POSITION PAPER

Response to Eurosystem's Consultation on Recommendations for the Security of Internet Payments

June 2012

Response to Eurosystem's Consultation on

Recommendations for the Security of Internet Payments

1- Introduction

ESBG is pleased to have had the opportunity to review and comment on the Eurosystem's Recommendations for the Security of Internet Payments. As an early contributor to and participant in the SEPA project ESBG had identified security of internet payments as one of the areas where beyond and above the continued and strenuous efforts of market players an oversight and regulatory perspective would be required to move towards a more efficient, more level playing field type of environment. ESBG therefore considers the present consultation as a very important milestone, and looks forward to seeing its contribution being taken on board.

This response is divided into a set of general comments, followed by a discussion of each Recommendation, and the related Key Considerations and Best Practices.

2- General comments

Fraud is a dynamic environment. Fraudsters take a business-like approach to their activities: they constantly review the options that offer better revenue chances than risk to them, and reallocate their resources accordingly, unencumbered by any other limitation. This fickle environment necessitates a commensurate response from policy makers, legislators and market participants, not only in terms of everyday caution and the dedication of the enforcers fighting fraud, but also in terms of the mindset with which fraud prevention needs to be approached.

In particular, the notion that fraud prevention is a collective responsibility of policy makers, legislators and market participants must be promoted far more forcibly, and permeate notably any action from policy makers and legislators. In this respect, the "Recommendations" very much focus on actions to be taken by service providers. Considering the challenges posed by this dynamic environment, such "Recommendations" should at the minimum acknowledge 3 audiences:

- Policy makers and regulators,
- Service providers including schemes,
- Users (with distinct Recommendations for both retailers/merchants, and consumers)

In this context, the "Recommendations" should clearly lay out that the above parties each shoulder a distinct set of responsibilities:

- Policy makers and regulators are accountable for the timely creation and maintenance of a legal and/or guidance-based framework that provides certainty to providers and users alike, is technology-neutral, creates a level playing field for all service providers, is balanced in terms of the costs for either providers or users, recognizes the internal market objective, and is sufficiently stable. Furthermore policy makers and regulators should review how legislation can be enforced better, so that committing payment fraud becomes truly onerous for fraudsters.

- Service providers including schemes are accountable for establishing a safe environment for the type of transactions that their customers perform, for informing the latter about their duties and obligations, and the risks associated with this transaction environment, and for appropriately monitoring how this environment is being used, and reacting to, and reporting abuse.
- Users are not only accountable for respecting the usage instructions their PSPs provided them with, but also being generally alert to the emergence of unusual patterns or events, and querying or reporting them.

Whilst it can be understood that the Eurosystem wrote the "Recommendations" mainly from the oversight perspective, an implication may not be that these "Recommendations" should be read as placing the whole burden of delivering secure internet payments on PSPs only. As outlined above, the security of internet payments is a shared responsibility between policy makers, legislators, PSPs, and users. This point should be made explicitly in the "Recommendations".

It should also be acknowledged by these Recommendations that players not subject to these (e.g. either PSPs, and/or schemes, and or e-merchants, located outside the EU) and/or accepting higher risks could be at a competitive advantage compared to those having to comply. There is a need for an impact assessment. Equally a timely, coherent implementation by players across countries will matter in order to maintain a level playing field within the EU.

Finally ESBG notes that the present set of Recommendations does not address the issue of "overlay service providers", which could also be called "access to account information by non-regulated, non-supervised third parties". This issue has moved into the spotlight with a high profile case opened last September by the European competition authority. At stake however is rather the confidence that bona fide customers may in the future have in online payment systems, against the reality that such third parties generally gather from customer accounts more than the information strictly necessary to allow for the execution of the single purchase transaction at the origin of the interaction. In addition, this practice needs to be scrutinized in the light of the legal framework for data privacy and protection (which is currently the object of an EC regulation proposal). ESBG understands that the Eurosystem has established a task force to look into this issue, and would expect the conclusions of this task force to be the object of a similar public consultation, prior to any "consolidated set of Recommendations for the Security of Internet Payments" becoming final.

