Response to the public consultation of the ECB on "Recommendations for the security of Internet Payments"

Provided by ABI

11 June 2012

- **Introduction**

Associazione Bancaria Italiana (ABI) has prepared this document in response to the public consultation on the recommendations made by the European Central Bank ("*Recommendations for the security of internet payments*", hereinafter, the "Recommendations"), after gathering comments from ABI Members, the ABI Lab Consortium (banking research and innovation centre), the Bancomat Consortium (manager of the Bancomat and PagoBancomat networks and owner of the related trademarks) and Corporate Banking Interbancario (manager of technological infrastructure for corporate banking that allows interchanges between consortium members in relation to payment services and document management).

This consultation has generated considerable interest, since it covers security aspects relevant to the development of internet payment services. These aspects are widely known to be key for the growth of electronic payments; in addition, the subject is important in view of the Digital Agenda for both the banking sector and the country as a whole.

ABI welcomes the 14 Recommendations, considering publication of the consultation document to be an important move designed to ensure that PSPs continue to pay close attention to payment security matters - both to tackle fraud and to strengthen customer confidence in use of the internet and payment cards. In addition, the opportunities for updating the procedures and systems used by PSPs for remote identification and authentication should not be overlooked, together with those for establishing a harmonised European framework for the security measures needed to protect cards and internet banking.

The decision to provide harmonised recommendations at EU level is also greatly appreciated. Until now, this matter has mostly been left to the judgement of individual countries or market operators, even though it is fundamental for the medium/long-term sustainability of the new channels.

- **General observations**

With regard to the scope of application, we fully agree with the decision to make recommendations concerning the use of cards for on-line payments, consistent with the approach taken in relation to on-line banking, not least given the current maturity of the market.

However, it is important for the document to make clear that the recommendations are addressed not only to payment service providers, but also to on-line merchants and other unregulated operators.

In this regard, while the banking industry pays close attention to payment security issues, other services involving so-called "third party access to customer accounts" are not covered by the recommendations. If these services are not appropriately monitored, they might generate significant transaction security risks and jeopardise on-line operations as a whole (see our attached reply to Question 13 asked in the EC Green Paper entitled "Towards an integrated European Market for Card, Internet and Mobile Payments").

While noting the explicit exclusions made in Section I of the consultation document, we believe it necessary to strengthen the concept of multichannel payments (pc,

mobile phone, tv, ...) by calling for the alignment of the security measures adopted by the various channels.

Analysing the document with regard to the nature of the activities carried out by the various parties, it appears that the ECB is mostly focused on internet banking and electronic money services. In this regard, we would appreciate validation of the apparent limitation on the scope of application of the recommendations to just web based payment services offered in a competitive environment (single bank link).

Another aspect where clarification would be desirable concerns the applicability/exclusion of the recommendations with reference to the classification of business customers and, consequently, their applicability/exclusion in relation to the use of security systems that rely on a digital signature.

With regard to the security profiles considered, certain specific proposals - if adopted - could adversely affect the valid organisational and technological investment already made by banks and, accordingly, generate substantial additional costs.

Firstly, on the topic of user participation in the security measures adopted by internet payment systems, it is worth emphasising that the end user has been found to be a weak link in recent years. Accordingly, the emphasis placed on customer awareness, in the final three recommendations contained in the last section of the document, is much appreciated. Nevertheless, we believe that the security of the system as a whole would benefit from the allocation of specific liabilities on to customers, considering the efforts required from PSPs, such that overall liability is divided between the PSP and the user. As noted in Annex I of the document ("*more clarity is needed regarding the burden of proof … and consumer liability*"), this factor is one of the controversial aspects arising from application of the Payment Services Directive (PSD), with the risk that the customer, as a protagonist in the system, feels no responsibility for its functioning. In this regard, the document excludes any user liability if the transaction took place without forms of "*strong authentication*". We propose to include (at least as a suggestion for the European Commission) specific user liabilities when PSPs have provided their payment systems with strong authentication and user notification measures, and users do not promptly notify non authorised transactions (as agreed with PSPs).

