Ref.:EBF_000395
Brussels, 12th April 2013

EBF Position on ECB Recommendations for "Payment Account Access" Services

Launched in 1960, the European Banking Federation is the voice of the European banking sector from the European Union and European Free Trade Association countries. The EBF represents the interests of some 4,500 banks, large and small, wholesale and retail, local and cross-border financial institutions. Together, these banks account for over 80% of the total assets and deposits and some 80% of all bank loans in the EU alone.

Key points

1. The EBF welcomes the Recommendations of the European Central Bank for Payment Account Access Services and the opportunity given to provide input to the related consultation.

   The Recommendations represent a very helpful document since they are dealing with one area of high concern for the banking industry.
   Our objective in this response is to contribute to a positive, safe and fair outcome on the on-going proposals on access to accounts by TPPs.

2. The EBF generally regrets that the document is restricted to **a focus on conceptual security aspects** of payment account access services and that security aspects of these services are therefore considered in isolation.

3. The EBF believes indeed that important **legal, regulatory and consumer protection issues** should also be addressed when dealing with payment account access services.

   The Recommendations risk otherwise being incomplete.

   The EBF strongly pleads to bring the various discussions on the legal, technical and security elements around payment account access services together, rather than looking at each area in isolation. We do not think it is helpful that the security aspects are being defined (through the SecuRe Pay consultation) before the legal framework has been defined or before the practical aspects of the relationship between these services and the account servicing PSPs have been better elaborated. These elements are all interdependent and should be addressed as such.

4. The EBF believes the recommendations fail to address in an adequate manner the biggest security risk present in payment account access services: identity theft through phishing or impersonation of the payer.
   Research by the Merchant Risk Council identifies identity theft and account takeover as two of the top concerns for e-commerce service providers. In research conducted by the Aite Group with e-commerce merchants in 2012, 50% of the surveyed merchants noted a

"significant increase in account takeover". According to Aite, 50% of malware are designed to compromise credentials and allow identity theft.

5. The EBF has notably identified key concerns as regards **confidentiality and privacy issues** which, we think should also be addressed when treating the subject of payment account access services. European banks are heavily regulated as regards the sharing and protection of sensitive data through bank secrecy provisions and compliance with the current Data Protection Directive[1]. The recent proposal of the European Commission for a new legislative package on data protection issued on 25th January 2012 confirms this approach[2]. Providing sensitive account information of customer accounts to unknown entities which have no relationship with the customer's financial institution responsible for the account and which are not subject to equivalent supervisory and regulatory obligations as those faced by banks therefore raises very serious concerns.

   The current EU Data Protection Directive (Directive 95/46/EC) prohibits the processing of personal data without the consumer's consent for other reasons than for the performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding.

   The EBF fears that there are risks with payment account services provided by third parties (TPs) that other data than strictly necessary for the payment transactions are requested.

   The EBF also believes that the essential issue and the related risks of **data storage** should also be addressed when dealing with the payment account access services.

6. In addition to the key points above we believe it is very important to stress the fact that TPPs should be put under effective supervision. Many of the recommendations and Key Considerations in the draft recommendation only have a meaning if a TPP is put under effective supervision. TPs offering PAAS must comply with a clear legal and supervisory framework. Unregulated and unsupervised TPs having access to information on customers' payment accounts and the funds kept in those accounts is unacceptable in light of consumer protection. Also, it does not allow for a level playing field (fostering competition and innovation), and creates issues regarding security, liability, data protection and banking secrecy. Currently, supervision of TPs offering PAAS is still incomplete and unclear.

   The effectiveness of the KCs will depend on the establishment of an appropriate regulatory and supervisory framework.

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[2] http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf

I- General Part

1. The Recommendations miss a key requirement: **dual consent concept**.
This concept should be enshrined into a legal and/or contractual framework where the TPP has agreements with all other parties involved i.e. the merchant, the Account Servicer PSP and the PSP's client (consumer).

It may be that this requirement is tacitly assumed by the European Central Bank in its Recommendations. We consider however as essential that it is explicitly stated.