The "Recommendations" could actually be described as being composed of 4 main blocks:

1) Security policy (Recommendation 1)
2) Behavior, culture (Recommendations 2 and 3)
3) Operational aspects (Recommendations 4, 5, 8, 9, 10 and 11)

4) Customer-facing aspects (Recommendations 6, 7,12, 13 and 14)

3- Specific comments

Recommendation 1: Governance
PSPs should implement and regularly review a formal internet payment services security policy.
1.1 KC. *The internet payment services security policy should be properly documented, and regularly reviewed and approved by senior management. It should define security objectives and the PSP's risk appetite.*
1.2 KC. *The internet payment services security policy should define roles and responsibilities, including an independent risk management function, and the reporting lines for internet payment services, including management of sensitive payment data with regard to the risk assessment, control and mitigation.*
1.1 BP. *The internet payment services security policy could be laid down in a dedicated document.*

Considering the dynamic nature of the Internet threat environment, it is suggested that:

- An Internet payment services security policy is reviewed at least once a year.
- Such review must include an assessment of the latest developments in technology, and the latest fraud occurrences.
- PSPs must lay down their Internet payment services security policy in a dedicated document.

Recommendation 2: Risk identification and assessment
PSPs should regularly carry out and document thorough risk identification and vulnerability assessments with regard to internet payment services.
2.1 KC. *PSPs, through their risk management function, should carry out and document detailed risk identification and vulnerability assessments, including the assessment and monitoring of security threats relating to the internet payment services the PSP offers or plans to offer, taking into account: i) the technology solutions used by the PSP, ii) its outsourced service providers and, iii) all relevant services offered to customers. PSPs should consider the risks associated with the chosen technology platforms, application architecture, programming techniques and routines both on the side of the PSP and the customer.*
2.2 KC. *On this basis and depending on the nature and significance of the identified security threats, PSPs should determine whether and to what extent changes may be necessary to the existing security measures, the technologies used and the procedures or services offered. PSPs should take into account the time required to implement the changes (including customer roll-out) and take the appropriate interim measures to minimise disruption.*
2.3 KC. *The assessment of risks should address the need to protect and secure sensitive payment data, including: i) both the customer's and the PSP's credentials used for internet payment services, and ii) any other information exchanged in the context of transactions conducted via the internet.*
2.4 KC. *PSPs should undertake a review of the risk scenarios and existing security measures both after major incidents and before a major change to the infrastructure or procedures. In addition, a general review should be carried out at least once a year. The results of the risk assessments and reviews should be submitted to senior management for approval.*

2.1 KC: PSPs will carry out risk identification and vulnerability assessments in particular with respect to their products, and the guidelines and recommendations they provide to users with respect to the usage of these products. Whilst PSPs can be accountable for having such guidelines and recommendations available timely, and in understandable language, users remain accountable for using these products according to these guidelines and recommendations.

2.2 KC: Whilst PSPs shall be expected to do their utmost to minimize the effects of any service disruption, the "Recommendations" should acknowledge that in particular in the case of an emergency PSPs will give priority to security considerations over other, e.g. service continuity considerations.

2.3 KC: Sensitive payment data should be protected and secured, including "any other information exchanged in the context of transactions conducted via the internet", provided such data is passing through one or several PSPs. PSPs cannot become accountable for processing of data in which they are not involved (be it directly or as a result of an outsourcing arrangement).

Recommendation 3: Monitoring and reporting

PSPs should ensure the central monitoring, handling and follow-up of security incidents, including security-related customer complaints. PSPs should establish a procedure for reporting such incidents to management and, in the event of major incidents, the competent authorities.

