not be made possible by using poor security. From a consumer perspective you could -maybe unaware- be set into a lower degree of security and level of consumer protection then you are entitled to. This is rather contradictive to the aim of these recommendations.

In some respect you address this issue in Annex 1 as a point to consider in the review of the PSD in point 1). But you are in that context only referring to "acquiring services" where the review of the PSD should include both sides and all participants of the payment process.

In Annex 1 point 4) you are covering the review of the scope of the PSD. You analyse and position that "The Forum believes that where a payer's PSP is located in the EU/EEA, this alone should bring the transaction under the scope of the Directive. A customer's liability for fraud should not be dependent on the location of the payee's service provider."

You state that "a customer's (payer's) liability for fraud should not be dependent on the location of the payee's service provider". The consequence of this statement is that a PSP for an EU/EEA payers' payment will face an

uncontrolled business risk for one leg transaction, if not the responsibilities for the counterpart is regulated. A legal framework should not introduce more uncontrolled risk for regulated PSPs. For this reason this statement should be re evaluated.

This issue is solved for card transactions as the participating parties rules and regulations cover the business rules for the payer and the payee through their respective payment service providers' relation in the inter bank – or inter payment service provider – area globally.

These consequences have an impact on several Key Considerations regarding specifically risk evaluation.
Key Considerations with relevance to above:
1.2, 2.1, 2.3, 4.2, 6.2, 7.1, 7.2,

These recommendations should be limited to security recommendations. They should not contain any considerations regarding remedies in case of disputes. Such considerations have to be discussed separately since all member states don't have the same legal systems in this respect.
Please see:

- [page 6 second paragraph]
- 6.1 BP. PSPs should decide how their contractual arrangements with the customer are organized.

Maintaining a high standard of security is the responsibility of all involved parties. The recommendation 2.1 KC should include that the customer should be responsible for protecting their computer environment and their means of authorization.

A clarification should be made regarding Apps. We consider Apps belonging to this domain and would like it to be more clearly specified within these recommendations.

The organisation of a company is different due to many different factors. These recommendations should not include organisational aspects of security implementation. Please note 4.4 KC, how testing is organized should be up to the PSP to decide.

As previously stated major incidents should involve reporting. This should also apply for recommendation 3.3 KC and be applicable for major breaches.

In recommendation 7, it is stated that PSPs could consider adopting less stringent customer authentication for outgoing payments to trusted beneficiaries included in previously established "white lists", i.e. a customer-created list of trusted counterparties and beneficiary accounts with strong authentication. We consider a PSP created "white list" to be more secure and these recommendations should include possibilities for PSPs to create white lists, in order to allow less stringent customer authentication.

All recommendations should be restricted to technology independent security requirements.

Svenska Handelsbanken
Att: Johan Wadmark
CCS
S – 106 70 Stockholm
Sweden
Email: jowa05@handelsbanken.se