Clear contractual agreements between the three parties concerned (TPP, the payment account holder and the account servicing PSP) are essential. The underlying principle should be contractual freedom (contracts between parties should be voluntarily agreed upon), subject to competition law. TPs should only be able to operate if dual consent is provided, directly or indirectly via a scheme. Both agreements should address liabilities, privacy, security, non-repudiation and commercial terms.
Customers (payment account holders) should be made aware that personal security credentials, issued by their PSP, must never be handed over to TPs if there is no underlying contractual arrangement. Also account servicing PSPs should reserve the right not to recognize the TP as such, when there is no underlying agreement between PSP and TP. In that case account servicing PSPs should be allowed to block any transactions that they suspect are not directly initiated by the account holder, in order to protect the interests of its payment account holders.

Also the contractual relationship must ensure end-to-end service levels of the payment. This covers for the following: 1. The financial completion of transaction should be clear and unambiguous for all parties involved, 2. authentication credentials must be kept confidential (security) and 3. Transparent rules concerning liabilities, with a clear point of contact and responsibilities for handling of complaints.

As such the document falls short of optimum security. KCs 9.4 and 11.4 only cover account owner consent. This is highly regrettable and surprising. This is a major weakness and vulnerability which failed to be addressed.

How can end-to-end interoperability and security e.g. connectivity, authentication, encryption, non-repudiation, data integrity, resilience, generic APIs...be ensured between all intermediaries involved in the cloud of providers if there is no cooperation /agreement between all involved parties including for example Account Servicer (AS) and Third Party services Providers (TPP)?

Nevertheless KC 5.6 calls for: "Account Servicing PSPs should be able to differentiate between payment account services by third parties (TPs) and access by account owners without TP involvement". It is not clear how this would be achieved in practice without an agreement between AS and TPP?

In general we note that a more formal relationship (e.g. an agreement) between TPPs and AS PSPs is mentioned in / implied by some of the Key Considerations and Best Practices. But these combined do not result in a clear set of rights and obligations between the parties. The relationship between these two stakeholders is insufficiently

covered in the recommendations but it is a crucial aspect in understanding the responsibilities of each of the parties in the payment chain.

How will supervisors/overseers implement and enforce many of the recommendations in the absence of agreements between involved stakeholders and if TPPs are not properly being supervised?

We refer to the approved recommendations for the security of internet payments where there is a repeated requirement on PSPs to ensure the integrity of the security methods via contractual arrangements (see e.g. 3.4, 4.7, 4.8, 5.1 BP, 11.3). Some of the internet recommendations or best practices foresee that PSPs should "contractually" require e-merchants to comply with the necessary security requirements. We ask why these "contractual" requirements are not extended to TPPs?

In addition, the definition of 'Account Servicing PSP' in the glossary states that any outsourced functions should be under contract. Thus, it would surely make sense to require a similar level of relationship to exist between AS PSPs and TPPs.

2. The legal/contractual framework should provide for the consumer (account holder) having to give his explicit (written) authorisation to the TP and to his PSP before the TP can provide *any* services relating to his payment account. The account servicing PSP must provide its approval to the TP accessing the payment account and possibly initiating a payment transaction, comparable to a power of attorney. In addition to this, a number of other areas (e.g. allocation of liability, execution timelines, extent of information and service, information provided to customers) will be impacted by the relevant TP when accessing the payment account and possibly initiating a payment transaction.

   The relationship between Third Party service provider and the Account Servicing PSP is mentioned in some of the Key Considerations and Best Practices, but these combined do not result in a clear set of rights and obligations between the parties. The relationship between these two stakeholders is insufficiently covered in the recommendations (e.g. requirement for a "strong customer authentication").

3. Several recommendations call for cooperation or bilateral authentication between AS and TPP (see below our remarks on specific recommendations).

   This is only possible in cases where there is an agreement in place between AS and TPP .The AS must be aware ex ante of the involvement of the TPP. Otherwise the recommendations cannot work and will remain ineffective.

4. We will focus on Payment initiation services (PIS), not Account information services (AIS) which as defined are concentration services.

   The definition of PIS is incomplete: it should read: "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 –*and the payer*- 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."

5. Objectives of the recommendations: we feel that they are neither ambitious nor comprehensive enough.

   One objective in particular is missing: the recommendations should clearly mandate that fully-fledged agreements must be in place between TPP and PSP and between TPP and client, otherwise the Recommendations themselves would remain ineffective; these contracts should define rights and obligations and allocate liabilities between the parties.