3.1 KC. *PSPs should have a process in place to centrally monitor, handle and follow up on security incidents and security-related customer complaints and report such incidents to the management.*

3.2 KC. *PSPs and card payment schemes should have a procedure for notifying the competent authorities (i.e. supervisory, oversight and data protection authorities) immediately in the event of major incidents with regard to the services provided.*

3.3 KC. *PSPs and card payment schemes should have a procedure for cooperating on all data breaches with the relevant law enforcement agencies*

3.2 KC: National authorities should make sure that they have in place both the facilities and procedures to enable a 24 hour, 7x7 reporting of "major incidents". At national level there should be a "single point" to report such incidents. Furthermore national authorities across the European Union must have in place facilities and procedures to timely exchange information on "major incidents", when relevant. Finally the Eurosystem should propose a definition (criteria based) of "major incidents".

3.3 KC: PSPs, card payment schemes, and where relevant large retailers/merchants (or representatives thereof), should have a procedure in place for cooperating on all data breaches with the relevant law enforcement agencies.

Recommendation 4: Risk control and mitigation

PSPs should implement security measures in line with their internet payment services security policy in order to mitigate identified risks. These measures should incorporate multiple layers of security defences, where the failure of one line of defence is caught by the next line of defence ("defence in depth").

4.1 KC. *In designing, developing and maintaining internet payment services, PSPs should pay special attention to the adequate segregation of duties in information technology (IT) environments (e.g. the development, test and production environments) and the proper implementation of the "least privileged" principle 10 as the basis for a sound identity and access management.*

4.2 KC. *Public websites and backend servers should be secured in order to limit their vulnerability to attacks. PSPs should use firewalls, proxy servers or other similar security solutions that protect networks, websites, servers and communication links against attackers or abuses such as "man in the middle" and "man in the browser" attacks. PSPs should use security measures that strip the servers of all superfluous functions in order to protect (harden) and eliminate vulnerabilities of applications at risk. Access by the various applications to the data and resources required should be kept to a strict minimum following the "least privileged" principle. In order to restrict the use of " fake" websites imitating legitimate PSP sites, 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, thereby enabling customers to check the website's authenticity.*

4.3 KC. *PSPs should have processes in place to monitor, track and restrict access to: i) sensitive data, and ii) logical and physical critical resources, such as networks, systems, databases, security modules, etc. PSPs should create, store and analyse appropriate logs and audit trails.*

4.4 KC. *Security measures for internet payment services should be tested by the risk management function to ensure their robustness and effectiveness. Tests should also be performed before any changes to the service are put into operation. On the basis of the changes made and the security threats observed, tests should be repeated regularly and include scenarios of relevant and known potential attacks.*

4.5 KC. *The PSP's security measures for internet payment services should be periodically audited to ensure their robustness and effectiveness. The implementation and functioning of the internet services should also be audited. The frequency and focus of such audits should take into consideration, and be in proportion to, the security risks involved. Trusted and independent experts should carry out the audits. They should not be involved in any way in the development, implementation or operational management of the internet payment services provided.*

4.6 KC. *Whenever PSPs and card payment schemes outsource core functions related to the security of the internet payment services, the contract should include provisions requiring compliance with the principles and recommendations set out in this report.*

4.7 KC. *PSPs offering acquiring services should require e-merchants to implement security measures on their website as described in this recommendation.*

4.2 KC: This Key Recommendation should not be read as applying solely and exclusively to PSPs. On the contrary retailers/merchants too should implement and observe the same processes and procedures for their public websites and backend servers. This remark also applies to the other Key Considerations listed under Recommendation 4 (except, for 4.7. KC, see below).

4.6 KC: The guiding principle must be that regardless of any formal of other outsourcing arrangement a PSP remains accountable for its sphere of responsibility.

