FINANSRÅDET

DANISH BANKERS ASSOCIATION

CONSULTATION ON THE DRAFT RECOMMENDATIONS FOR "PAYMENT ACCOUNT ACCESS SERVICES" - COMMENTS FROM THE DANISH BANKERS ASSOCIATION

12 April 2013

Finanssektorens Hus
Amaliegade 7
DK-1256 Copenhagen K

Phone +45 3370 1000
Fax +45 3393 0260

mail@finansraadet.dk
www.finansraadet.dk

File no.
Doc. no.

The Danish Bankers Association welcomes the opportunity to comment on the draft recommendations for Payment Account Access (PAA).

PAA is a highly complex topic, which raises, inter alia, a number of technical, legal, regulatory and consumer protection issues. Payment systems are critically reliant on consumer confidence for them to be widely used and even more so when considering the uptake of new and innovative solutions. The SecuRe Pay Forum Recommendations on the security requirements for PAA are thus one important building block in ensuring the integrity of the payment system. However, it is very difficult to consider this in isolation, without knowing the wider legal and regulatory framework in which the recommendations are to be implemented. Hence, while we certainly welcome the document, we believe that further clarification on the wider framework for PAA is needed in order to ensure the thorough discussion of these recommendations that they deserve.

Due to the above, we have restricted ourselves to more general remarks, and we hope that it will be possible to revisit the recommendations, once the legal framework for PAA has been further clarified.

Our comments are based on the following general concerns:

1. Clarification of the wider framework. The recommendations cannot be considered in isolation – further clarification on the wider framework for PAA is needed.
2. A legal vacuum exists. Such further clarification could probably best be achieved by extending the scope of the PSD to cover PAA – ensuring a level playing field, adequate consumer protection and a clear and transaparent liability regime.
3. Ensuring a level playing field. The approach of supervisors and overseers to retail payment systems vary a lot. Hence, specific focus should be given to ensuring that the recommendations are not implemented differently in different countries – and to the need to ensure that sufficient resources are present in the relevant authorities.
4. The need for agreements between involved parties. Several recommendations are based on the tacit assumption that

agreements between third party service providers and PSPs exist – such agreements are in our view vital to protecting the integrity of the payment system.

5. Personal security credentials are personal. Business models that rely on consumers handing over security credentials to third parties are highly problematic – even more in the Nordic countries, where access to someones security credentials not only gives access to their bank account but to public authorities among other things. Handing over ones security credentials is currently prohibited under the PSD. We believe this should remain the case.

For more detailed comments, we would refer you to the responses of the UK Payments Council and the EPC, both of whom we support wholeheartedly. Our general remarks are given in the template provided in the attached document.

EUROPEAN FORUM
ON THE SECURITY OF RETAIL PAYMENTS

ECB-PUBLIC

12 April 2013

TEMPLATE:
COMMENTS ON THE DRAFT "RECOMMENDATIONS FOR PAYMENT ACCOUNT ACCESS SERVICES"

Contact details (will not be published)	MR	**Tobias Thygesen**
	TNT@finansraadet.dk	
	+45 3370 1077 (direct) / +45 6016 1077 (mobile)	
☐	The comments provided should NOT be published	

The table below shall serve as a template collecting comments received in a standardised way.

- Please **add** to the table **only issues where you consider that a follow-up is necessary**, i.e. no general statements like "We welcome the recommendations."
- All comments should be **separated per issue** concerned so that a thematic sorting can be easily applied later on. (i.e. one row for each issue).
- If needed, replicate page 2 for the provision of further comments.

