PAN-Nordic Card Association
Business Adress:
PNA Card Service AB
Skomakaregatan 6, 2 trp, S-211 34 Malmö
Phone +46 (0)40 2507 78
Fax +46 (0)40 2507 79
e-mail mail@pan-nordic.org
homepage www.pan-nordic.org

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

18 June 2012

Forwarded via E-mail to:

ECB.SECRETARIAT@ECB.EUROPA.EU

PAN-Nordic Card Association (PNC) welcomes the European Central Bank initiative of launching recommendations for the Security of the Internet - and hereby submits our view on the recommendations.

PNC represents all the Banks in Sweden, Norway, Denmark and Finland active within international card issuing business and/or card acquiring business.

Our response reflects the view of our member banks active in general card business domestically and cross border in the Nordic Region of the European Community.

The response is divided in a section with general comments and a section with comments to specific recommendations with reference to the individual recommendation – KC or BP.

General Comment:

The PNC welcomes the initiative to publish security measures for internet payments but would like to draw your attention to the fact that internet payments and the security requirements accustomed to it is a truly international problem and not a problem isolated to the EU. Furthermore, the total level of security depends on the weakest link and, in that sense, the PNC strongly supports that the security rules not only should apply in Europe, but should be enforced internationally.

Therefore, it is of utmost importance that recommendations regarding required security measures are agreed upon and implemented internationally and not only in the EU. Recommendations enforced only by European supervision and oversight bodies would not necessarily apply to non-European players which could be detrimental to a level playing field and security.

We find that your recommendations in general are in line with the requirements from Payment Card Industry, Data Security Standard (PCI-DSS), which most international card schemes stands behind, whereas we would recommend that the ECB take initiative to a close cooperation with PCI in order to secure total alignment of the recommendations from ECB and the PCI DSS requirements. All involved parties in internet payments are aware of the costs of security and a close cooperation with PCI would secure that investments in security only has to be done once in order to comply with international standards.

It is very important that all rules apply to all players involved in the internet payment chain, not only to PSPs but also to e-merchants, non-regulated service providers, etc. when relevant. This is exactly the case in regard to the PCI requirements.

No matter whether it ends with international requirements or EU only recommendations it is necessary that national supervisors and overseers apply, interpret and enforce the proposed security measures in a uniform manner, thereby creating a level playing field, a consistent consumer experience and an environment conductive to the development of internet payments. This will be very problematic if the recommendations are European and not internationally based.

In addition, many players essential for the security of payments (e.g. Overlay Service Providers and non-licensed institutions), are currently not subject to supervision and oversight. All providers of e-payment services should be subject to oversight and supervision.

International as well as EU Rules on security measures should be consistent with other regulated domains such as cybercrime, data protection, anti-money laundering, etc.

The implementation must also take into account, that a number of initiatives are ongoing covering partly or entirely same issues, such as:

1. The e-Commerce Directive
2. PSD-revision
3. E-Money Directive and the 2nd e-Money Directive
4. Proposal by the Commission for EU Data Protection Regulation (January 2012)
5. SEPA – supported by the work of PCI and OSec
6. EMV and EMV Next Generation
7. EC Green Paper: “Towards an integrated European Market for cards, internet and mobile payments”

In this regard it is important that there is a strong need for improving and harmonising European law and procedures in respect of the domains mentioned above so that liabilities and responsibilities, as defined in the corresponding legislation, are consistent with and reflect internet payment security recommendations, also in relation to the PCI DSS requirements.

In order to secure a level playing field it is a must to “ensure an effective and consistent implementation across jurisdictions” in the member states. The experience from the implementation of the PSD – which is referred to in the general part - is in this context scaring as consistency across Europe not exists. Way out too many options in the PSD rules was the main reason and it must be a very high priority not the repeat that failure if a framework is to be decided.

Generally all recommendations should be restricted to technology independent security requirements, rather than prescribe specific technical solutions. Too specific and detailed recommendations always create the risk that these measures could become either inappropriate to some contexts, or obsolete as a result of innovation.

All means of payments need to be subject to the same minimum security recommendations irrespective of the instrument, scheme or channel involved. That would be an expansion of the PCI DSS rule set, but still very appropriate.

Interpretation of the various concepts, definitions and classifications used throughout the document, e.g. classification of authentication instruments, must of cause be consistent.

Finally the timeframe for implementation of mid 2014 is much too ambitious and therefore unrealistic.

Recommendation comments:

1. Governance

Can only be supported if non-licensed institutions also are covered. All PSP' do not have a separate risk management function, whereas it is necessary to accept that the responsibility in regard to the security policy can be placed else ware in the organisation. Furthermore, "Independent" needs to be defined.

2. Risk identification and assessment

It is the responsibility of each PSP to comply with the security recommendations from ECB and the requirements from PCI in regard to their own installation. But as security is related to the whole value chain customers, e-merchants and other service providers must also comply with the same recommendations and requirements in regard to both sensitive data and payment transaction data. The whole chain of participants in an internet payments transaction has to be evaluated in order to secure that the necessary legal/contractual arrangements is in place.

3. Monitoring and reporting

Will in many cases put a heavy investment burden on the PSP', but it is very important in fraud fighting that the necessary monitoring is in place. The recommendation should include a concept/framework in regard to streamlining fraud incident reporting. You have to be aware that banks today already must report fraud incidents to the international card schemes, whereas this reporting procedure has to be included in the above in order to avoid duplication.