4.7 KC: The security measures described under Recommendation 4 should be applied by e-merchants in general. These measures should be applied in a harmonized way throughout the European Union. PSPs should of course inform merchants about their duties in this respect, yet PSPs cannot be expected to perform an “enforcement role”. The wording of Key Consideration 4.7 should be amended accordingly (i.e. “require” being replaced by “inform”).

Recommendation 5: Traceability

PSPs should have processes in place ensuring that all transactions can be appropriately traced.

5.1 KC. *PSPs should ensure that their service incorporates security mechanisms for the detailed logging of transaction data, including the transaction sequential number, timestamps for transaction data, parameterisation changes and access to transaction data.*

5.2 KC. *PSPs should implement log files allowing any addition, change or deletion of transaction data to be traced.*

5.3 KC. *PSPs should query and analyse the transaction data and ensure that any log files can be evaluated using special tools. The respective applications should only be available to authorised personnel.*

5.1 BP. *[cards] It is desirable that PSPs offering acquiring services require e-merchants who store payment information to have these processes in place.*

5.1 BP: there are 3 comments to the proposed Business Practice:

a) e-merchants should be obligated to disclose on their website to any potential customers which customer information they retain, and whether they process themselves, or outsource. It is not for PSPs to enforce any such obligation.

b) When complying with this disclosure requirement, e-merchants should make a clear distinction between the information that they consider strictly necessary for the performance of their contract with the purchasing customer, and other information.

c) The proposed requirement should not only apply to payments with cards, but to any e-payment transaction.

Recommendation 6: Initial customer identification, information
Customers should be properly identified and confirm their willingness to conduct internet payment transactions before being granted access to such services. PSPs should provide adequate "prior" and "regular" information to the customer about the necessary requirements (e.g. equipment, procedures) for performing secure internet payment transactions and the inherent risks.

6.1 KC. *PSPs should ensure that the customer has undergone the necessary identification procedures and provided adequate identity documents and related information before being granted access to the internet payment services.*
6.2 KC. *PSPs should ensure that the prior information 11 supplied to the customer contains specific details relating to the internet payment services. These should include, as appropriate:*
- clear information on any requirements in terms of customer equipment, software or other necessary tools (e.g. antivirus software, firewalls);

- guidelines for the proper and secure use of personalised security credentials;

- a step-by-step description of the procedure for the customer to submit and authorise a payment, including the consequences of each action;

- guidelines for the proper and secure use of all hardware and software provided to the customer;

- the procedures to follow in the event of loss or theft of the personalised security credentials or the customer's hardware or software for logging in or carrying out transactions;

- the procedures to follow if an abuse is detected or suspected;

- a description of the responsibilities and liabilities of the PSP and the customer respectively with regard to the use of the internet payment service.

6.3 KC. *PSPs should ensure that the framework contract with the customer includes compliance-related clauses enabling the PSP to fulfil its legal obligations relating to the prevention of money laundering, which may require it to suspend execution of a customer's payment transaction pending the necessary regulatory checks and/or to refuse to execute it. The contract should also specify that the PSP may block a specific transaction or the payment instrument on the basis of security concerns. It should set out the method and terms of the customer notification and how the customer can contact the PSP to have the service "unblocked", in line with the Payment Services Directive.*
6.4 KC. *PSPs should also ensure that customers are provided, on an ongoing basis and via appropriate means (e.g. leaflets, website pages), with clear and straightforward instructions explaining their responsibilities regarding the secure use of the service.*
6.1 BP. *It is desirable that the customer signs a dedicated service contract for conducting internet payment transactions, rather than the terms being included in a broader general service contract with the PSP.*

Recommendation 6: in the context of internet/online banking PSPs are expected to provide any "prior" and "regular" information about the necessary requirements by electronic means only. Paper-based information will only be provided at the express request of a customer.
6.1 KC: It should be unambiguously stated that PSPs do not have to undertake separate customer identification for online banking and for "traditional" customer account

relationships, and that PSPs only have to maintain a single set of supporting customer documents.

