Response to the public consultation of the ECB on Recommendations for "Payments Account Access" Services

Provided by ABI

March 2013

1. Introduction

The Italian Banking Association (ABI) has prepared this document in response to the public consultation on the Recommendations made by the European Central Bank in relation to account access services ("*Recommendations for "Payment Account Access" Services*", hereinafter, the "Recommendations"), after gathering comments from ABI Members as well as from the ABILab Consortium (Centre for banking research and innovation) and "CBI - Corporate Banking Interbancario" (manager of technological infrastructure for corporate banking that allows interchanges between consortium members in relation to payment services and document management).

The Association welcomes the 14 Recommendations which the *European Forum on the Security of Retail Payments* (henceforth, the "Forum") prepared because they contribute to defining the prerequisites which non-regulated "Third Parties" (henceforth, the "TPs") must comply with when they offer services for accessing information on payment accounts. These Recommendations not only concern aspects related to security but also those pertaining to transparency and traceability; they represent the natural continuation of the "*Recommendations for the security of internet payments*"; whose final version was recently published by the ECB.

This consultation is of relevance given the significance of the topic and the impact which the Recommendations can have in consideration of the risks of violation of security and the protection of the personal data of affected users. With regard to this point, it should be noted that the Italian banks had already expressed significant reservations in these areas at the time of the consultation of the European Commission on the *Green Paper* "*Towards an integrated European market for card, internet and mobile payments*" as well as when providing their contribution to the Commission in relation to the open questions in the revision of the PSD (refer to Attachments 1 and 2).

We believe that the introduction of the Recommendations within the oversight and supervisory frameworks of EU competent authorities will allow for:

- a greater formalization of the processes;
- a clear assignment of responsibility to all parties involved in a payment transaction;
- an increased level of attention in stipulating agreements with TPs.

This is particularly true because the Recommendations also target the so-called "Third Parties".

However, the Recommendations under consultation are very similar to those already issued in relation to the security of online payments and do not seem to capture potential specificities and peculiar features that are typical of TPs.

2. General observations

First of all, the introduction of the future final version of the Recommendations within the framework of the Monitoring and Supervisory Authorities is not exhaustive of all regulatory aspects. For the purposes of ensuring a level playing field, an effective protection of users and the proper functioning of the payment services, we deem it essential that – as recommended in the document itself – the suppliers of account access services must be **governed by binding norms, beginning with the rules which already are in force for payment service providers (PSPs)** under the Payment Services Directive. In other words, they should be subject to the PSD legal framework, thereby rendering them equivalent – in terms of status and responsibilities – to all other PSPs.

In fact, the operation of the so-called TPs is effectively that of PSPs: the Recommendations themselves lead to conclude that a significant part of the phases through which an e-payment service is effected – and that were well described in the document – are provided by the so-called TPs. If there were still areas which require regulation once the TPs in question are subject to the same the regulatory framework of PSPs themselves, the process of the PSD revision (PSD2) which is underway could serve as an opportunity to fill out these areas.

In addition to obvious reasons pertaining to the creation of a level playing field between operators which act within the same market, the extension of PSD rules to TPs seems to be an essential condition in order to appropriately regulate the obligations and responsibilities of all parties which are part of the supply chain of an online payment as well as to ensure that their relations are stipulated in a contract in a transparent and effective manner. The **contract** is, in fact, a key element that cannot be ignored. The Recommendations seem to assume - without ever stating so explicitly – the presence of contractual agreements between PSP and TP and between the latter and the user. We believe that this **requirement must be stated explicitly and rendered mandatory given that many of the Recommendations would not be applicable in the absence of this contractual agreement.**

Moreover, the final Recommendations on the security of internet payments - published by the ECB at the same time of initiation of this consultation – had already, in a number of instances, referred to aspects pertaining to security, data protection and traceability which the PSP must include within their contracts with online merchants; it is also stated that a default, on the part of the e-merchants, with respect to the obligations defined in the contract can lead to its cancellation. We believe that the same approach should also be applied when TPs are included within the payment chain.

With regard to this aspect, it should be noted that regulations currently in force in Italy (Provision of the Bank of Italy implementing section II of Legislative Decree 11/2010 of July 2011) already state that "*overlay services,*

where not accompanied by agreements with the Payment Service Provider*, are especially exposed to the risk of fraud*".

Within the contractual structure, each PSP must, in any case, be free to decide whether to allow TPs to offer their services to its customers and to refuse this offer if the TP does not comply with security criteria that are acceptable to the PSP and which can be verified by the competent Authorities.