4. Risk control and mitigation

Once again the focus is on the PSP, but e-merchants and other participants in an internet payments delivery chain must comply with the security recommendations. As mentioned in “general comments” these rules should cover all participants in the whole delivery chain and hopefully be harmonised across the Globe and not only cover Europe. European only recommendations may harm the business connected to European internet payments badly. If a part participating in a payment transaction not is adhering to requirements that part should carry the risk of flaws, fraud and other unwanted effects. This should also apply to consumers and merchants. In fact this practice prevails since many years in the insurance industry – if you break the security requirements, compensation can be withheld.

We acknowledge that testing is required and important, but how to organize it should be left to the market to decide as the market has huge experience in this regard.

5. Traceability

Easy traceability is of cause important, but too detailed recommendations can easily put a heavy investment burden on small businesses. In card business traceability is already a must as it is required in regard to e.g. fraud detection, transaction requests and complaint handling.

6. Initial customer identification, information

Careful and comprehensive customer identification in regard to establishing new customer relations is very important in order to minimize the possibilities of fraudulent internet payments. The same goes for the information supplied to new and existing customers in regard to e.g. transaction handling, security measures, available transaction information and complaint procedures. It is also important that customers are updated frequently on these areas about new security measures but also to secure that the customer maintain high attention on security. Fulfilment of this information commitment is clearly in the interest of the PSP’ whereas we do not see the need for detailed recommendations on this area.

It is also important that security and information recommendations on the areas mentioned in this section do not go further than the PCI DSS requirements as it will hamper European internet payments business and make it more difficult for European providers to compete in the global market. In this connection it is our opinion that the PSD contained rather specific and comprehensive requirement in regard to mandated customer information.

Organization of contractual set-up should be left to the market and not regulated as the organizations possibilities are multiple and still with a clear description of liabilities and responsibilities of the parties engaged.

Anti-money laundering is very important, but it has nothing to do with the security of internet payments, whereas it should be taken out of this document.

7. Strong customer authentication

PNC fully support the use of strong customer authentication when sensitive data are included.

But, you need to address the more modern types of attacks on internet payments as they are largely unaffected by the strength of the authentication. These types of attacks (e.g. Trojans) changes the receiver account, the amount etc. on “the fly” after the authentication has been done by the consumer.

Once again we want to stress that it is important that the use of strong customer authentication is a global, mandatory requirement. The international card schemes do promote strong authentication, but it is not mandated yet in Europe or Globally. If it only becomes a European recommendation it will provide the European market participants with a huge and horrendous disadvantage.

Be aware that the issuer does not have any contractual agreement with e-merchants, but only with the acquirer and therefore any liability arrangements should be between acquirer and merchant.

8. Enrolment for and provision of strong authentication tools

See comments under section 7.

9. Log-in attempts, session time-out, validity of authentication

The proposals are all in use today as a natural and basic part of serious security set-ups. There is no need to specify these recommendations as they all are commonly known and used.

10. Transaction monitoring and authorisation

Real time fraud detection and prevention systems are of cause the ultimate goal of all fraud detection, but it has to be balanced with factors like e.g. is it on-line transactions, what is the existing security level, customer authentication method used and size and type of customer base. Without a balanced approach and global standards it will require unbearable investments from European actors.

11. Protection of sensitive payment data

Protection of sensitive payment data is very important and heavy protection can only be supported as long as the recommendations are proportionate and mandated for all participants.

The PCI DSS standards includes detailed requirements on this area (e.g. during transportation and storage) which we strongly recommend that the ECB recommendations comply with. Eventual expansion of these requirements has to be negotiated with PCI in order to make them global. Otherwise they will harm European internet payment business. The ECB should be aware that the PCIDSS standards have a working maintenance and development process, a necessity in this fast moving market. If the ECB promotes a pure European solution there is also a need to develop and fund maintenance and development structure for Europe alone.

The challenge is that the recommendations has to be mandatory to all participants in the value chain of internet payments, not only to PSP', issuers and acquirers. Global reach is a must.

12. Customer education and communication

Anyone will agree that education is important and it is important to keep customers updated with new security initiatives, but also to maintain and revive security information and procedures given at an earlier stage.

It is important to stress that lack of compliance with "education duties" does not free customers from their responsibility in regard to security in own environment.

13. Notifications, setting of limits

PNC see no need of specifying recommendations on this area as it already is a natural part of a professional customer relationship and agreement.

Furthermore, we are in the competitive domain in which the actors must be given the freedom to offer individualised services and features to their customers. Regulation will hamper the competition.

14. Verification of payment execution by the customer

The PSD included requirements on this area in order to protect and give information the customers. Further recommendations are not necessary for the time being.

Conclusion

We strongly recommend not to establishing a regulatory framework for security, but to follow the international standards development and agreed upon by markets and/or sectors. If the authorities choose not to follow this recommendation it is important that any regulation comprise all types of internet payments.

Initiatives such as the introduction of 3D Secure and the compliance programmes associated with PCI-DSS have shown that the industry takes the issue seriously and is addressing it without the need for regulatory intervention.

Market driven solutions do create sufficient security solutions for internet based payments. If a regulatory framework is set up it may protract the development of future innovative and secure means of payment methods, and is therefore potentially detrimental to the stated ECB objectives.

If the ECB decides to establish a regulatory framework it is of utmost importance that it is carried out in close cooperation with EPC' SEPA work around "Volume – Book of requirement” and PCI DSS as it must mirror/comply with international standards and requirements.

Best regards,

Kurt Gjesten
MD & CEO
PAN-Nordic Card Association