6.2 KC: Of course customers are responsible for constantly updating their hardware/software environment.

With respect to the respective responsibilities and liabilities of PSPs and customers with regard to the use of the internet payment service, the transposition of the Payment Services Directive has not led to a more level playing field. Whilst it is much desirable to work towards achieving the latter, this may not be at the expense of yet an additional burden for PSPs.

6.1 BP: The "Recommendations" should acknowledge that going forward internet/online banking will be the primary manner of interaction between customers and their PSPs. Therefore, in terms of best practice, contracts between PSPs and their customers should reflect this growing reality, with dispositions regarding internet/online banking being included into the "main" or the single PSP-customer contractual arrangement. Other manners of interaction should be considered as "default" channels.

Recommendation 7: Strong customer authentication
Internet payment services should be initiated by strong customer authentication.

7.1 KC. *[CT/e-mandate] Credit transfers (including bundled credit transfers) or electronic direct debit mandates should be initiated by strong customer authentication. PSPs could consider adopting less stringent customer authentication for outgoing payments to trusted beneficiaries included in previously established "white lists", i.e. a customer-created list of trusted counterparties and beneficiary accounts with strong authentication.*
7.2 KC. *Obtaining access to or amending sensitive payment data requires strong authentication. Where a PSP offers purely consultative services, with no display of sensitive customer or payment information, such as payment card data, that could be easily misused to commit fraud, the PSP may adapt its authentication requirements on the basis of its risk analysis.*
7.3 KC. *[cards] For card transactions, all PSPs offering issuing services should support strong authentication of the cardholder. All cards issued must be technically ready (registered) to be used with strong authentication (e.g. for 3-D Secure, registered in the 3-D Secure Directory) and the customer must have given prior consent to participating in such services. (See Annex 3 for a description of authentication under the cards environment.)*
7.4 KC. *[cards] All PSPs offering acquiring services should support technologies allowing the issuer to perform strong authentication of the cardholder for the card payment schemes in which the acquirer participates.*
7.5 KC. *[cards] 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. Exemptions to this approach should be justified by a (regularly reviewed) fraud risk analysis. In the case of exemptions, the use of the card verification code, CVx2, should be a minimum requirement.*
7.6 KC. *[cards] All card payment schemes should promote the implementation of strong customer authentication by introducing liability shifts (i.e. from the e-merchant to the issuer) in and across all European markets.*
7.7 KC. *[cards] For the card payment schemes accepted by the service, providers of wallet solutions should support technologies allowing the issuer to perform strong authentication when the legitimate holder first registers the card data. Providers of wallet solutions should support strong user authentication when executing card transactions via the internet. Exemptions to this approach should be justified by a (regularly reviewed) fraud risk analysis. In the case of exemptions, the use of CVx2 should be a minimum requirement.*
7.8 KC. *[cards] For virtual cards, the initial registration should take place in a safe and trusted environment (as defined in Recommendation 8). Strong authentication should be required for the virtual card data generation process if the card is issued in the internet environment.*
7.1 BP. *[cards] It is desirable that e-merchants support strong authentication of the cardholder by the issuer in card transactions via the internet. In the case of exemptions, the use of CVx2 is recommended.*
7.2 BP. *For customer convenience purposes, PSPs providing multiple payment services could consider using one authentication tool for all internet payment services. This could increase acceptance of the solution among customers and facilitate proper use.*

Recommendation 7: Internet payment services should certainly be initiated by strong customer authentication, but assurance must be sought that the actual customer is at the origin of such session, and not any third party or "man-in-the-middle".
7.1 KC: there must be assurance that any "white list" is being created and/or maintained by the customer him/herself.

7.2 KC: Again it must be unambiguous that it is strong customer authentication that is meant and required in this context.

7.3, 7.4, 7.5 KC – (and others): It is unclear why these requirements seem to be limited to payments with cards. They should apply to any online payment – as much as possible.