Another aspect which should be considered within the Recommendations is that relative to **risk management systems**: in fact, it is not explicitly provided that TPs execute stress tests or worse case scenarios as is, conversely, required for regulated banking entities. This fact – in addition to creating a "weak link in the chain" which could negatively affect other parties and customers – creates a sort of competitive disadvantage. We would therefore request that provisions for TPs in this area be rendered uniform with those applied to other entities.

In addition, we believe it is necessary that these Recommendations - although focusing on security factors – should also clarify certain essential elements pertaining to **customer authentication credentials** and that they opportunely distinguish the characteristics of the various operational models: for example, the Recommendations and best practices should be scaled on the basis of the difference between the so-called "aggregators" and the TPs[1] and in relation to the volume of transactions that are processed as well as on the basis of an accurate risk assessment.

In particular, the implementation of a PCI-DSS certification is required; the three primary prerequisites are:

- data security;
- the standardization of accesses;
- an audit of TPs by an independent regulatory authority.

While, as regards security issues, it is possible to consider the possibility of utilizing "open" standards for the interactions between the various players (e.g. *ws-security*, SAML…), we fully agree with the intention to regularly update the Recommendations which, despite being drafted in accordance with principles of general nature, require continuous revision as technologies advance and new methods of fraud are created.

Regardless of the technical solutions which will be implemented, it should be noted that the customers must not share their security credentials with the TPs, in accordance with what is already established by the aforementioned Provision of the Bank of Italy implementing section II of Legislative Decree

[1] With regard to this point, a distinction should be made - in the "definitions" sections - between *payment integrators* which are already subject to the aforementioned final Recommendations on the security of internet payments, *account information services* and *payment initiation services* which are the subject the Recommendations under consultation.

11/2010, issued in July 2011 (refer to the extract of this Provision that is reported as commentary to Recommendation 6).

With regard again to security measures which should be adopted in order to prevent data breaches, it is not clear how these can be defined between the parties and guaranteed (e.g. in the case of end-to-end or cryptography procedures, etc..) without having all affected parties explicitly reaching an agreement. There are multiple risks of a data breach for which the bank could become liable; the bank could become exposed to litigation with the consequent risks of sanctions - both financial and non - if the obligations of all the parties and their relative responsibilities are not clearly and explicitly defined.

This is even more true if one considers the fact that EU regulations must take into account the specificities of national regulations pertaining to **data protection.** In Italy, for example, banks will soon (December 2013) be required to implement a series of security measures prescribed by the Guarantor in addition to those already required by the Privacy Code and Directive 95/46/EC itself; these aim to trace accesses to bank data in order to avoid data breaches.

Finally, with regard to sensitive data, certain critical factors and risks of violation of both national and EU regulations should be noted.

In particular, and specifically in relation to these critical factors, access of TPs to payment accounts must be limited to the sole request for the balance of the payment account; as a result, the possibility of a complete access to all accounts – with details of operations or access to other accounts of the customer (e.g. savings accounts) - must be excluded.

Activities by TPs within the account, on the other hand, should be prevented (e.g. payment operations, guarantees on the availability of funds, blocking of funds, etc.).

Each PSP must always and in all cases by capable of respecting privacy and the obligations deriving from banking secrecy that are imposed by national and EU regulations.

The handling of customer data on the part of the banks - including data access, communication and storage - is regulated in a very rigorous manner. The communication of this data to TPs can only be implemented - without the consent of the customer – in the cases that are explicitly determined by the law (such as the execution of a legal or contractual obligation). Finally, it should be stressed that TPs should be prevented from acquiring or accessing any data of the customer which is not necessary for purposes that are strictly related to the payment transaction.

Customers must be correctly and directly informed by the bank of the limits set for such access services. Customers must be aware of the fact that the

bank will not be held liable for any potentially fraudulent activity that is linked to the access of their accounts by TPs.

In summary, we believe that the Recommendations should be supplemented with the following:

- specific rules pertaining to responsibilities, thereby creating uniformity between the rules applied to TPs and the current ones for PSPs that are authorized under the PSD;
- certification on the part of the TPs;
- access to payment accounts should be limited to the request for the account balance;
- access services must be optional so as to always guarantee compliance with currently effective privacy and data protection regulations;
- rules which aim to create "greater transparency" not only for account holders but also for the PSPs which manage the account in order to guarantee maximum security, the relative communication activities on the part of the PSPs and the TPs must be made mandatory;
- a provision for contracts/agreements between the TP and the *Account Servicer* (AS) which guarantees "traceability through correct authentication during all communications between affected parties"; we are, in fact, convinced that the TP must identify and authenticate itself with the AS;
- obligation for information disclosures between TPs and PSPs.

With all of the above incorporated within a regulatory regime – PSD2 – that is defined at the level of the EU.