   The Recommendations should clearly state that TPPs as any other actor operating in the payment chain shall be properly supervised and overseen by the competent Oversight Authority.

   - Then when setting "increased transparency" as an objective, the document limits transparency for account owners. This should be extended to transparency for Account Servicing institutions, for maximum security. TPPs are not transparent vis-à-vis the customers as to the fact that they use the customers' credentials to log-on to their internet bank.

   - "Traceability through proper authentication in all communications between the entities involved" cannot be achieved if there is no agreement between TPP and AS PSP. How can traceability and impersonation of the customer co-exist? We indeed believe that the TPP needs to identify and authenticate itself to the AS.

   - "Improved exchange of information" is not enough. It should read:"Mandatory exchange of information". It is stated that "Improved exchange of information in the event of repudiation, security incidents and/or fraud" is one of the requirements the recommendations should meet. A requirement should also be that it needs to be clear which involved party is responsible in which part of the end-to-end process in the event of repudiation, security incidents and/or fraud.

6. Legal Basis: we attach the EBF comments regarding Access to Accounts in our response sent to the EC consultation on the PSD review (see attachment).

   The suggestion that Account Access Services are brought within the scope of the PSD is helpful.

   In the meantime it is suggested that "Currently, the legal basis for implementation of the recommendations is the existing oversight and supervisory competence of the relevant authorities". It is not clear how this interim measure would work in practice and further explanation would be welcome.

   Until changes to the PSD are incorporated into EU/domestic laws, the legal basis for these services is unclear.

We conclude that it would be logical for these PAAS recommendations to be finalised only once there is more clarity on how the legal framework around these services will be defined.

7. Scope and addressees: The recommendations are not specific to TPPs but very much based on the Recommendations for the security of internet payments (see for example Recommendation 6). They do not take enough into account the specificities of PIS and more specifically of overlay services with impersonation of the payer.

   Furthermore, rules regarding non-EU based TPs providing services within the EU should be clarified.

   Do these guidelines cover eWallets as well as Third Party Service providers?

   Indeed the eWallet provider may guide the customer to an account with another PSP.

   The major risk carried by access to account services by third parties is the risk of identity theft i.e. the theft and misuse of a payer's identity through his credentials to initiate payments not authorized by the payer. This form of fraud is rapidly growing on the internet.
   According to the 2012 Identity fraud report released by Javelin Strategy and Research, in 2012 12,6 million consumers have become victims of identity fraud in the US and fraudsters have stolen over USD 21 billion.

   Over the summer of 2012, 30.000 European online banking customers were robbed of nearly 36 million euro. The attack campaign was discovered by software company Versafe and Check Point software Technologies and named "Eurograbber".
   Many other recent examples of identity theft or phishing to get access to a customer's account appear regularly in the specialized press.
   To reduce this risk to the minimum possible, all payment orders should be initiated by the payer himself.

8. Consistency with other EU and National Legislative texts-Applicable laws

   Many existing or in-the-process legislative/regulatory texts deal with internet transactions and/or payments.
   We suggest a "consistency check" be carried out in order to make sure there is no contradiction/impediment/exclusion between all of these texts.
   A thorough legal assessment must be carried out, to ensure amongst others compliance with data protection and banking secrecy laws - especially ensuring that PSPs are not compromising any regulation imposed on them today.
   As a matter of illustration, we mention the General Data protection Regulation, the 4th Anti-money laundering Directive, the Regulation on electronic identification and trusted services for electronic transactions in the internal market; directives on cyber-crime; the proposal for a "Directive of the European Parliament and the Council regarding measures to ensure a high common level of network and information security across the Union", published on 7 February 2013; the Regulation on information accompanying

transfers of funds , more specifically Article 2(6) thereof and the definition of "intermediary PSP" which could apply to TPPs.