7.5 KC (specifically): The last sentence should read "… the use of CVx2 or any other process with a similar effect…..".

7.6 KC: In a 4-corner model there is usually no contractual relationship between the e-merchant and the issuer.

7.7 KC: The last sentence should read "… the use of CVx2 or any other process with a similar effect…..".

7.1 BP: The last sentence should read "… the use of CVx2 or any other process with a similar effect…..". Any e-merchant failing to comply with the requirements laid down under this Recommendation will have to accept a liability shift.

Recommendation 8: Enrolment for and provision of strong authentication tools

PSPs should ensure that customer enrolment for and the initial provision of strong authentication tools required to use the internet payment service is carried out in a secure manner.

8.1 KC. *Enrolment for and provision of strong authentication tools should fulfil the following requirements. The related procedures should be carried out in a safe and trusted environment (e.g. face-to-face at a PSP's premises, via an internet banking or other secure website offering comparable security features, or via an automated teller machine).*

Personalised security credentials and all internet payment-related devices and software enabling the customer to perform internet payments should be delivered securely. Where tools need to be physically distributed, they should be sent by post or delivered with acknowledgement of receipt signed by the customer. Software should also be digitally signed by the PSP to allow the customer to verify its authenticity and that it has not been tampered with. Moreover, personalised security credentials should not be communicated to the customer via e-mail or website.

[cards] For card transactions, the customer should have the option to register for strong authentication independently of a specific internet purchase. In addition, activation during online shopping could be offered by re-directing the customer to a safe and trusted environment, preferably to an internet banking or other secure website offering comparable security features.

8.2 KC. *[cards] Issuers should actively encourage cardholder enrolment for strong authentication. Cardholders should only be able to bypass strong authentication in exceptional cases where this can be justified by the risk related to the card transaction. 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.*

8.1 KC: Again, any reference to "strong authentication tools" must be understood – and made explicit – as meaning "strong customer authentication tools". Any customer enrolment must be through a site which is certified by a PSP or a scheme. The channels used by the PSPs for the delivery of personalized security credentials must reflect the PSP's risk assessment, and may vary in function of the type, value and environment of the transactions under consideration.

8.2 KC: It is unclear why these requirements seem to be limited to payments with cards. They should apply to any online payment – as much as possible. At any rate the last sentence should read "… the use of CVx2 or any other process with a similar effect…..". Furthermore, any "redirection" of a session or a transaction must be pre-announced, and formally accepted by the customer. Any such re-direction must be to a site which is certified by a PSP or a scheme.

Recommendation 9: Log-in attempts, session time-out, validity of authentication
PSPs should limit the number of authentication attempts, dine rules for payment session "time out" and set time limits for the validity of authentication.

9.1 KC. *When using a one-time password for authentication purposes, PSPs should ensure that the validity period of such passwords is limited to the strict minimum necessary (i.e. a few minutes).*
9.2 KC. *PSPs should set down the maximum number of failed log-in or authentication attempts after which access to the internet service is (temporarily or permanently) blocked. They should have a secure procedure in place to re-activate blocked internet services.*
9.3 KC. *PSPs should set down the maximum period after which inactive payment sessions are automatically terminated, e.g. after ten minutes.*

9.3 KC: It is not recommended to provide a time limit example after which inactive payment sessions should be automatically terminated. Whilst the principle of having a time limit for the validity of a payment session is supported, the extent of such time limit must be function of a risk assessment undertaken by the PSP, and may vary in function of the type, value and environment of the transactions.

Recommendation 10: Transaction monitoring and authorisation
Security monitoring and transaction authorisation mechanisms aimed at preventing, detecting and blocking fraudulent payment transactions before they are executed should be conducted in real time; suspicious or high risk transactions should be subject to a specific screening and evaluation procedure prior to execution.

