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

Holmens Kanal 2-12
1092 Copenhagen K
Denmark

1st June 2012

Group Financial Infrastructure
Reg.4365/Mihof/B50595
Contact person:
Michael Hoffmann
Mail to: michael.hoffmann@danskebank.dk

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

Consultation:

Recommendations for the security of internet payments
(April 2012)

Danske Bank welcomes the European Central Bank launching a public dialog re. the security of internet payments - and hereby submits our view on the recommendations.

Danske Bank Group is the largest bank in Denmark and a leading player in the northern European financial markets, with 645 branches in 15 countries. The Group focuses on retail banking by offering a wide range of financial services including insurance, mortgage finance, asset management, brokerage, real estate and leasing services. The Group has more than 5 million retail customers and a significant share of the corporate and institutional markets.
The Group has retail banking activities in Denmark, Finland, Sweden, Norway, Northern Ireland, the Republic of Ireland and the Baltic's. Danske Bank also have branches or subsidiaries in London, Hamburg, Luxembourg, Warsaw, New York, and St. Petersburg.

Danske Bank does not offer acquiring services directly and this is reflected in our response.

RESPONSE:

Danske Bank recognizes the recommendations from the European Forum on the Security of Retail Payments (SecuRe Pay Forum). We appreciate this initiative from the European Central Bank which gives us the opportunity to contribute with our views in this area.

It is timely that ECB issues these recommendations at the same time as the European Commission is considering responses to its Green Paper on cards, internet and mobile payments. In our response to the Green Paper we raised a number of issues that are relevant to the ECB recommendations and it is appropriate that we share these with the ECB in order that ECB considers joint initiatives with the Commission. The Danske Bank response to the EC Green Paper is for inspiration included as an Appendix 1.

All market players (Consumers, Merchants, Banks, Acquirers, Service Providers and even more . .) have a business rationale to minimize security issues and doing everything to prevent fraud – in order to ensure trust in e-Payments.

Danske Bank's initial understanding is that the recommendations are good ones and we would all agree with them for the most part - however the proposed implementation period is too tight.
The requirements derived from the recommendations are not simply for Payment Service Providers to implement alone, as also the retailers/merchants will need to support the required changes in order to harvest the potential benefits hereof. Alone based on this issue we must recommend a longer or stepwise transition period to ensure a successful implementation.

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. – and the above mentioned EC Green Paper: "Towards an integrated European Market for cards, internet and mobile payments"

All of them impacting the actors of the internet based payment and trade markets, with complicated impact on the future daily business – and in fact the list may not be complete.

We strongly recommend not to establishing a regulatory framework for security, but base the standards on market and sector development and agreements, and that these should cover both consumer cards and corporate cards. Initiatives such as the introduction of 3D Secure and the compliance programmes associated with Payment Card Industry, Data Se-

curity Standard (PCI-DSS) have shown that the industry takes the issue seriously and is addressing it without the need for regulatory intervention.

Market driven solutions should 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. Further regulation could reduce competition and innovation that could benefit the consumers and increase security in internet based payments transactions.

Merchants are not overseen by the local central banks and therefore they may choose not to comply with the recommendations. This will hamper the increase in security in e-Payments and put merchants at a disadvantage.

Danske Bank doubts that European regulation is capable of following the fast changing face of fraud and fraudsters, and by that not being able to support solutions to new fraud trends and patterns.

A Self-regulatory Approach should be the primary option, and the self-regulatory approach within the Payment Card areas shows the efficiency needed, via:

- The Payment Cards Industry body (PCI). PCI has issued recommendations for data protection: 'Data Security Standards' to whom all card issuers and acquirers must comply.
  (Link: https://www.pcisecuritystandards.org/security_standards/).
  PCI Council has also appointed a number of Assessors to help the PSP' comply with the recommendations.
- Within the European Payment Council (EPC):
  SEPA Cards Standardization (SCS) (- also known as the "Volume" – Book of requirements, and the SEPA Card Framework (SCF) is governing card security. The above PCI regulative recommendation could be included in the SCF Volume to outline standards.
  (Link: http://www.europeanpaymentscouncil.eu/content.cfm?page=sepa_vision_for_cards)
- The EU Commission
  'The Payment Service Directive' (PSD) states a set of regulatory issues to be followed and implemented in the member states. Both the general data protection requirements and the data protection rules for financial institutions are already laid down in EU law, with which all current payment systems have to comply. These rules are supervised by the Financial Supervision Authorities and the Data Protection Authorities and we find this appropriate.

It is the view of the Danske Bank that Payment Service Providers (PSP) in the Nordic countries have implemented these recommendations to a wide degree to the benefit of customers, issuers, acquirers, and merchants - pushing the general view on internet payments security in a positively direction.

