FEDERATION
BANCAIRE
FRANCAISE

12th April 2013

Response to ECB Recommendations for "Payment account access services"

The French Banking Federation (FBF) is the professional organisation that represents all banks doing business in France. It has 430 member banks of all types (commercial, cooperative or mutual), French and foreign alike.

One of its mission is to promote banking and finance on the French, European and international markets, and to define the positions and proposals of the profession with regard to governments and authorities in the economic and financial field, at the national, European (the FBF has a location in Brussels) and international levels. It is also inform member banks of any issue relative to their business.

In addition, the FBF issues professional recommendations and agreements, and shares its experience with members.

Contact details	Fédération Bancaire Française 18 rue La Fayette F- 75009 Paris Olivia Laplane olaplane@fbf.fr +33 1 48 00 50 65	 Jérôme Raguénès jraguenes@fbf.fr +33 1 48 00 51 81

The comments provided below can be published.

1. PRELIMINARY KEY COMMENTS

The French Banking Federation is pleased to have the opportunity to review and provide comments on the Recommendations for the "payment account access" services proposed by the Eurosystem's. Banks are particularly vigilant on the security of payment services and consequently of the information related to the payment account which may be accessed by third parties.

1.1. A COMMON EUROPEAN LEGAL FRAMEWORK

The FBF considers that any third party services providers granting account information services and / or payment initiation services should be supervised by a competent authority and preferably obtain a license to undertake its activity. In addition, the role and responsibility of each stakeholder (third party services providers, account servicing PSPs, account owners) would have to be defined in a legal framework and where necessary completed by contractual agreements.

ECB safety requirements could serve as a reference for the internal market, as long as it is certain that they will be applied in a harmonized way and be consistent with the European legal framework related to payment services and data protection.

Contractual relationships between third party services providers and account servicing PSPs should not only take place within the existing legal framework but also be compliant with the principle of contractual freedom.

In addition, each account servicing PSP should be able to define higher security requirements than those established by the ECB recommendations.

Last but not least, national and European authorities should focus their actions on setting high level principles as soon as possible in order to pave the way to the forthcoming legal status, supervisory requirements, liability and transparency rules, etc. The objective should remain that third party providers are forced to apply these recommendations.

The FBF calls for a revision of the payment services directive encompassing any third party services providers granting account information services and/or payment initiation services. Regarding account information services, while they do not allow the initiation of payment transactions as such, they still may cause damages to the account owner. As a consequence, they should also be included in this directive.

1.2. DATA PROTECTION

French banks grant high attention to the protection of data related to the account owner. Regulations in force require banks to manage strict processes to ensure confidentiality and privacy of their customers' information.

The current data protection directive sets strict limits to the collection and use of personal data. They may be processed by a third party only if the account owner has unambiguously given his/her consent. The directive also establishes that data may be processed by a third party if the processing is necessary to the performance of a contract to which the account owner is a party. As a consequence, providing payment account data to a third party without being certain that the account owner **has given his explicit consent to the transfer of these data, neither that he has a specific contract with the third party,** raises deep concerns. French banks fear that "payment account access" services could result in the transmission of data which may not be necessary for the performance of the third party contract with the account owner, and still be held liable for this transmission.

The FBF asks for a safe framework to ensure that only appropriate data for the purpose of their activities may be processed by third party services providers, without compromising the liability of the account servicing PSPs.

1.3. CONSISTENCY OF CONCEPT, TERMS AND DEFINITIONS

Several European Directives or Regulations deal with services providers, payment services, data protection, anti-money laundering, the fight against criminal activities and it is feared that it may result in a lack of consistency and result in multiple and diverging interpretations. At minimum, the concepts and related terms as well as their definitions have to be coherent across the Internal Market.

It is expected that the key terms and their definition used all along the ECB recommendations are coherent with the concepts and terms defined by the key European directives such as the Payment Services Directive and the Data Protection Directive.

Furthermore, a strong expectation is that these recommendations are consistent with the recently published Eurosystem's Final recommendations for the security of internet payments. One example of necessary coherence would be the security requirement applicable to log-in attempts, session time out and validity authentication.

1.4. PERSONAL CREDENTIALS

French banks are keen on providing personal credentials to the ultimate user (either his client or the third party provider) In no circumstance, should such credentials be used by someone else than the ultimate user. This is a key security pillar.

This requirement is fully in line with the Payment Services Directive related to the obligations of the payment service user and of the payment services providers in relation to payment instruments (articles 56 and 57).

The FBF would like to highlight that the provision of distinctive credentials to the account owners and to the third party services provider of the account owner will imply important IT developments, contractual arrangements and roll-out procedures for the banking industry. This has to be taken into account in the timeline given to the implementation of these recommendations.

1.5. THE MANDATORY NATURE OF THE ECB RECOMMENDATIONS

French banks consider that these ECB recommendations should be enforceable by law in order to constrain the third parties to apply them.
Moreover these recommendations cannot suffer of heterogeneity of the application in the European Union and require a European harmonization of the recommendation's application at national level.