10.1 KC. *PSPs should use real-time fraud detection and prevention systems to identify suspicious transactions, for example based on parameterised rules (such as black lists of compromised or stolen card data), abnormal behaviour patterns of the customer or the customer's access device (change of Internet Protocol (IP) address[12] or IP range during the internet payment session, sometimes identified by geolocation IP checks,[13] abnormal transaction data or e-merchant categories, etc.) and known fraud scenarios. The extent, complexity and adaptability of the monitoring solutions should be commensurate with the outcome of the fraud risk assessment.*
10.2 KC. *Card payment schemes in cooperation with acquirers should elaborate a harmonised definition of e-merchant categories and require acquirers to implement it accordingly in the authorisation message conveyed to the issuer.*
10.1 BP. *It is desirable that PSPs perform the screening and evaluation procedure within an appropriate time period, in order not to unduly delay execution of the payment service concerned.*
10.2 BP. *It is desirable that PSPs notify the customer of the eventual blocking of a payment transaction, under the terms of the contract, and that the block is maintained for as short a period as possible until the security issues have been resolved.*

10.1 KC: The fraud detection and prevention systems implemented by PSPs should reflect their risk assessment(s), and may vary in function of the type, value and environment of the transactions concerned.
10.2 KC: It is unclear in what respect this "Key Consideration" will assist in detecting and/or preventing fraud. On the contrary, in a fast changing fraud environment – as refereed to earlier – it may provide a false sense of certainty to either issuers or acquirers.

Recommendation 11: Protection of sensitive payment data

Sensitive payment data should be protected when stored, processed or transmitted.

11.1 KC. *All data or files used to identify and authenticate customers (at log-in and when initiating internet payments or other sensitive operations), as well as the customer interface (PSP or e-merchant website), should be appropriately secured against theft and unauthorised access or modification.*

11.2 KC. *PSPs should ensure that when transmitting sensitive payment data, a secure end-to-end communication channel is maintained throughout the entire duration of the internet payment service provided in order to safeguard the confidentiality of the data, using strong and widely recognised encryption techniques.*

11.3 KC. *[cards] PSPs offering acquiring services should encourage their e-merchants not to store any sensitive payment data related to card payments. In the event e-merchants handle, i.e. store, process or transmit sensitive data related to card payments, such PSPs should require the e-merchants to have the necessary measures in place to protect these data and should refrain from providing services to e-merchants who cannot ensure such protection.*

11.1 BP. *[cards] It is desirable that e-merchants handling sensitive cardholder data appropriately train their dedicated fraud management staff and update this training regularly to ensure that the content remains relevant to a dynamic security environment.*

11.1 KC: Regarding data storing, the same remarks as made previously with respect to e-merchants apply.

11.3 KC: PSPs and schemes of course inform merchants of their obligations in the context of online payments, also when these are either stored and/or processed and/or transmitted. However, it must be acknowledged by the policy makers and regulators that PSPs are not in a position to enforce compliance with such requirements. Hence any failure to comply, and the consequences thereto, are the e–merchant's liability.

Recommendation 12: Customer education and communication
PSPs should communicate with their customers in such a way as to reassure them of the integrity and authenticity of the messages received. The PSP should provide assistance and guidance to customers with regard to the secure use of the internet payment service.

12.1 KC. *PSPs should provide at least one secured channel 15 for ongoing communication with customers regarding the correct and secure use of the internet payment service. PSPs should inform customers of this channel and explain that any message on behalf of the PSP via any other means, such as e-mail, which concerns the correct and secure use of the internet payment service, is not reliable. The PSP should explain:*
- the procedure for customers to report to the PSP (suspected) fraudulent payments, suspicious incidents or anomalies during the internet payment session and/or possible social engineering 16 attempts;

- the next steps, i.e. how the PSP will respond to the customer;

- how the PSP will notify the customer about (potential) fraudulent transactions or warn the customer about the occurrence of attacks (e.g. phishing e-mails).