Danske Bank supports increasing security on card payments and e-payments via Strong Authentications methods – like two factor authentication. As recommended in the document this authentication - or similar functionality should be encouraged in order to build more trust in internet payments from consumers and merchants.

As an example, the ECB is suggesting that such tools as 3D Secure are not sufficient for internet transactions based on static pass codes and requires a dynamic pass code system by 2014. Even though PSP's can arrange to supply dynamic authentication tools to customers for internet based payments, there is a need for merchants/retailers to support the use of those tools. Getting the merchants on board with such solutions is outside the remit of the European Central Bank - but PSP's are unable to comply with the recommendations without the retailers also being on board.

All players have a business rationale to minimize security issues and have made great strides to prevent such risks for instance by using 3 D Secure (- described in the recommendation, annex3), based on a dynamic password.
Such solutions are already in use for instance in Finland based on the domestic (so called TUPAS-solution), and in Denmark (via NemID) – trusted electronic identification methods used by both banks and the public sector, which can be included into 3D Secure.

The recommended possible exemptions by CVx2 based authentication is considered inadequate in the future, and stronger authentication methods can be developed in a competitive market.

In general Danske Bank supports standardisation (regarding security, protocols etc. for operability and security reasons) - in preference to regulation - in order to reduce the cost & complexity of participating in the internet payment market.

We fail to see why the transfer of e-money between two e-money accounts should be omitted, as also these accounts are subject to infiltration through Phising scans or other fraud. Hereby e-money can be transferred from one of these e-accounts to an e-account owned by a criminal - without the prior authentication by card- or accounts holder. The accounts of the fraudster are also often established through fraudulent means.

Annex 1, in the recommendation paper – re. PSD Review:

- The paper lists a number of Points to Consider, and Danske Bank has no arguments against the intention of the content hereof
- Danske Bank supports the recommendation that acquiring services should only be provided by licensed providers
- Danske Bank also supports repudiation and related liability to be clearly described and communicated in order to create trust in e-Payments, but we must stress that sector driven standards are preferable to regulation
- Danske Bank acknowledge the use of liability shift as a means to support the enrolment of merchants to strong authentication methods - however consumers convenience must not be neglected. Doing so will hamper the use of e-Payments, and may result in cash entering online trade - as it has already happened in India, where

"Cash on Delivery" is the #1 payment when shopping at e-merchants.
In KC 7.6 the ECB paper concludes that liability shift from e-merchant to issuer should be introduced – however in a 4 corner model (used for instance by Danske Bank) there is no contractual relationship between the e-merchant and the issuer. It should read from the acquirer to the issuer. If a consumer is bypassing strong authentication, it should be under the consumers responsibility only – not the issuers.

As electronic payments are discussed we must create standards and potential regulation in the light of a global world, and not limit our inspiration to EU/EEA or Europe. Over-regulated European electronic payment tools will hamper our local customers' and especially our local merchants' ability to operate in a global market place

Back in July 2003 Bank for International Settlements (BIS) issued a paper 'Risk Management Principles for Electronic Banking' as a result of the work of 'Basel Committee on Banking Supervision'. Many of the recommendations in today's ECB paper are also covered in this paper, and in a similar manner:

- One conclusion from that paper was that regulation formed as an 'one-fits-all'-approach should be avoided, as each PSP, each Bank etc. has its own risk profile. Therefore clear tailor made risk management tools should be set up by each PSP and it should be monitored by senior management, which is also suggested in the recommendations from ECB.
- Another conclusion was that no technical standards should be covered by regulation – as this must follow the market development on an 'on-going-basis'. Danske Bank encourage to follow this statement in order to ensure that security standards keep up with the technical development in e-Payments.

The 'Basel Committee on Banking Supervision' members are not only resident in the EU, but also represent USA, Japan, Australia, Canada, Hong Kong, and therefore it could potentially create a basis for worldwide standards – in order not to limit the options and possibilities for consumers and merchants operating within the EU/Europe compared to their competitors operating outside of EU (- as mentioned above).

Danske Bank has reservations about the need for a separate Risk Monitoring organisation for e-Payment with the PSP's – it should be an integrated part of any PSP's Risk Monitoring processes.

The call by the European Commission to set up an EU-wide utility for reporting and sharing information related to data security breaches is supported by Danske Bank, as well as the recommendation for further and ongoing information to advise consumers and merchants of how best to act in a secure manner when doing e-Business.

Implementation overseen by national supervisory authorities on a voluntary co-operative basis and based on the existing legal frameworks in host countries is considered a good solution – especially if based on the market driven developed standards and not based on European regulations.
However Danske Bank must strongly urge the implementation to be performed in a uniform way in all European countries in order to create a level playing field where all parties

are under same restrictions - and a consistent consumer experience across European borders is ensured.

Also Danske Bank believes it is essential that all providers of e-payment services (including present non-licensed institutions) should be subject to oversight and supervision under uniform processes.