In Italy Banca d'Italia issued a regulation implementing PSD obligations on the PSP and PSU relating to the use of payment instruments (e.g. as regards handling of sensitive customer data). According to this regulation it is necessary that the AO obtains authorisation from the AS before giving the codes for the use of the payment service or instrument to third parties. *"[…] Where the contract between payment service user and provider prohibits the former from communicating personalized security features to third parties, infringement of this prohibition constitutes negligent conduct by the user".*

In another EU country, banking secrecy is constitutional law. Due to national law the customer has to allow his account servicer expressively and in writing to give account information to third parties. This allowance includes the scope of the access to the third party.

9. Global Dimension

Internet purchases, by definition, can take place with one of the parties (the consumer, merchant or TPP) not being established in the EU. Consumers could therefore be enticed to give their credentials to a TPP not established in the EU, not subject to EU regulation nor ECB recommendations, will all the possible negative consequences in case a problem arises with the payment. Europe has very high standards with regard to security of payments. It cannot be that these standards are lowered in any way under the pretext of encouraging new entrants in the market. This would be welcome only by fraudsters.

II- Recommendations

- **Rec. 1: Governance**

  Will the governance authority have a role in approving TPs such that PSPs themselves need not vet the TP and its procedures?

  It would indeed be inefficient for PSPs to have to vet every TPP.

  BP 1.2 requires cooperation between PSPs and Third Party Service Provider (TPP). This B.P can only be put in force if an agreement is put in place between the Account Servicer (AS) and the TPP. Will cooperation be enforced by the supervisors/overseers or by law?

  It is not clear whether the minimum technical and security standards will be defined multilaterally as part of the GA's duties or bilaterally between particular TPs and PSPs nor how they will be enforced.

- **Rec. 2.1: Risk Assessment**

  We are supportive of the intention to require GAs and TPPs to consider potential risks to AS PSPs in their risk assessments. However, it is not clear how this would be achieved in practice without a formal relationship (e.g. a contract) in place between the AS PSP and the TPP. For example, the KC suggests that the GAs and TPPs need to '*consider the risks associated with the chosen technology platforms, application architecture, programming techniques and routines… on the side of the AS PSP*'.

- **Rec. 3: Incident monitoring and reporting**

  KC 3.3 and BP 3.1 recommend procedures for cooperating and arrangements between TPs and PSPs. This can only be put in force if an agreement is put in place between the Account Servicer (AS) and the TPP. We believe that a procedure should be setup which clearly describes how the TP and account servicing PSP should co-operate in the event of a security incident. This should be covered by the agreement in place between account servicing PSP and TP.

- **Rec.4: Risk control and mitigation**

  - KC 4.8

    There is an option for TPs to outsource functions related to the security of payment account access services. This may increase risk to customer and the payments system. While in theory risks from out-sourcing can be managed and liability clarified, in practice having several layers of parties to the transaction is likely to make managing risk less effective and/or cumbersome and costly.

  - KC 4.9

    Not only should TPs not authorise e-merchants to store sensitive payment data, they must ensure it does not happen and take action in case of a breach.
    Were sensitive data to be misused or lost this will present a major risk to customers and the payment system.

- BP 4.1

  What exactly are TP security tools? TP security tools have to be described in detail, including liability. Also, the security differences between PSP credentials and TP security tools need to be explained. This is a crucial issue, in order to maintain trust.

- **Rec. 5: Traceability**

  - In our view 'traceability' is probably not sufficient. Customers and PSPs have a right to know upfront about the relevant details of the TPs prior to using or relying on their services. This should be reflected in a new KC.
    It is for this reason that for example current Italian legislation requires that customers must obtain the authorization of their PSPs before divulging the codes for the use of the service or payment instrument to TPs. This permits providers to identify requests for security codes from parties simulating a legitimate request, as in the case of phishing attempts. In addition, this also allows the limitation of the risks associated with the use of payment services over Internet platforms (especially those services that draw on an account, such as bank transfers) not authorized by the PSP employed by the user (known as "overlay services").

  - The aspect of **impersonation** of personal security credentials is of major importance from a liability (please refer to PSD Articles 56, 57 and 59), banking secrecy and data protection perspective.
    The practice of impersonation and the legal and regulatory issues raised as a result of some of the impersonation practices should be addressed in these recommendations through specific new KCs.
    A new KC should reflect the need for TPs to authenticate themselves towards the PSPs prior to accessing the account in line with the statement on top of page 3 (first indent) of the recommendations.