Secondly, one of the most problematic aspects introduced in the consultation document is the extension of the universally adopted definition of "*strong authentication*", to include the requirement that at least one of the elements should be non-reusable and non-replicable. While agreeing with this proposal's rationale, we believe that such a change might adversely affect the technologies and tools already in use by many PSPs, making compliance longer, harder and more costly, especially given the objectively close deadline for implementation (about two years). We strongly believe that solutions not preventing reuse or replication may nevertheless provide an adequate level of security. Therefore, we suggest transforming these additional requirements into Best Practices (at least during a transition period). In this regard, reference is made to the *European Payments Council* document (EPC424-10 "*Preventing Card Fraud in a mature EMV Environment*") that identifies alternative solutions for strengthening the authentication of cardholders, other than "*strong authentication*", which do not specifically require the prevention of reuse and replication.

Due attention should also be paid to the integration of the above recommendations with current national regulations being, specifically, the Bank of Italy's implementation of Section II of Decree 11/2010 adopting the PSD, issued in July 2011.

In addition, it should be possible to integrate the envisaged analysis, risk assessment, monitoring and control activities with the risk management, security and auditing processes already in place at banks. This would avoid the duplication of costs and procedures allowing banks to define their organisational procedures in a flexible way.

Given its importance, we believe that special attention should be paid to card payments where, in the absence of clear regulations, certain parties do not use the same security measures as those adopted by banks, thus exposing the entire system to considerable risks.

For this purpose, we believe it is useful to include (at least as a recommendation to the European Commission) a clear statement about the need for the regulations to apply to all interested parties (including technical service providers and e-merchants - the latter are often addressed in the document solely in terms of "Best Practices"). Furthermore, in order to facilitate transparency and user awareness, we suggest standardisation of the on-line communications sent to customers about the payment security guarantees offered by e-merchants.

In addition, we believe that it might be more effective to avoid references to specific technology and infrastructure: the spirit of the recommendations should be technologically independent, so that they are not rendered obsolete by the rapid evolution of systems and devices. In addition, the adoption of different technological solutions would reduce the risks deriving from possible attacks.

With regard to timing, the document states that PSPs should implement the recommendations by 1 July 2014. We consider this deadline to be too close, given that the work required is not always easy or readily implemented.

- **Observations on individual Recommendations**

The consultation document includes a number of Recommendations that, without prejudice to the minimum level of security to be guaranteed, should give PSPs freedom to develop various technological solutions addressing the security of their systems.

Our specific observations regarding these Recommendations are presented below:

Recommendation 1

In general, the *Key Considerations* (KC) included in Recommendations 1 (*Governance*) and 2 (*Risk Identification and Assessment*) do not appear to be fully in line with the Bank of Italy's implementation of Section II of Decree 11/2010 implementing the PSD and, by contrast, envisage technical/software/organisational analyses that would be burdensome for banks. More specifically, an independent function is required to perform risk assessment activities while, by contrast, national regulations make this optional. Furthermore, the KC does not mention the certification of security solutions as a guarantee of their quality.

Key Consideration 1.1

As mentioned in the general observations, the specified security measures should apply not only to PSPs, but also to the other parties that offer payment services, such as e-merchants and operators not covered by the Recommendations.

In addition, the reference to risk appetite in the overall context of sector objectives appears complex and unclear, given the dynamic and constantly evolving environment.

Key Consideration 1.2

When defining roles and responsibilities, the concept of an "independent risk management function" should be clarified further, in order to avoid a considerable organisational impact on the audit and risk management functions already established by banks; in this regard, it may be useful to mention, even by way of example, the international reference standards for security and IT governance (such as the ISO/IEC 2700x series).

Additionally, we believe it is important for any new organisational structures and related responsibilities identified by the Recommendations to be adaptable and capable of integration with existing structures, depending on the size of the bank concerned.

Key Consideration 2.1

It is important to highlight that customers should also be made responsible for the use of payment systems and for the security and protection measures adopted, paying attention to and taking the necessary care whenever making internet transactions (as covered in Recommendations 12 to 14).

