Svenska
Bankföreningen
Swedish Bankers' Association

**POSITION PAPER**



20/06/2012

European Central Bank
Secretariat Division
Kaiserstrasse 29
D-60311 Frankfurt am Main
Germany

ecb.secretariat@ecb.europa.eu

# Recommendations for the Security of Internet Payments – April 2012

## General comments

Great care must be taken not to harm European competitiveness on the global payment market. E-commerce, Internet payment and the card payment market has a global reach. If stricter rules are applied to European e-merchants there is a significant risk that e-commerce in Europe is harmed. It must be ensured that customers do not perceive that rules that apply to European merchants and payment service providers make the service less attractive or less user-friendly if there is no perceived change in risks or responsibility. We believe that security measures preferably should be coordinated on a global level. If licensed payments institutions in Europe still bear all the risks associated with a payment that is executed outside the European market, where security measures might be less stringent, this surely creates a situation which would be detrimental to the development of innovative e-payment solutions.

Security measures must be implemented in a uniform manner for all participants in the payment chain in order to ensure a level playing field. The same rules should apply to both licensed and non-licensed institutions who engage in the payment infrastructure. We believe it is important to address the security issues that arise out of the activities of third parties including so called Overlay Payment Service Providers. It must also be ensured that rules are implemented on a similar basis in

Besök (Visit):
Regeringsgatan 38
Stockholm
Sverige (Sweden)

Post:
Box 7603
SE-103 94 Stockholm
Sverige (Sweden)

t: +46 (0)8 453 44 00
f: +46 (0)8 796 93 95
e: info@swedishbankers.se
www.swedishbankers.se

the respective countries. Recommendations should not go into too much detail on technical issues and should preferably be implemented as Best Practices, where "implementation" can be coordinated via appropriate standardization and payment organizations both in Europe and globally.

**Specific comments**

*Definitions and glossary of terms*

- There is a need to define "customer". It is not clear if also companies are in scope.
- It needs to be further clarified what "…elements selected must be mutually independent," refers to in the section called Guiding Principles.

*Comments on Recommendations*

Recommendation 4:

4.4 KC. We believe the text about tests is too detailed.

4.7 KC. The document should not mix rules that are applied for e-merchants and PSP. E-merchant rules should be described separately.

Recommendation 6:

6.3 KC. The text about on how customers are able to block or unblock transactions or services is to detailed, which could harm the development of innovative solutions.

6.1 BP. Each institution should be able to decide how they organize their contractual relationship with the customer.

Recommendation 7:

7.1 KC. At present, strong authentication benefits cannot justify its costs in some countries. We suggest having other risk mitigation possibilities, such as low cumulative transaction limits, subject to risk analysis. Furthermore there are risks for other fraud attacks post authorisation but prior to final payment to consider. There is also a need to clarify what "bundled transfers" refers to.

7.2 KC. We do not believe it is clear enough what "sensitive data" refers to.

7.3 KC. 3DSecure is a proprietary Visa Inc property and should not be mentioned here. Nor should there be a need for prior customer consent for internet payments from all cardholders in Europe. The recommendation mentions the necessity to pre register all cardholders in a 3DS directory when cards are issued assuming that all cards/card holders should be connected to internet payment services. It must however be possible for a PSP to offer cards without internet payment

capability and it must also be possible for cardholders to opt not to use cards on the internet. If so, there is no need to pre-register ALL cards in a directory for internet purposes.

7.6 KC. Liability shifts were very effective measures to ensure stronger authentication in payment schemas around the world. However it is important to understand that liability shifts do not work in global markets due to the fact that some regions do not implement them. ECB should call for ensuring similar liability shifts in other, non-European markets. The requirement on liability shift should state from issuer to acquirer since normally the merchant does not have any relation to the issuer of the card.

Recommendation 8:

8.2 KC. The word "exceptional" should be deleted. Bypassing of strong authentication by the cardholder should not be allowed.

Recommendation 10:

10.1 KC. The term "real-time" needs to be defined. It should not be expected that "real-time detection" can be used for any type of monitoring. The text goes too much into detail, i.e. referring to "geolocation IP checks" etc.

Recommendation 12:

We believe the text about customer education goes too much into detail. The PSP cannot be responsible for the customer/client PC but can give proper advice.

Recommendation 13:

13.1 KC. Managing spending limits should be left to responsible market players in relation to their customers. At least, the words "prior to" should be deleted. It should be allowed to use the concept of "default limits", to be changed by the customer after enrollment to a service.

*Annex 1*

We would welcome a harmonization of the implementation of article 61.3, which has led to very dissimilar liability regimes in the different Member states. We are also somewhat surprised that the Swedish implementation of article 61.3 is not mentioned in the text and/or footnote.

As regards the scope of the directive we are strongly in favour of keeping the rules applicable only where the PSPs of both the payer and the payee are located in the EU/EEA and where the transaction is in euro or in the currency of a non-euro area Member State. An extension to so called leg-out transactions would be very far-reaching and would cause serious concerns for the banks. There is no possibility for the banks to include in the conditions i.e. maximum execution times for a

payment in all currencies to every other country in the world as well as guarantee payments D+1.

SWEDISH BANKERS' ASSOCIATION

Johan Hansing

Lars Rutberg