Finally, it should be noted that the period of time required to implement the Recommendations under consultation must be at least 24 months from the date of publication of their final version.

3. Observations on the individual Recommendations

Our specific observations regarding these Recommendations, as well as the *Key Considerations* and *Best Practices,* are presented below.

Recommendation 4 – Risk control and mitigation

We recommend clarifying, within the first phrase, that the "layered" security level must be decided autonomously by each party on the basis of a risk analysis.

Key Consideration 4.8

As noted in the general section, we believe it is necessary that relations between the PSPs and the TPs should be subject to mandatory contractual agreements at all times. This recommendation, in fact, covers the "final" relationship of the TPs and not the relationship between PSPs and TPs which, on the other hand, must be governed by the EU rules pertaining to payment

services (PSD2) and by specific agreements that are subject to free negotiations between the parties.

Best Practice 4.1

The implementation of this BP could be complex if, e.g., the TP and the customer are in different and distant geographical locations. The subsequent evaluation on the part of the authorities must take this aspect into account.

Key Consideration 5.4

Cooperation between many different parties (which in turn may have conflicting interests) can be very complex. For this reason, this cooperation must be based on legal norms that are binding for all affected parties, in particular for those which currently are not regulated and which, as previously noted, should instead be included within the scope of application of PSD2.

In fact, and solely on the basis of these Recommendations, cooperation between actors within the supply chain of the payment operation could result in conflicts if the actions of the various parties are not coordinated (e.g., if a TP repeatedly refuses operations whose execution the payer relies upon as a result of its agreement with its PSP and, for this reason, complains to the latter; or in the case that, following a fraudulent operation, the PSP of the payer is forced to reimburse the latter despite the fact that the transaction was generated by the TP non complying with the Recommendations, perhaps only with contributory negligence).

Key Consideration 5.5 and 5.6

With regard to authentication, it should be noted that the standards should be set by the PSP which manages the account and not the TP; these should obviously comply with the Recommendations already issued by the Forum for internet payments given that these standards are also those which the PSP utilizes with respect to the user.

In order to prevent potential situations of competition, it would be preferable to promote the use of “open” protocols (e.g. *ws-security*, SAML, …).

In any case, we do not believe it is possible that the PSP should have two sets of credentials which would be used in the case that TPs are or are not present.

Best Practice 5.1

In accordance with that also reported in KC 4.9, we believe that transferring credentials through TP components is very risky for data security.

Recommendation 6 – Customer identification

We believe it is necessary to introduce a KC which regulates the communication - to TPs from the user - of the codes which the user utilizes for the payment service or the payment instrument in order in order to fight and prevent the theft and misappropriation of customers’ digital identity.

With regard to this point, it should be noted that this issue has already been covered in the Provision implementing section II of Legislative Decree 11/2010 which implemented the PSD in Italy, issued by the Bank of Italy in July 2011. In particular, and in the case that the payment is made remotely – e.g. by means of a telephone device or Internet web site – it is "*necessary that the user obtains an authorization from his/her PSP before supplying third parties with the codes relative to the use of the service or of the payment instrument*: *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 payment service provider employed by the user (known as "overlay services"). If the contract between the user and provider of payment services prohibits the former from divulging security codes to third parties, breach of this prohibition constitutes negligent conduct on the part of the user, and thus represents grounds for forfeiture of the exemption from liability in the case of anomalous or unauthorized transactions".*

The current version of the Recommendations therefore does not seem to cover this issue in detail; in addition, if these Recommendations are approved without modifications, they could turn out to be in conflict with Italian regulations currently in force.

Key Consideration 6.2

For reasons identified in this KC, we believe that the participation of the TP within a scheme or a single transaction must be subject to a contractual agreement that covers all elements, both with respect to the user as well as the PSP which manages the account.

Key Consideration 6.3

We believe that the obligation set forth in this KC in relation to only the TPs risks rendering the PSP non-compliant and is therefore not in compliance with the provisions of the PSD. It is, in fact, inadmissible that the TP could block a transaction (even with a contract that provides for such a scenario) without the PSP being aware of it, thereby risking being liable on the basis of the PSD. It should again be reiterated that the obligations and responsibilities of all intervening parties – and, in the case in question, the responsibilities of the TP with respect to both the user and the PSP - should be governed by the same single legal framework.

Recommendation 7 - Strong customer authentication

Note 19 appears to state that only a single dynamic PIN could comply with the requirements of these Recommendations. It should be noted that this solution is not very widespread unless a "dynamic token" or digital signature is used. We would request a confirmation that this is the correct interpretation of the Recommendation.