  - The recommendations as currently drafted do not seem to address the question of how compliance with existing national legislation for PIS which could be seen to be at odds with the recommendations can be ensured.

- Again KC 5.4 and KC 5.5 call for cooperation and proper bilateral authentication between TPs and AS PSPs. This can only be put in force if an agreement is put in place between the Account Servicer (AS) and the TPP.

- We believe that KC 5.6: "Account Servicing PSPs should be able to differentiate between payment account services by Third Parties (TPs) and access by account owners without TP involvement" is fundamental. This key consideration is unfortunately not met today in all cases with Payment Initiation Services (PIS) by overlay service providers who impersonate the payer using his/her account credentials without the knowledge of the AS and who refuse to enter into agreements with AS.
  AS cannot be given the responsibility for this differentiation if they are not provided with the practical means to do so i.e. if the TPP does not identify itself to the PSP and impersonates the payer.
  It can even be argued that even with an agreement, it may be impossible to make this distinction.

- BP 5.1 (special credentials provided by AS to enable use for PIS) is interesting but would certainly bear a cost to the AS. In the absence of appropriate agreements, how would costs and liabilities be distributed between the parties? This approach is likely to require a major rebuild of online banking services. It may be disproportionate and alternatives should be sought.

  This Best Practice could be interpreted as the only method of detecting when a TP is the one accessing the account and not the customer and is therefore a natural consequence of KC 5.6. We however believe that it is [totally] unrealistic that a PSP should issue two sets of credentials. One when the customer is using his "normal" internet banking service and another when a TP is being used. We would point out that, while perhaps being technically possible, the use of specific security credentials with PAAS will potentially lead to further confusion for the customer and may lead to errors. We do not believe that all customers would be able to diligently handle two sets of security credentials. In addition to being costly and complex, such scenario would risk leading to erroneous use of the credentials.

  This BP therefore raises a lot of questions. Should PSPs allow customers to hand over bank-delivered credentials to (any) TP? Or, should the PSP keep control over *which* TP the customers can hand over credentials to, also without an agreement between TP and PSP. Which criteria should apply for such an evaluation of TPs?

- **Rec. 6: Initial customer identification and information**

- It is not clear to whom the customers should confirm their willingness to make use of account access services. To the TPP? To the AS? To both? We strongly believe that this consent also needs to be communicated to the AS PSP.

  The PSP needs to have assurance that the mandate given to the TP is properly implemented and then the service is being properly operated. It needs to understand its liability in case of unauthorised transactions and those cases where its customer may have a claim against the TP.

  If the TP is insolvent how are any outstanding claims resolved?

  This again relates to the lack of clarity around the legal framework for these services. We therefore suggest that it is more logical to wait to finalise the PAAS Recommendations until it is clear how these services will be defined under the PSD (which will also help facilitate the wider discussions around payment account access). Clarity on the legal framework for PAAS would ensure that the responsibilities of all parties to detect and prevent money laundering are understood.

- KC 6.2 seems more applicable to the relationship AS-Account Owner (AO). It is based on the *Recommendations for the security of internet payments*.

  We assume that there is no new liability for PSPs. All parties must be clear as to their risk and liability. PSPs not involved in a transaction should not be liable.

- KC 6.3: Change the sentence to: "Block a transaction or the payment account access service on the basis of security concerns"

- **Rec. 7: Strong customer authentication**

  KC 7.1 calls for an agreement between TPP and AS PSP. This can only be put in force if an agreement is put in place between the Account Servicer (AS) and the TPP.

- **Rec. 9: Log-in attempts**

  KC 9.4 is where AS agreement should be made mandatory on top of AO's specific consent for optimal security (Dual consent concept).

- **Rec. 10: Monitoring:**

  KC 10.5 calls for active cooperation between all professional entities involved in the account access service including TPs and AS PSPs in case of fraud. This can only be put in force if an agreement is put in place between the Account Servicer (AS) and the TPP. The duty to co-operate to deal with fraud or dispute needs to be more precise and stronger.

- **Rec. 11: Protection of sensitive payment data**

  We question whether a TP should be able to *store* sensitive payment data at all. Data protection requirements must at all times be observed.

  - KC 11.2 requires end-to-end encryption between the communicating parties. Is this possible if there are no agreements between TPP and AS PSP?