2. DETAILED COMMENTS

Issue	Comment	Reasoning
Payment account access services (pages 1-2)	clarification	Comment: Definitions have to be in line with the concepts, terms and definitions of existing directive.
Payment initiation services (page 2)	amendment	Proposal: "Payment initiation services initiate payment transactions via a person's internet-enabled payment account. The technical implementation of this service can differ depending on whether or not the payee is actively involved in the payment initiation (e.g. during online shopping) and whether the TP's *is active on the account owner behalf.* ~~*software is used by the account owner to transmit his/her credentials to the account servicing PSP*~~." Reasoning: credentials are personal and can never be used by someone else than the ultimate user.
Scope and addresses (page 3)	clarification	Comment: The scope should be precise on what payment services are subject to payment account services.
Guiding principles (pages 3-4)	clarification	Comment: The revision of the Payment Services Directive is expected to encompass any third party services providers granting account information services and/or payment initiation services. Account information services may also cause damages to the account owner and should also be included in this revision.
Guiding principles (pages 3-4)	clarification	Comment: without an appropriate framework, third party providers may not be forced to apply these recommendations.
Recommendation 1 (page 5)	clarification	Comment: these recommendations should remain minimum requirements, allowing any party to require additional security requirements proportionate to the level of risk. This would be an additional risk mitigation measure.
1.2 BP (page 5)	amendment	Proposal: this Business Practice should be set as a Key Consideration.
Recommendation 2 (page 5)	clarification	Comment: Audit firms, appointed by competent authorities, should be able to control that the third party services provider has correctly implemented the recommendation. It is a healthy management activity.
4.7 KC (page 7)	clarification	Comment: Audit firms, appointed by competent authorities, should be able to control that the third party services provider has correctly implemented the recommendation. It is a healthy management activity.

Issue	Comment	Reasoning
5.2 KC and 5.3 KC (page 8)	clarification	Comment: The length of storage of log files should be based on what they will be used for. In addition, they should be kept as long as required by the European legislation in force (e.g. The Payment Services Directive for payment initiation services or Data Protection Directive for account information services).
5.5 KC (page 8)	amendment	Proposal: "*when communicating with an e-merchant and / or an account servicing PSP,* TPs should ensure proper *host to host mutual authentication as well as* bilateral authentication ~~*when communicating with*~~ *between TP and e-merchant as well as between TP and account servicing PSP*." Reasoning: Authentication should be undertaken on both security layers.
5.6 KC (page 8)	other	Comment: French banks strongly support this key consideration.
5.1 BP (page 8)	amendment	Proposal: "… could provide *TP's* ~~*customer*~~ with specific…" Reasoning: Security norms entail that credentials are only provided to the end users.
New KC to be added under recommendation 5	amendment	Proposal: " *TPP should never use the personal credentials of the account owner*". Reasoning: Security norms entail that credentials are only provided to the end users.
6.1 KC (page 8)	amendment	Proposal: "TPs should ~~*where applicable ensure that the customer has undergone*~~ *undergo* the customer due diligence procedures and *requests* adequate identity documents …" Reasoning: KYC controls should also by applied by the TPP.
6.2 KC (page 8)	amendment	Proposal: "TPs should ~~*where applicable*~~ ensure…" Reasoning: there is no reason for an exception.
6.2 KC (page 9)	amendment	Proposal: "- guidelines for the proper and secure use of personalized security credentials *delivered by TPs*;" Reasoning: such guidelines to be provided by the TPs should only address the credential delivered by the TPs.
6.5 KC (page 9)	other	Comment: French banks strongly support this key consideration.
6.1 BP (page 9)	clarification	Comment: Whilst it is legitimate that payment account access services be subject to contractual

Issue	Comment	Reasoning
		arrangements, TPs and account servicing PSPs should be allowed to decide how they organise their contractual relationships with the account owner.
Recommendation 7 (footnote page 9)	amendment	Proposal: "… only the user knows, e.g. static *or dynamic* password …" Reasoning: password may also be dynamic.
7.1 KC (page 10)	amendment	Proposal: "… for the customer's access to payment account access services. *In the case of a payment initiation service, an account servicing PSP does not have to perform strong customer authentication. ~~However, a TP could agree with an account servicing PSP to rely on the account servicing PSP's authentication methods.~~*" Reasoning: the initiation being undertaken by the TPs, it is the responsibility of the TPs to conduct the strong customer authentication.
7.2 KC (page 9)	deletion	Comment: this KC goes against consumer protection. 7.1 KC is sufficient.
7.3 KC (page 9)	amendment	Proposal: "… in a safe and trusted environment *controlled and operated by the TP ~~while taking into account possible risks arising from devices that are not under the TP's control.~~*" Reasoning: TPs should be held responsible for all initial registration processes of its customers.
7.3 KC (footnote 20 page 9)	amendment	Proposal: « … ii) a secure website under the responsibility of *and controlled by* the TP *~~or the GA offering comparable security features inter alia as defined in Recommendation 4; or iii) automated teller machine (ATM) services. (In the case of ATMs, strong customer authentication is required. Such authentication is typically provided by chip and PIN, or chip and biometrics.)~~*." Reasoning: TPs should be held responsible for all initial registration processes of its customers.
7.1 BP (page 9)	deletion	Comment: this could result in misunderstanding for the account owner.
Recommendation 8 (pages 9)	amendment	Proposal: "TPs should *~~where applicable~~* ensure…" Reasoning: there is no reason for an exception.
8.1 KC (page 9)	amendment	Proposal: "Enrolment *~~(if any)~~* for and provision of …" Reasoning: there is no reason for an exception.
8.2 KC (page 9)	amendment	Proposal: "TPs should actively *undertake ~~encourage~~* customer enrolment with strong authentication."

