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Contact details (will not be published)	Ms	Leonor MACHADO
	lmachado@cgd.pt	
	+351 21 795 32 56 (office) / + 351 96 393 48 96 (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☐	The comments provided should NOT be published	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)	Portuguese Banking Community	PRT	

Comments on the recommendations for "payment account access" services

Issue	Comment	Reasoning
Prerequisites	Clarification	There are vital prerequisites that must be in place before defining standards around this kind of document. The discussion of rules for interaction between financial service parties should only occur if the interaction is being regulated upon, which is not the case.
General - Legal	Clarification	This document presents a TP definition, however it is still not clear the legal and regulatory framework that can supervise and act on these TPs. Furthermore, depending on the jurisdiction where the TP is located, different levels of security obligations and controls depending may be enforced. When rules are defined, it becomes critical to put in place mechanisms to guarantee that the rules are met (e.g. sanctions definition according to the kind of breach). Without this kind of clarification, these TPs rules take the risk of not being effective, creating an unbalanced level playing field between third party and PSPs in terms of security and obligations.
General - Regulation	Clarification	Nowadays the PSPs are under a set of legal and regulatory obligations that highly exceeds the rules identified and defined in this document. The "*know your customer*" rule present in the *"anti Money laundering"* framework as well as the PCI DSS security standards, are examples that can be considered to highlight these legal and regulatory differences, enforcing the unbalanced level playing field between the PSPs that issue accounts and the TPs providing account access services for these accounts.

General – Contractual Agreements	Clarification	Account servicing PSPs bear significant costs for supporting an online banking infrastructure and in particular, its adaptation to accommodate secure and identifiable access by TPs. Therefore, if a TP uses this infrastructure for its own commercial benefit, PSPs become a "de-facto" service providers to these TPs. PSPs should therefore be able to charge reasonable and proportional fees for the services rendered to TPs offering PAAS., not only because of incremental cost, but also from a revenue sharing perspective as is common in the digital world. Agreements regarding risk mitigation, operational aspects and allocation of liabilities are needed, otherwise there is a risk that the responsibilities related to security of payment account access services, or the lack of the sufficient level of security, might remain with the account servicing PSPs' – who should not be responsible for the possible negligence by TPs.
General - Security	Clarification	The TPs security policy should be enforced in this document so as to meet the same level of security as present actors in the payment industry and not compromise user's confidence. The PSPs have built and are under their systems in accordance with a rigorous straight security policy in order to guarantee that online transactions are as safer as possible for their Clients. It must be guaranteed that these TPs will never have a security level similar policy, lower than the one that the PSPs have for their online transactions. Access to payment accounts by TPs should preferably be defined at EU-level so that access to a specific PSP's infrastructure is provided in a standardised and structured manner, i.e. in the same way for all TPs.
General - Service Levels	Amendment	The involvement of the TPs should not affect the service levels of the PSPs towards the customer.
Scope	Amendment	Apps which offer TP services should be in scope of the recommendations, since PAAS are frequently offered through apps. These apps can (and do already) have access to internet banking-based account servicing PSPs. Mobile Payments "other than browser-based payments" should be in scope. Given the growing prevalence of mobile payments, we run the risk of inconsistent regulations between browser-based and non-browser-based regulations for account access services.
Scope	Amendment	The specific rules regarding non-EU based TPs providing services within the EU should be clarified.
Scope	Amendment	This section should clearly specify if the scope of the recommendation covers e/m Wallets providers.

