Position Paper

10/04/2013
P10727 FEB176124
Anne Demelenne
Final

febelfin

ECB public consultation on the draft "Recommendations for payment account access services"

Belgian Banks reply

Belgian banks welcome the ECB Consultation and the opportunity to comment upon the important issue of account access services.

Position of the Belgian banks on access to account

The **ECB initiative** is very welcome as a **first step**. Various legal and regulatory initiatives are being prepared and the Belgian banks are of the opinion that all of the aspects of this matter should be discussed. The security aspects, which are a matter of high concern for the banks, in particular should be included into a **general debate** which takes into account the overall supervision regulation, the rules that apply, consumer and data protection, etc.

Consequently, the Belgian banks suggest tying up the current debate with the general debate on the PSD review.

Stimulating increased competition is sustainable only if there is a level playing field for all players who are active in the payment markets. Any distortion in the regulation and supervision applicable to the various players (and the various payment methods) must be avoided in order to guarantee **fair competition** and a **smooth functioning of the market** and **avoid a loss of consumer confidence in payment instruments**.

Banks have the **legal responsibility to safeguard data privacy** and ensure **data protection** for their customers. These safeguards call for particular attention in e-channels and this explains the continuous series of regulatory initiatives aimed at enhancing security in this environment. So, **banks invest** heavily in updating and maintaining the **security** of their banking channels and core banking infrastructure. The provision of access to current accounts to **third parties** would entail a **significant reputational risk** for banks due to the addition of an external party into the one-to-one contractual and trust relationship between a bank and its customers. In our view, security and consumer protection in this matter are of overriding importance, because it is not always obvious for a consumer to see what the possible consequences of this third-party access may be. Therefore, Belgian banks think that even the fact that the customer confirms to the third party that it can have access to her/his

Belgian Financial Sector Federation
Rue d'Arlon 82 - 1040 Brussels | http://www.febelfin.be
T + 32 2 507 68 11 | F + 32 2 888 68 11

account is not sufficient to allow such a third party to have access to account data and/or funds.

Another concern is the **absence of a level playing field in regulation and supervision**, which leaves bank customers unprotected from misuse and security flaws to a large extent. If for example the database of this third party has been hacked, massive fraud could occur and harm the bank customers as well as severely affect the confidence in this bank.

According to the Belgian banks, there are no market failures that could justify access for non-banks to bank account information. Several Payment Service Providers are quite successful without having access to bank account data. Besides, well-regulated payment schemes (card schemes, SDD, etc.) exist in order to make sure that, under tried and tested terms and conditions, payment transactions will reach bank accounts. In order to reach a similar security level, one should take a look at the following question: what are the circumstances and the technical, regulatory and security standards that would justify additional access? In practice, this would lead to a new type of scheme with specific rules and regulations and new (redundant) infrastructure investments, and consequently an increase of the overall cost of the payments market in general.

For these reasons, Belgian banks oppose regulation that would give non-banks access to bank account information, because this poses a serious threat to the integrity of payment services and even banking services in general. Adequate mechanisms exist to provide an efficient and secure payment landscape.

General remarks on ECB Draft Recommendations document

- "Payment account access services": these services must be clearly defined. Are payments automatically involved after access (cf. page 2, §2, of the ECB consultation) ? In case of a payment, all PSD provisions have to be met.
- Banks are reluctant to give (all) non-banks access to their customers' accounts (and potentially to any kind of customer information such as salaries, loans, payments etc.). Confidentiality and privacy issues are key concerns. Providing access to sensitive information for third parties which have no relationship with the customer raises very serious concerns.
- Need for regulation: Third Party Providers must be duly supervised (direct prudential supervision) and only well-regulated entities (e.g. Payment Services Provider status or PSP) could be given access to accounts. This requirement is essential in order to guarantee a level playing field.
- Contractual basis between the accessing PSP and the account holding bank (and not only based on mandatory reachability imposed by regulation) including:
  - ✓ assignment of liabilities to the relevant parties
  - ✓ possible charging of costs generated by this access : processing, standardization, security, maintenance, etc.

  - ✓ this kind of contract should also take into account the risk management for any funds that would be transferred via the account of the PSP. The reputation risk for banks should also be taken into account.

- Explicit customer agreement and consent: the bank must be sure that the customer will be informed and that he has given explicit consent to allow a third party to have access to his account/information.
- The risk of identity theft is very high and is a cause of serious concern for the banks.
- All Payment Services Directive provisions and rules for data protection and consumer protection must be taken into account.
- Hardware and software security for each individual entity as well as in the field of communication must be guaranteed.
- Standardization of access at European level including requirements, parties' certification, etc.