Key Consideration 2.3

If the document's definition of "sensitive data" is not clarified further, it could be the subject of multiple interpretations at system level, causing difficulties when communicating with customers and creating misaligned expectations. In general, throughout the document certain data is considered "sensitive" in some Recommendations and "not sensitive" in others. Accordingly, we suggest finding a definition for "sensitive data" that encompasses solely the minimum set of data deemed truly critical for protection of the customer.

Recommendation 3

We greatly hope that the entry into force of these Recommendations will promote the establishment of formalised and compliant processes between PSPs throughout Europe, with a view to exchanging information on cyber attacks and security incidents. This would maximise the effectiveness of the action taken to combat and prevent fraud. In particular, such procedures would enable Law Enforcement Agencies (LEAs) to commence national and cross-border investigations on a timely basis. Currently, cross-border collaboration is greatly hindered by differences in local regulations that do not facilitate the exchange of information at European level. In this context, it is worth mentioning a formal agreement signed by ABI and Italian LEAs to promote the information sharing related to committed fraud and security incidents. In addition, efforts should be made to integrate the various

platforms used in member States to manage fraud in relation to electronic money, e-commerce and e-banking, thus enabling the work of the various LEAs to be more effectively aligned.

Key Consideration 3.2

With regard to this KC, a classification of the "major incidents" mentioned would be desirable. In Italy, banks experiencing security events linked to fraud already have procedures in place for reporting them to parties allowed to monitor fraudulent events and to the police while, in the case of major events linked to the functioning of IT systems, banks already report them to the Bank of Italy in order to assure the operational continuity of the IT infrastructure.

Key Consideration 3.3

Currently, in Italy, there are no regulations governing the "data breach notification" process (notifications about the improper use of personal information are classified as “suggested” by the Italian Authority on Data Protection and Privacy); therefore, we do not see any need to introduce ad hoc regulations on this matter, to the extent that procedures for notifying the police are already in place.

Recommendation 4

In general, the Italian banking sector has already introduced tools and technologies for the continuous monitoring of security access, networks and on-line transactions with customers, in order to make the work to identify attempted fraud and anomalous transactions more effective and, as a result, accelerate reporting and action to block attacks. Additionally, banks have already formalised procedures for the proper assignment of profiles or authorisations for access to data. Furthermore, following recent regulatory changes made by the Italian Authority on Data Protection and Privacy, all access by bank personnel to the banking data of customers in relation to banking transactions is logged. Accordingly, the actions specified in the KCs for this Recommendation are already good practice throughout the banking system.

Key Consideration 4.2

Identification of websites ("*transactional websites offering internet payment services should be identified by extended validation certificates drawn up in the PSP's name or by other similar authentication methods*"). This requirement is clearly understandable and applicable in relation to "institutional" websites (portals for home-banking customers or payment card holders). The applicability of these Recommendations is less clear when it comes to interactions with the web pages used for e-commerce transactions by e-merchants (e.g. 3D-Secure protocols that, by contrast, might not be compliant: in this regard, the opening of "*a separate window*" at the authentication stage is not mandatory - which differs from the contents of Annex 3 point 3); interactions frequently take place within a frame in the merchant's page, effectively making it impossible to verify the certificate of the 3D-Secure website. Further clarification about this would be appreciated.

Key Consideration 4.4

Although test work is useful and important, it is worth highlighting that the related organisational procedures and implementation should be determined at PSP level.

The risk factors have indeed impact on the whole applications; therefore, to refer solely to risk management functions for the performance of tests could be a limit for PSPs, due to the exclusion of other competent functions (security, operational and business) from the simulation of significant transactions.

In addition, the Recommendation stating that "*Tests should also be performed before any changes to the service are put into operation"* is very broad, offering little protection on the one hand and being too invasive on the other. In our view, the Recommendation should apply on the basis of the number of changes made, as well as to major changes or changes with a significant effect on security levels.

Key Consideration 4.5

As mentioned in the introduction, we believe it is appropriate to clarify the concept of "independent" experts responsible for audit activities, not least having regard for the Bank of Italy's recent secondary legislation on Section II of Decree 11/2010 implementing the PSD, which does not make it mandatory to use independent third parties for risk assessment activities.