  - KC 11.4 is where AS agreement should be made mandatory on top of AO's specific consent for optimal security (Dual consent concept).

  - BP 11.2 may not be possible with many e-banking portals where information on all the customer accounts is immediately visible and accessible from the access page (home page). Changing this would entail important costs, which in the absence of contracts, would be impossible to allocate.

- **Rec. 12: Customer education and communication**

  Further consideration needs to be given to the issue of communication to customers on the importance of keeping their security credentials safe. Currently, Article 56 of the PSD (in conjunction with the Terms & Conditions of the AS PSP) is clear that customers should not divulge their security credentials to any third party and a great deal of effort has been expended in anti-fraud messaging to make this clear to customers. Thus there is potentially an inconsistency with regard to PAAS which needs to be addressed. Indeed it is potentially confusing for TPPs to educate customers on the need to protect their security credentials, whilst at the same time requiring them to divulge their online banking credentials to a third party.

  It is essential that customers understand the liability regime they are entering into when TP and how this may differ from other payment methods.

- KC 12.3

  The requirement that TPs make assistance for all queries available to customers needs to be stronger. In particular consideration should be given to a single point of contact for customers to use in case of disputes. Without such an approach consumers may find themselves being passed from one party to the other (TP, PSP, GA, merchant) possibly with no-one taking responsibility.

- KC 12.6 requires from TPPs a transparent liability regime to customers and the functioning of a complaints process. This is not enough: for maximal customer security; a transparent liability regime and the functioning of a complaints process must also exist between TPP and AS PSP.

- KC 12.9

  The requirement for customers to give permission to TPs to use data needs very careful consideration. Even if agreed, disclosure needs to be the minimum required to operate the services. Customers are at risk if they disclose sensitive data. It needs to be clear that they understand the risks of doing so and that those TPs can handle it safely. It would be better if other methods were developed so no such disclosure was made.

- **Rec. 13: Notifications, setting of limits**

  It is unclear how the limits applied by TPPs will work in conjunction with the limits of the AS PSPs. Again, it seems to indicate that a more formal relationship between TPPs and the AS PSPs (e.g. a contract) would be necessary. We refer back to our argument made under point 2: defining the security requirements of PAASs in isolation is not logical or advisable. Other aspects, such as the legal framework and the nature of the relationship necessary between AS PSPs and GAs/TPPs, need to be discussed further in order to fully analyse the implications of some of these recommendations and whether they are fit for purpose.

III- Glossary

- There are very different understandings and interpretations of the exact services covered by the terms PIS and AIS. This leads to quite some confusion on "what exactly are we talking about" and on the way these services operate in practice. Unfortunately the literature available from the service providers themselves is not always clear (nor complete) about the precise process flow of the services offered-especially for PIS.

  Therefore, we deem it essential to start by clarifying the exact terminology and process flows. As a matter of illustration, very different terms with very different meanings and processes are used to define PIS: overlay services, pass-through services, payment messaging services, impersonation services, software-based services, protocol-based services, indirect access, re-direction services, etc.

  The 3 types of PIS identified by the ECB are not comprehensive enough to really differentiate the services and the crucial question of who really accesses (i.e. logs-in to) the on-line account (the payer, a software? a third-party with or without a proxy).

- **Account Servicing PSP**: It is mentioned that "any outsourcing (by AS PSP) must be based on a contractual agreement defining the parties' respective rights and responsibilities". This requirement shall apply equally to overlay services which should also" be based on a contractual agreement defining the parties' respective rights and responsibilities" between AS PSP and TPP.

This difference in treatment is not understandable.

- **Credentials** are defined as "generally confidential" information. We believe this definition is weak and may go against many legislative and regulatory obligations referring to credentials (see PSD).

- The definition of **Payment initiation services** is questionable and not precise enough. It only speaks about payee involvement, ignoring the degree of payer involvement and limits the use of the TP's software to transmit the AO's credential's to the AS. It totally ignores the cases where the TP's software is used to impersonate the AO and use his credentials to access the account. These later cases are however precisely the riskier ones and those which deserve full security attention.