Best Practice 7.1

We would also request a clarification as to which technological component should be "tamper resistant": the one provided to the customer or the entire structure. We believe it should only be the one provided to the customer.

Recommendation 10 - Monitoring

With regard to this point, it would be appropriate to also formalize what monitoring obligations should be respected by TPs for operations processed via them. The document, in fact, does not seem to indicate what type of monitoring the TPs must implement.

Best Practice 11.1

We believe that the requirement described in this BP should not be described as "desirable" given that we believe that access to the data, as described, should not be allowed.

Annex 1

Extract from ABI Position Paper on "Review of Directive 2007/64/EC on payment services in the internal market – new issuer paper" (16 November 2012)

3.4. Definition of payment services covered

OVERLAY PAYMENT SERVICES (CURRENTLY NOT REGULATED)

- WHETHER AND IF SO UNDER WHICH CONDITIONS SHOULD THESE NEW SERVICE PROVIDERS PROVIDE THEIR SERVICES AND NOTABLY HAVE ACCESS TO INFORMATION ON BANK ACCOUNTS?
- WHICH OTHER ISSUES SHOULD BE ADDRESSED (DATA PROTECTION, SECURITY ISSUES) AND IN WHICH REGULATORY FRAMEWORK?

With respect to this highly debated issue we consider:

Firstly, that the PSD has set the conditions to operate fairly and with transparency in a competitive market based on rules for safe operation. The PSD gives every entity which is in a position to observe those rules the possibility to operate. Enormous opportunities like wallets, e-money accounts, free of charges payment accounts are available and the new payment schemes (SCT/SDD) as well as the "old" ones, like cards, enable timely and safe fund transfers.
It seems that those entities, claiming that access to user's payment account with third party providers is indispensable for the development of innovative payment services, wish to circumvent safe handling and approach payments from a technological point of view only, which is exactly the contrary of the target set by the Overseers and by the PSD. As mentioned before, the technological level shall not be blurred into the regulatory and functional one. Making a technological approach become a legal right is very risky, from an evolutionary point of view.

Secondly, in line with the "inclusive approach" illustrated above, we believe that any service provider in the payment area must be clearly identified in its activities, role and liabilities: this is what the PSD is meant to do. Once all the services providers are regulated under the same regulation and supervision, citizens, both consumers and corporates/merchants, are in the conditions to make or receive payments in a safe way.
Breach of security, data protection and privacy, fraud losses, reputational risks are issues to be considered carefully for each single channel access to customers' accounts might come from (online service, cards, etc.).

Thirdly, overlay services are particularly delicate in so far as they deal with clients' accounts, therefore:

- their role shall be regulated in contracts between the client, the PSP and these actors, these contracts are necessary to define rights and obligations, diligent behaviour and liability which can stand in court
- they should ensure adequate information on the functioning of the services they offer, on the risks and responsibilities, of all concerned parties
- They shall be fully liable in case of problems
- They shall ensure proper protection of data related to payment instruments and services, e.g. excluding the use of such data for other purposes, due protection of databases etc.

Annex 2

Extract from ABI Position Paper answering to the EC "Green Paper – Towards an integrated European Market for Card, Internet and Mobile Payments" (20 March 2012)

Section 4.1.7 Information on the availability of funds

Q. 13) Is there a need to give non-banks access to information on the availability of funds in bank accounts, with the agreement of the customer, and if so what limits would need to be placed on such information? Should action by public authorities be considered, and if so, what aspects should it cover and what form should it take?

A. 13) Third-parties shall not have access to information pertaining to the availability of funds in accounts without the consent of the account holding bank. Breach of security, data protection and privacy, fraud losses, reputational risks are issues to be considered. Any granting of such access should be entirely secure for both the customer and the PSP holding the account, should be commensurate to the sharing of the costs related to the provision and holding of the account and should be fair as to the responsibilities and opportunities of both PSPs and third parties.

In case a strong political willingness to pursue such unsound approach materializes despite the above considerations, a principle of full reciprocity of rights and obligations should be ensured among PSPs and third parties.

We point out that in the instructions on "*Implementation of Title II of Legislative Decree 11 of 27 January 2010 concerning payment services*" issued by Bank of Italy in July 2011, it is specified that where an instrument calls for the use of personal security measures (e.g., PINs and passwords), the user is required to take actions aimed at keeping such measures confidential with the aim of preventing unauthorized use of the payment instruments concerned. If the contract between the user and provider of payment services prohibits the former from divulging security codes to third parties, breach of this prohibition constitutes negligent conduct on the part of the user, and thus represents grounds for loss of the exemption from liability set out in the PSD. We consider that this rule is fair and ensures adequate protection of account information, fosters prudent behavior of the customers and awareness of the consequences of misbehavior.