Key Consideration 4.6

We suggest adding the following text, for the sake of clarity: *Contract provisions and clauses with outsourcers should be specified as binding for all components of the chain of sub-contractors and suppliers, as well*.

Key Consideration 4.7

The security of payments in the Italian market is normally "guaranteed'' by the payment networks and the banks (via a redirect to the payment gateway). The pan-European network Mybank also uses this approach. We have noticed however that, despite repeated requests from issuers, many international e-merchants operating in the Italian market use procedures that memorise card PAN numbers, thus weakening data security and creating vulnerabilities (see KC 11.3 in this regard, which recommends merchants not to retain data).

Furthermore, since the loss of image in the event of problems would also affect the bank (indirectly), we suggest both revising this KC with regard to the payment section of the website, which is under the direct control of the bank, and monitoring this issue constantly, not least to avoid jeopardising the investment in security already made by Italian banks.

For the implementation procedures, we suggest reference to the PCI Council's standard PCI-DSS.

Key Consideration 5.2

We suggest adding the following text: *Log files should never contain sensitive payment data (see Glossary of Terms on page 17)*

In addition, it should be specified that this activity has to be fully automated in order to guarantee the integrity of the files.

Best Practice [cards] 5.1

Consistent with the point raised in relation to KC 4.7, banks would be unable to monitor implementation of this suggestion, since they have no guarantees about the quality of the e-merchant's security systems. Accordingly, we suggest deleting this point. More importantly, the division of responsibility between the e-merchant and the PSP should be clarified, without transferring the e-merchant's responsibilities to the PSP, but rather by end-to-end dialogue with the authorities.

Recommendation 6

On the one hand, this Recommendation does not apply to e-commerce processes where, prior to payment, a contract must be formalised specifying the nature and characteristics of the service and establishing a process for the identification of the customer. These requirements would prevent internet users from making extensive use of such on-line services. On the other hand, this recommendation is consistent with the policies already adopted by banks for their internet banking services, which involve signature by the customer of an ad hoc contract.

Key Consideration 6.1

Among the methods for the remote identification of customers, we believe it important to consider the possibility of reading information from their electronic ID documents, as part of a public/private federation covering the identity of citizens and integration of the related services. Currently, there is strong focus on this at a European level, as seen by the recent financing of research projects that also include involvement by Italian banks.

Of course, such innovations in technology and processes should be accompanied by suitable regulatory changes, not least in relation to the anti-money laundering regulations. Besides, the Digital Agenda of the Italian banking system also highlights regulatory restrictions that directly or indirectly impede the completion of processes in an entirely digital manner; for example, the remote formalisation of contracts without physical recognition of the customer, or the management of contracts and documentation using solely electronic means. We therefore look forward to regulatory changes at a European level that allow such new approaches to the remote identification of users.

Key Consideration 6.2

We suggest adding other card-related information (CVx2, PAN etc.) to the list of information provided to customers wishing to access internet services.

In addition, we believe that customers should be informed about updates to be downloaded and added to their anti-virus protection, as part of efforts to tackle new types of fraud and cyber attack. In this regard, we also consider that the information provided to customers should distinguish between the types of service provided (e.g. e-commerce activities).

Recommendation 7

As already emphasised in our general observations, one of the most critical aspects introduced by the consultation document is the change in the universally-accepted definition of *strong authentication*; in particular, reference is made to the concepts of “mutual independence”, “non-reuse” and “non-replication” of the means used. If implemented, this Recommendation would make inadequate various approaches to

strong authentication already used by banks, with a considerable impact in terms of cost and technology in order to align their systems. In particular, the proposed change would not take into account some of the effective strong authentication solutions already implemented for secure identity management and for combating fraud. Accordingly, we suggest leaving it to individual PSPs to evaluate the adoption on a discretionary basis of systems with equal or greater levels of protection (as a best practice).

In addition, we recommend adding the graphometric signature to the list of biometric technologies recognised as strong authentication solutions, given the widespread use among Italian banks of devices for collecting this signature.