- It would be beneficial to include examples to the definitions of the Account Information Service and Payment Initiation Service (on page 2) to illustrate the type of service the ECB links to each of the classifications. In particular to illustrate the difference between a 'service used to initiate a payment transaction via a person's internet-enabled payment account' and a standard internet payment governed by the Security of Internet Payments Recommendation.

* * *

Contact Persons: Mr. Patrick Poncelet: p.poncelet@ebf-fbe.eu and Mrs. Séverine Anciberro, s.anciberro@ebf-fbe.eu

Attachment: EBF comments regarding Access to Accounts in our response sent to the EC consultation on the PSD review.

EBF Comments regarding Access to Accounts in our response sent to the European Commission consultation on the PSD review

Our general stance is that the entry of new players and forms of payment should be encouraged, provided it does not undermine the integrity of existing payment systems or expose customers to undue risk of fraud.
Technical and business model neutrality should be driving forces when defining rules about payment services covered.

In the end, the purpose of extending the PSD scope to third parties accessing payment accounts, such as overlay services is mainly to:
(i) give consumers and merchants confidence in the financial and business reliability and integrity of the overlay service providers;
(ii) protect payers from potential security breaches, fraud and unauthorised transactions; and
(iii) protect the PSP of the payer from security risks and liability for unauthorised transactions initiated by an overlay service provider or other third party accessing payment accounts.

We will comment only on overlay services.

It would be useful if the revised PSD clearly indicated if overlay services fall within or outside the scope of the PSD and consequently if overlay payment service providers fall within or outside the realm of the PSD. As a general principle, it can be argued that any new entity which appears in the eyes of customers to make payments, such as providers acting on behalf of end-users and acting as an intermediary between a PSP and its customer, needs to be regulated and supervised appropriately, with the goal of ensuring that any risks are managed, and that there is a level playing field.

Currently there are several different types of overlay service providers. Overlay services that require the customer to give out his or hers credentials must be regulated. In addition, they should not be allowed to conduct business without an agreement with the payment account servicer. This means that agreements between all parties involved - with clear description and allocation of liabilities - should be at place. Overlay services should only be able to operate if consent has been given by the customer as well as the customer's payment service provider. This is due to the possible security risks, liability, data protection and cost/benefits issues, amongst others that arise. Moreover, should a customer use an overlay service provider for initiating an online payment, the security level offered should be equivalent to that of the customer's online banking application, in particular for the initiation of payments.

As regards the question which other issues should be addressed (data protection, security issues) and in which regulatory framework, EBF wishes to reiterate what it stated in its position paper dated 5 April 2012 over the Green Paper towards an integrated European market for card, internet and mobile payments, namely:
Access to personal data, especially of a financial nature, requires high protection. Access by third-parties to any information on payments accounts is only thinkable provided that it does not undermine the integrity of existing payment systems or expose customers to undue risk of fraud.

In any event, providing sensitive account information of customer accounts to unknown entities which have no relationship with the customer's financial institution responsible for the account and which are not subject to equivalent regulatory obligations as those faced by

banks raises very serious concerns. It needs to be recalled that European banks are heavily regulated and supervised as regards the sharing and protection of sensitive data through bank secrecy provisions and compliance with Directive 95/46/EC. The recent proposal of the European Commission for a new legislative package on data protection issued on 25th January 2012 confirms this approach.

Overall, a consensus needs to be reached at European level over the conditions whereby access to information about the availability of funds could be granted to third-parties other than the account owner (principles based). It should start by defining what is exactly meant by "giving access to information", to what information precisely, in which circumstances, for what purposes (e.g. evaluating the ability to pay?) and then define the conditions. To begin with, a clear definition of the services and activities provided by overlay service providers should be given in the revision of the PSD. Not only should these actors be granted an appropriate status, but their activity should be clearly identified in the scope of the PSD.A driving factor should be the contractual coherence between the actors involved in the payment process end-to-end.
At the very least, pro-active and case-by-case authorisation by both the account owner and the account-holding institution on the exact nature and scope of the information to be given access to should be minimal conditions to safeguard sensitive data. Overlay service providers tend to rely only on customer's consent. Customer's consent should not however be sufficient. Contractual relationship between the account servicer and overlay service provider must be the *sine qua non condition* of using online banking platforms and account information. It should also be acknowledged that the account servicer should be free to evaluate potential risks related to such services and service providers individually in the account servicer's own terms and perspective, keeping also freedom of contract in mind. The account servicer should also be granted a right to step in when necessary.