Issue	Comment	Reasoning
		Reasoning: Enrolment with strong authentication should be mandatory.
8.3 KC (page 9)	amendment	Proposal: "TPs and GAs should ensure that ~~*where applicable*~~ …" Reasoning: There is no reason for an exception. This KC should be coherent with the Final recommendations for the security of internet payments.
Recommendation 9 (page 10)	amendment	Proposal: "TPs should ~~*where applicable*~~ limit…" Reasoning: there is no reason for an exception.
Recommendation 9 (pages 10-11)	clarification	Comment: the level of requirements of all these KCs should be coherent with the Final recommendations for the security of internet payments.
9.4 KC (page 11)	amendment	Proposal: "…upon the *account owner's* ~~*customer's*~~ specific instruction ~~*and on a case-by-case basis*~~." Reasoning: "Case by case basis" could be interpreted as a possibility for the TPs to sometimes derogate from the customer instruction. TPs should always (and only) act upon the account owner's instruction.
10.3 KC (page 11)	amendment	Proposal: "…… in order not to unduly delay the initiation and/or *moment of reception by the account PSP* ~~*execution*~~ of the payment transaction …." Reasoning: according to the PSD, the execution can only be undertaken by the PSP. An undue delay could result from the initiation or the moment of reception of the payment order.
Recommendation 11 (page12)	amendment	Proposal: to delete everywhere in these KC and BP the word "payment". Reasoning: Sensitive data are not only payment data. TPs may access other data of the payment account.
11.2 BP (page 12)	amendment	Proposal: "It is *mandatory* ~~*desirable*~~ that TPs only …" Proposal: this Business Practice should be set as a Key Consideration after 11.4 KC. Reasoning: TPs should not have access to other data than those requested by the account owner.
11.4 KC (page 12)	amendment	Proposal: and TP~~*'s involvement*~~ should ~~*be limited*~~ *limit its involvement* to the extent …" Reasoning: It is the responsibility of the TPs to limit their involvement.

Issue	Comment	Reasoning
11.4 KC (page 12)	amendment	Proposal: "…upon the account owner's specific instruction ~~*and on a case-by-case basis*~~." Reasoning: "Case by case basis" could be interpreted as a possibility for the TPs to sometimes derogate from the customer instruction. TPs should always (and only) act upon the account owner's instruction.
11.5 KC (page 12)	amendment	Proposal: "…TPs storing *other sensitive* data should ensure that." Reasoning: clarification
12.4 KC (page 13)	other	Comment: French banks strongly support this key consideration. Customer should no more communicate its credential to anyone.
New KC to be added under 12.4 KC (page 13)	amendment	Proposal: "*TPs should relay to account owners any message of competent authorities related to customer education and awareness*" Reasoning: official messages should be forwarded by any actors to duplicate the effect
12.6 KC (page 14)	amendment	Proposal : "… and/or the terms and conditions)~~,~~ ~~*including the maximum amount of indemnification in the event of unauthorized use/fraud and*~~ the functioning…" Reasoning: Who would bear the amount above the upper limit? There is no reason for such a maximum. The KC should be in line with the PSD.
Recommendation 13 (page 14)	amendment	Proposal: "risk limitation within these limits. *These limits are without prejudice to those fixed by the PSP*. They may also …" Reasoning: PSP limits should not be impacted by the limit fixed by the TP.
Glossary of terms (page 16)	amendment	Proposal: "credential" - "*The personal and confidential* information ~~*- generally confidential -*~~ provided by a *TP to* a customer or *by an account servicing* PSP *to a customer or by an account servicing PSP to a TP* for the purpose of authentication. Credentials can also …" Reasoning: The words "generally confidential" are to be deleted because, in any case, each person equipped with credentials must keep them strictly confidential for its proper use. It may also be important to recall that there are three categories of credentials. These amendments seek to clarify the situation.

Issue	Comment	Reasoning
Glossary of terms (page 16)	amendment	Proposal: “payment initial services” - “Internet-based services to initiate payment transactions via payment accounts. ~~*The technical implementation of this service can differ based on whether or not the payee is actively involved in the payment initiation and whether the TP’s software is used by the account owner to transmit his/her credentials to the account servicing PSP.*~~” Reasoning: The second sentence is not a definition.
Glossary of terms (page 16)	clarification	Comment: a definition of sensitive data would be welcomed.