Lastly, it is unclear if usage of the dual factor is also recommended for the first level of authentication, as with the log-in to remote banking for information-only purposes. We would prefer this choice to be at the discretion of banks, whether for additional security or consequent to their assessment of risk (possibility that appears to arise from KC 7.2), with the inclusion of this recommendation as a best practice.

Lastly, we suggest adding the definition of strong authentication to the glossary of terms.

Key Consideration 7.3 [cards]

Usage of a strong multichannel authentication system (e.g. using SMS-based technology) might be suggested as a Best Practice to overcome the vulnerability of fixed passwords used by 3D Secure.

Key Consideration 7.7 [cards]

As part of card security management, we suggest keeping these recommendations in line with those of the PCI-DSS standard. The scenario envisaged would involve the supplier of the wallet retaining the CVx2 codes, which contrasts with PCI-DSS (3.2 - Do not store sensitive authentication data after authorization).

The considerations presented also appear to make use of the wallet solutions more complex for the customer. If, on the other hand, the intention of the KC is to recommend the use of strong authentication by suppliers, we believe that wording such as "*Providers of wallet solutions should support strong user authentication when executing payment transactions via the internet*" might be more appropriate, with a liability shift in favour of the issuer if this is not the case.

The "SEPA Cards Standardisation (SCS) “Volume” Book of Requirements, Version 6.0" seems more reasonable when it comes to recurring transactions (*5.6.2.2.1 Card acceptors, acceptance processing platforms and remote transactions acquirers shall acquire and transmit Card Security Code values or their equivalent. However, for recurring payment transactions where the merchant has stored the card number and the expiry date but not the Card Security Code or its equivalent, the presence of the Card Security Code value, or its equivalent or better means of authentication is only required for the initial transaction.*).

Best Practice 7.1 [cards]

The clause *"It is desirable that e-merchants support strong authentication of the cardholder by the issuer in card transactions via the internet"* appears to contrast (note the difference between "it is desirable" and "should require") with KC 7.5 ("PSPs offering acquiring services should require their e-merchant to support strong authentication of the cardholder by the issuer for card transactions via the internet").

Recommendation 8

This Recommendation relates to the "secure" delivery of strong authentication tools. This aspect could have a major impact and the recommendation does not appear to be unequivocal. Accordingly, in this regard, we request greater clarity concerning:

- whether or not the "secure" methods for the delivery and activation of a strong authentication tool relate to the actual delivery of the strong authentication tool (physical or software) that banks typically provide together with the access credentials (*username-password*), which some use to validate instructions and others also use for access control;

- if the response to the above is yes, the question is whether delivery should take place at the branch/by post or - in the case of software - if other forms of distribution and remote activation can be envisaged; furthermore, in the case of remote activation, we need to know if that process must use a component delivered in the above manner (branch/post, such as a secret code contained in a sealed envelope), or if a password generated by another strong authentication tool given previously to the customer at the branch/delivered by post would be sufficient, or otherwise if a process that the issuer believes and determines to be secure may be used.

Key Consideration 8.1

With regard to the recommendation that passwords should be physically distributed, we note that this would significantly impede use of the internet, while recourse to properly checked and protected digital channels would reduce costs and the environmental impact of the activity.

"*Activation during shopping*" appears to be problematic: the chances of completing the original transaction are low and, as a result, this option would cause many cardholders to abandon the purchase. Finally, the "exceptions" mentioned in the document should be clarified.

Key Consideration 8.2

In terms of the clarity of "definitions" with regard to the following paragraph **"***(…) In such instances, weak authentication based on the cardholder name, personal account number, expiration date, card verification code (CVx2) and/or static password should be a minimum requirement",* it is unclear if the logic is "and" (all elements of authentication "together") or "or" (if a subset would be sufficient).

Key Consideration 9.1

The technical attachment to the decree related to Section II of Legislative Decree 11 dated 27 January 2010 implementing the PSD - issued by the Bank of Italy in

July 2011 - indicates the maximum time for the validity of a *One-Time-Password* as "100 seconds".