Customer awareness, education and communication	Amendment	The SecurePay draft document fails to mandate the use of a dedicated authentication means per entity and authorization and doesn't take into account the fact that one of the main vectors to defend against some major types of threats (such as phishing) is based on the strong message that cautions users to never share credentials with anyone, whatsoever. The Portuguese banking community has been largely investing in promoting the internet users best practices. NOT sharing the login credentials is one of the core messages that has been being disseminated among the internet banking users. If this rule be exempted it will create confusion among the users and will place their internet experiences at risk.
Recommendation 1 – Governance (1.2 BP)	Clarification	This can only be made with the integration of the PSPs and the TPs information systems in a way that the Client won't lose autonomy or service level. To protect the client against abusive use of his account, the implementation of a strong authentication process by the TP is critical. The price that the client is going to pay for these kinds of services must not generate surcharging of merchant service fees when paying with a payment card. The cost of this new development should be covered by all parties gaining benefits of the development.
Recommendation 1 – Governance (1.2 BP)	Clarification	It is not clear whether the minimum technical and security standards will be defined multilaterally as part of the GAs duties or bilaterally between particular TPs and PSPs. Moreover, it is not clear how the minimum technical and security standards will be enforced. The BP should be more explicitly formulated towards all parties including GAs.
Recommendation 3 – Incident monitoring and reporting (3.3 KC)	Clarification/Amendment	This point should consider not only the incidents report, but also the monthly statistics reports that are in practice for banks and PSPs. Considering the fact that the PSP can be left completely outside the contract signed between the TP and the Client, the cooperation between the TP and the PSP should be consider contemplated under the established contractual relationship. TPs should have the same level of reporting as the PSP's.
Recommendation 5: Traceability	Clarification/Amendment	If the account access is made by a TP on behalf of a client, there is a possibility that the bank may not be able to identify who is accessing the information. In this case the bank and the client will be exposed to additional risk that they won't be able to manage.The PSP needs to effectively manage the transactions risk and so, identifying the origin of an account access is critical for making the appropriate risk management. Is must be discussed and clearly defined who has the right to data, and how are mandates for the access to data perceived.

Recommendation 6: Initial customer identification and information	Clarification	Customers should be properly identified in line with the European anti-money laundering legislation. Internet Payments are subject to a proper identification of customers in line with the European anti-money laundering legislation. Account Access Payments should be subject to the same rules.
Recommendation 7: Strong customer Authentication	Clarification/Amendment	PSPs have conducted risk analysis and have implemented an authentication system to mitigate the evaluated risks. The fact that a TP has knowledge of these credentials increases the probability of compromise and may render the authentication system unsuitable. Authentication credentials are the cornerstone to a secure and strong authentication system. PSPs go to great effort to reduce the exposure of credentials: by reducing the number of places where they are processed, by not storing credentials (sometimes not even in encrypted form such as with CVV's) and reducing the time they exist (for example they are eliminated as soon as authentication is accomplished). By having a TP receiving the credentials through a communication channel and processing the credentials on their systems the attack surface is significantly enlarged even in the case where the same levels of security are met.
Recommendation 10: Transaction Monitoring	Clarification/Amendment	PSPs have conducted risk analysis and have implemented an authentication system to mitigate the evaluated risks. The identification of the system where the payment is performed is of primordial importance, to determine (or score) the transaction as being genuine or not. By having a third party as an intermediary this vital fraud detection information is lost. Fraud detection systems rely heavily on activity patterns and the payment originating system is in many detection systems one of the most important pieces of information. By having a third party intermediate these services much of this intelligence is lost.
Recommendation 10: Monitoring (10.5 KC)	Amendment	This point should include additional text: "considering the established contractual relationship". The cooperation should be regulated by a contractual relationship.

Recommendation 11: Protection of sensitive payments data	Amendment	A contract must be signed between the final user and the TP to allow the access and account transactions, on his behalf. In Portugal, there exists legislation to assure that only legally authorized person or entities have access to account information. There are mechanisms in place to assure that the access and account transactions can only be performed by the authorized persons. This kind of legislation has much value for the clients giving them additional comfort that his account information is safe and treated with the demanded confidentiality. Banks see as critical the maintenance of this level of trust and quality service with their clients. Therefore, a thorough legal assessment must be carried out, to ensure compliance to data protection laws and other laws or regulations - especially ensuring that Banks are not compromising any regulation imposed on them today.
4.9 KC	Amendment	TPs should not authorise e-merchants to store sensitive payment data, they must ensure it does not happen and in addition take action in case of a breach.
REC 6	Amendment	A specific KC about impersonation must be included. The relation PSP/Client is compromised when the personal security credentials are shared with other TPs impacting on the liability, banking secrecy and data protection issues.
8.2 KC	Amendment	TPs should actively mandate (instead of *encouraging*) customer enrolment for strong authentication with the TP.
11.3 KC & 11.5 KC	Clarification	The interpretation of 'sensitive payment data may differ due to national legislation.
Glossary	Amendment	A definition for GA should be added to the Glossary.