Position Paper

10/04/2013
P10727 FEB176124
Anne Demelenne
Final

EUROPEAN FORUM
ON THE SECURITY OF RETAIL PAYMENTS

ECB-PUBLIC

30 April 2013

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

Contact details (will not be published)	Febelfin	Patrick Wynant - Anne Demelenne
	Patrick.wynant@febelfin.be – anne.demelenne@febelfin.be	
	+ 32 2 507 68 51 - + 32 2 507 68 53	
☐	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

Belgian Financial Sector Federation
Rue d'Arlon 82 - 1040 Brussels | http://www.febelfin.be
T + 32 2 507 68 11 | F + 32 2 888 68 11

Originator:

Name of the originator (e.g. name of the company or association)	Febelfin (Belgian Financial Sector Federation)	ISO code of the country of the originator	BE

Comments on the recommendations for "payment account access" services

Issue	Comment	Reasoning
Scope	Amendment	Throughout the document, technology independence is aimed for. However, in the Scope and on other occasions in the document, explicit reference is made to "internet" based payment account access services. The document should aim for abstraction of "internet".
Scope	Amendment	The report should include the list of major weaknesses and vulnerabilities detected (in an annex, for instance)
Scope	Amendment	"*Mobile Payments other than browser-based payments*" should be in scope. Given the growing prevalence of mobile payments, we run the risk of inconsistent regulation between browser-based and FAT-based regulations for account access services
Implementation	Amendment	Add with reference to the PSD: the revision of the PSD should address the position of the TPs in the payment landscape and evaluate, among other things, the liabilities of the different parties, in particular PSP versus TP.
Implementation	Amendment	The document does not cover the relation between the PSP and TP. Maybe this is to be added to the PSD revision, but as long as the PSD is not revised the TP's position in the payment landscape is not clear. Several KCs and BPs refer to collaboration between both parties. The following topics should be covered somewhere: - Contractual relationship between both parties: TP & PSP – what are the minimum obligations of both parties to be covered in the contract - Obligations of PSPs to "allow/refuse" TPs to interface with them (In the current context, the TP would become regulated, but could be excluded by the PSP from delivering services. This could seriously impact the opening of the TP channel.

3.3 KC	Amendment	This control is typical one where an agreement (see above) between PSP and TP/GA is necessary.
4.1KC	Amendment or Deletion	A TP or GA should not be obliged to take into account the protection of the IT at the PSP. Security best practice is that any party, including the PSP, should protect itself from any external (including TP/GA) malicious act. The current formulation would require that TP/GA is aware of the IT (security) of the PSP, its evolution and its weaknesses and has appropriate controls in place to defend against the exploit of those, and even to be liable in case something happens. TP/GA is in this case performing part of the infrastructure/security risk analysis and implementing/operating mitigation for the PSP. Complex situations arise when one TP/GA collaborates with different PSPs (e.g. Overlay Service Providers).
4.11 KC	Amendment	To be added: TP & GA are accountable to inform PSP that they are using their account access services because PSPs are not always aware of TPs making use of their services.
4.12 KC	Amendment	To be added: TP & GA are accountable to initiate necessary tasks and activities to implement the recommendations set out in this Directive and report any compliance gaps to impacted PSP and/or the competent authorities
REC 3	Amendment	Any fraud that impacts a PSP customer (even a single one) should be reported to the PSPs. This is required for the PSP to fulfill its regulatory obligations of effectively managing fraud
Footnote 12	Amendment	GA is not included in the footnote.
Footnote 14	Clarification	Definition of “Privacy by design”
4.1 BP	Amendment	The ECB should set objectives of *what* should be done by the TP. The Directive should not impose solutions.
5.1 BP	Deletion	This would represent a huge burden on PSPs as they have to cater for registration, distribution, reset, revoke, renew these credentials to accommodate customers using TPs.
5.1 BP	Deletion	This is not a Best Practice but a possible implementation of the 5.6 KCs. It is however likely that GAs and TPs will issue their own credentials. Suggest to remove the 5.1 BP.
6.1 KC 6.2 KC Footnote 17	Clarification	Cf. Implementation: this should be covered by a contractual agreement and clear liabilities.
6.3 KC	Clarification	Cf. Implementation: this clause (“block a specific transaction”) can be in conflict with PSD/SEPA obligations. This must be further analysed and addressed.

6.1 BP	Clarification	Cf. Implementation: this should be covered by a contractual agreement and clear liabilities.
6.1 BP	Amendment	“TP and or/the” => “TP and/or the”.
10.3 KC	Clarification	Same remark as for 6.3 KC.
10.5 KC	Amendment	TP and PSP should not only work together ex post but also ex ante, i.e. exchange information on fraudulent behaviour, transactions, customers, in order to prevent fraud. However, the topic of preventative controls has not been elaborated upon.
14.2 KC	Amendment	Clear legal position on the parties authorised and the format under which, issuance of account statements can be done (only PSP or also TP).
	Amendment	Check for consistent use of TP and GA throughout the whole document.

Belgian Financial Sector Federation
Rue d'Arlon 82 - 1040 Brussels | http://www.febelfin.be
T + 32 2 507 68 11 | F + 32 2 888 68 11