Recommendation 10

Greater clarity is requested since, in general, the Recommendation requires PSPs to block the transaction in real time, while KC 10.1 just talks about detection without requiring the transaction to be blocked. It should be noted that some PSPs have monitoring programs only for the periodic analysis of transactions, so the requirement would mean making significant changes to their procedures. Accordingly, the level of monitoring (periodic or real time) should reflect the level of risk identified and the level of security required, as well as the protection measures adopted by the banks and made available to customers.

Lastly, we believe that acquirers could also make an important contribution, but no mention is made of them.

We would also like to know if PSP usage of transaction monitoring systems that do not intervene at the authorisation stage (block) is considered compliant with the recommendations.

Key Consideration 11.2

We believe that the adoption of high levels of security for end-to-end data transmissions should be evaluated with reference to the level of risk involved.

As mentioned earlier, the PCI-DSS standard could be a point of reference for card processing.

Recommendation 11.3 [cards]

This point does not appear consistent with the definition of sensitive date provided in the glossary. Some data (e.g. postal address, e-mail, …) is in fact needed by e-merchants in order to provide the service and, as such, it is hard to imagine e-merchants not retaining those data for their own safeguard.

Recommendation 12

We agree with the need to provide intensive customer education, especially with regard to the safe management of personal digital credentials, the most appropriate way to use the internet, and the protection of access to internet banking, together with training for each PSP's technical personnel. However, we would also like to note that such actions do not relieve the customer from responsibility for the diligent use of the internet and payment cards. We also note that some customers might consider technological assistance from the bank to be "invasive".

Key Consideration 12.1

We believe that customers must take greater responsibility and, accordingly, they should be required to follow the issuer's rules on security. In addition, we consider that the requirement for acquirers to ask e-merchants to comply with their security rules should be compulsory and not merely "desirable".

Recommendation 14.2

This point does not appear consistent with the definition of sensitive date provided in the glossary. Certain data (e.g. postal address, e-mail,...) cannot be hidden since it is used for communications purposes.

- **Annex I**

The recommendations place considerable obligations on the PSPs that deserve detailed examination from a legal standpoint e.g. contracts for the provision of internet banking services and the communications relating to anti-money laundering.

The absence of these elements could result in a strong presumption that orders are legally not authorised, with consequent liability of the PSPs and limitations on the liability of the customer. The ECB document presents this clarification as a proposed change to the Payment Services Directive. In this regard, while we fully agree with the need for greater EU harmonisation in the adoption of rules regarding liability and with the idea of making the liability of PSPs and e-merchants more closely dependent on the implementation of security measures, we ask that the greatest attention should be paid to the proposed extension of the Directive's scope of application.

In particular, while it is clear in the case of on-line transactions and e-commerce that geographical limitations do not make sense, we must be careful not to impose obligations on EU PSPs that they are totally unable to meet, such as when the counterpart PSP does not operate in the EU and is subject to other regulations. In this regard, reference is made to the considerations repeatedly expressed by the banking industry concerning the extension of the PSD to so-called "*leg out transactions*", with a resulting competitive disadvantage with respect to non-EU operations.

- **Annex 2**

As mentioned in the introduction, the content listed and described in this Annex should be deemed illustrative, leaving decision-making flexibility to PSPs concerning the technological solutions to be adopted for security purposes.

Considering such content in greater detail, the strong authentication mechanisms employed in Italy are starting to evolve into transaction signing mechanisms, as represented by one-time codes generated from the transaction data that help to avoid "*man in the middle*" style attacks. We suggest that greater consideration should be given to these security systems more than the "traditional" device token systems.

Lastly, with regard to the "*Software*" paragraph, we suggest changing the title to "END USER DEVICES". In particular, the demarcation line is unclear between the topics discussed in the previous paragraph ("*Internet Infrastructure and Technology*") and this paragraph; if it is decided to include detailed information about technologies/infrastructure in the document, we suggest focusing the "End user devices" paragraph more on the problems and risks associated with end-user devices, including specific examples perhaps, and covering the analysis of infrastructure issues in the previous paragraph.

Annex: extract from ABI's response to the European Commission public consultation on the "Green Paper – Towards an integrated European Market for Card, Internet and Mobile Payments"

Section 4.1.7 Information on the availability of funds

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?
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.