Overlay services are commercial services that use information retrieved from private data bases and systems owned and maintained by the account servicer, so there are also issues related to intellectual property rights and constitutional protection of property.

In any case, the EBF suggests waiting for the conclusions of the Eurosystem's SecuRePay forum which is precisely addressing the security aspects of payment account access.

Regulations should be implemented that prohibit any payment initiation or access to account information by proxy from a payment account when it is not made evident to the account servicer that it is made by proxy, so that the account servicer may assess the validity and identity of the proxy – this is the rule in the physical world and it should prevail also for e- and m-payments.

A third party accessing the customer's account by using the customer's personal security authentication details would have the opportunity to review all personal and private financial data, which without explicit customer consent would be a breach of personal data privacy.

The EBF would like to emphasize that most on-line banking portals were designed in such a way that giving one's credentials to access the portal means giving access to all information about the account owner (his accounts, his transactions, his securities holdings, savings and placements, insurance, mortgages, credits, payment cards etc). Substantial concerns arise in terms of confidentiality and security of such data. Even a single transaction may also include indirectly delicate information of a person register (transactions related to health care services

etc.) regarding not only the customer but also his/her family member or other person on whose behalf the transaction is made.

On the other hand, trying to restrict access just for information on an account or to initiate a payment would entail important changes and therefore costs, contrary to what one specific overlay payment service provider publicly and constantly affirms ("no additional costs for banks"). These additional costs would be totally disproportionate with the benefits brought about because there exists many valid alternative business models enabling the same effect i.e. the possibility to initiate an on-line credit transfer or direct debit transaction using a payment account but without the need to resort to an intermediary "man-in-the-middle service provider. These alternatives to overlay services have the very serious advantage that the payment would be directly initiated by and totally in control of the payment account owner himself.

Servicing payment accounts which entails a very wide range of products and services linked to the account, may not be reduced to a simple "host" for the account acting as a bridge with other economic actors, and making the information associated with the account easily accessible by other economic actors for their own benefit.

There needs to be full transparency on responsibilities and liabilities and there cannot be any enforceable liability in the absence of contracts between parties establishing these.

Banks are not permitted to provide third-parties with information linked to an account without the prior approval of the customer. By doing so, the bank would stand the risk of breaching data protection, privacy and banking secrecy laws. Ultimately, transparency is paramount – customers should be aware who has access to what information and the account holding institution should be informed if operators are making use of the online banking systems, i.e. service providers should have to seek consent from the account servicer for access to the account information.

It would, however, be difficult for customers to fully understand where their information is being used and by whom, which service they are currently logged in and who is ultimately responsible for the service. The overlay service transfers to and processes information in its' own systems and platforms. Information might be processed also outside the EU/EEA. The customer should be provided with all relevant information on the service by the overlay service provider in accordance with relevant legislation applied at consumer's place of residence.

Banks for example do not have access to account information in other banks.

For the security of the account holder, the personal security / authentication code or device may not be presented to anyone else. This is supported by the PSD.

Banks also face sophisticated criminal threats on the Internet, including so-called "man in the browser" malware which attempts to mimic and subvert the behaviour of a customer. In some cases attempts by a payment service operator to obtain account information or to initiate payments can trigger banks' security and anti-fraud systems, leading to unintended consequences for the customer such as the rejection of a payment or the suspension of the customer's account.

Effective data security is a fundamental requirement both from the customers' and the service providers' perspective. Techniques used by overlay service providers can directly compromise both technical and functional data security. After the transaction has been initiated and processed it may be impossible to find out whether it is the customer him/herself or a potential middle-man who has initiated or confirmed the defected payment orders and who actually submitted data content to the transaction If customer communication and services are allowed to be interfered or exploited by third parties which are neither identified by the account servicer nor regulated in accordance with the PSD, any amendments related to account servicer's or consumers' liability will provide only partial or insufficient solutions.

It would for example be important to assign liability for unauthorised transactions and transactions that go wrong; for the authorities to ensure that the service provider's systems and controls are strong and secure, and that complaints and redress procedures are in place.