The assessment form consists the four items which are suggested to be filled as follows:

- **Originator:** Name of the originator and ISO code of the country of the originator (e.g. NAME (AT/BE/BG/...))
- **Issue** (states the topic concerned): General comment, Scope, Terminology, REC 2, 1.1 KC, 3.2 BP, Glossary,
- **Comment:** Suggestion for amendment, clarification or deletion
- **Reasoning:** Short statement why the comment should be taken on board

Originator:

Name of the originator (e.g. name of the company or association)	**Danish Bankers Association**	ISO code of the country of the originator	DK

Comments on the recommendations for "payment account access" services

N°	Issue	Comment	Reasoning
1	General (Wider framework)	Clarification	We believe that it is vital to have an understanding on the wider framework for Payment Account Access in place, before entering a discussion of the actual recommendations of the SecuRe Pay Forum. In essence, it is quite difficult to discuss the recommendations as they stand. In order to have the thorough discussion that these important issues deserve, we need further clarification on the legal, technical and consumer protection issues, which we believe are core to any discussion of payment account access.
2	General (Legal vacuum)	Clarification	TPs are currently outside the scope of the domestic regulatory and oversight frameworks, not being covered by the PSD. Until the revised PSD enters into force (and – perhaps – then covers TPs), there is thus a legal vacuum, leaving the implementation of the recommendations uncertain at best. We believe that the PSD should be extended to cover PAA – and would appreciate further clarity on how the interim period is to be handled.
3	General (Need for a level playing field across borders)	Clarification	The national supervisory and oversight frameworks are implemented differently across Europe, not the least when concerning retail payments. Hence, the recommendations may be administrated differently because of this. This endangers the level playing field and opens the door for regulatory arbitrage. Even when regulation is implemented through Regulations or Directives, the risk of differing national implementations remains significant, as the implementation of the PSD has illustrated. This is a risk that needs to be kept in mind. Furthermore, the resources needed to enforce the oversight frameworks towards a plethora of PSPs/TPs and the ability of supervisors to maintain an up-to-date overview of PSPs causes concern. In order to maintain level playing field and ensure a uniform application of oversight and supervision, it is pivotal that all PSPs/TPs and banks are subject to the same level of enforcement.

4	General (Legal relationships)	Clarification	Several of the KCs (e.g. 3.3, 5.4, 5.5 among several others) rely on the tacit assumption that TPs enter into agreements with PSPs – but this is currently not always the case, nor is it necessarily something that can be achieved until the PSD is amended to cover payment account access services. We believe that such services should require clear agreements between all relevant parties in the chain (TPs, PSPs, customers). Such agreements should cover, inter alia, liability, security, fraud prevention activities and fees. The agreements should leave the consumer in no doubt what the TP does and does not do on her behalf. Here as elsewhere, we see contractual freedom as a key principle. Otherwise, consumer confidence in the retail payment systems and, in the final instance, the integrity of these systems themselves, are at risk.
5	General (TP identification)	Clarification	Business models that rely on the TP impersonating the customer should be prohibited - and the general principle should remain that consumers are not allowed to pass on their security credentials to thirds parties (as articulated in article 56 of the PSD, and BP 5.1 in the recommendations). In Denmark, the terms and conditions of banks with customers state that credentials are personal and must not be handed over to third parties. Several of the KCs and BPs (e.g. KC11.4, BP11.2) assume that access to the customer's internet bank can be "layered" – that it is possible to restrict which data the TP gets access to. This is currently not possible when the TP logs on, impersonating the customer. By impersonating the customer, the TPs get full access to all information and all operations. This gives rise to serious security issues and to problems for the PSP, which will log the activities of the TPs as those of the customer – and could potentially lead to the risk of the security of the account being compromised. Furthermore, the security credentials used for online payment and banking services in Denmark (NemID), Sweden (BankID) and Norway (BankID) to a large extent allow access to data with the public authorities (e.g. tax) and allow users to sign transactions towards public services electronically (e.g. land registries in connection to the trading of real-estate property), allowing the consumer to rely on only one security solution. We therefore also see a wider risk of data theft etc. if credentials are compromised.

6	General (Commercial conditions)	Clarification	Based on the above, there may be a need for the PSP to develop specific solutions for TP access, especially to prevent security breaches. In general, PSPs should be allowed to charge for TP access to cover the costs they incur in this regard (both running and development costs). PSPs should thus be allowed to charge fair and proportional fees relating to the needed development. A proper distribution of costs only becomes possible, once PSPs and TPs have entered into some sort of agreement. This is a further illustration of the fact that discussing these issues, without knowing the wider framework, becomes quite difficult.