12.2 KC. *Through the designated channel, PSPs should keep customers informed about updates in procedures and security measures regarding internet payment services. Any alerts about significant emerging risks (e.g. warnings about social engineering) should also be provided via the designated channel.*
12.3 KC. *Customer assistance should be made available by PSPs for all questions, complaints, requests for support and notifications of anomalies or incidents regarding internet payments, and customers should be appropriately informed about how such assistance can be obtained.*
12.4 KC. *PSPs and, where relevant, card payment schemes should initiate customer education and awareness programmes designed to ensure customers understand, at a minimum, the need:*
- to protect their passwords, security tokens, personal details and other confidential data;

- to manage properly the security of the personal device (e.g. computer), through installing and updating security components (antivirus, firewalls, security patches);

- to consider the significant threats and risks related to downloading software via the internet if the customer cannot be reasonably sure that the software is genuine and has not been tampered with;

- to use the genuine internet payment website.

12.1 BP. *[cards] It is desirable that PSPs offering acquiring services arrange educational programmes for their e-merchants on fraud prevention.*

Recommendation 12: Whilst indeed PSPs will be intent on communicating with their customers and educating them, the reassurance that PSPs can provide as to the integrity and authenticity of messages received by customers to an extent depends on customers' compliance with the security requirements expressed by the PSPs.

Recommendation 13: Notifications, setting of limits
PSPs should provide their customers with options for risk limitation when using internet payment services. They may also provide alert services.

13.1 KC. *Prior to providing internet payment services, PSPs should agree with each customer on spending limits applying to those services (e.g. setting a maximum amount for each individual payment or a cumulative amount over a certain period of time), and on allowing the customer to disable the internet payment functionality.*
13.1 BP. *Within the agreed limits, e.g. taking into account overall spending limits on an account, PSPs could provide their customers with the facility to manage limits for internet payment services in a secure environment.*
13.2 BP. *PSPs could implement alerts for customers, such as via phone calls or SMS, for fraud-sensitive payments based on their risk-management policies.*
13.3 BP. *PSPs could enable customers to specify general, personalised rules as parameters for their behaviour with regard to internet payments, e.g. that they will only initiate payments from certain specific countries and that payments initiated from elsewhere should be blocked.*

No comment.

Recommendation 14: Verification of payment execution by the customer
PSPs should provide customers in good time with the information necessary to check that a payment transaction has been correctly executed.

14.1 KC. *PSPs should provide customers with a facility to check transactions and account balances at any time in a secure environment.*
14.2 KC. *Any detailed electronic statements should be made available in a secure environment. Where PSPs periodically inform customers about the availability of electronic statements (e.g. when a new monthly e-statement has been issued, or on an ad hoc basis after execution of a transaction) through an alternative channel, such as SMS, e-mail or letter, sensitive payment data should not be included in such statements or, if included, they should be masked.*

No comment.

About ESBG (European Savings Banks Group)

ESBG – The European Voice of Savings and Retail Banking

ESBG (European Savings Banks Group) is an international banking association that represents one of the largest European retail banking networks, comprising of approximately one-third of the retail banking market in Europe, with total assets of over €7,470 billion, non-bank deposits of €3,400 billion and non-bank loans of €4,000 billion (31 December 2010). It represents the interests of its members vis-à-vis the EU Institutions and generates, facilitates and manages high quality cross-border banking projects.

ESBG members are typically savings and retail banks or associations thereof. They are often organised in decentralised networks and offer their services throughout their region. ESBG member banks have reinvested responsibly in their region for many decades and are a distinct benchmark for corporate social responsibility activities throughout Europe and the world.

ESBG - Association internationale sans but lucratif/Internationale vereniging zonder instoogmerk/ International not-for-profit association

Rue Marie-Thérèse, 11 ■ B-1000 Brussels ■ Tel: +32 2 211 11 11 ■ Fax: +32 2 211 11 99
info@savings-banks.eu ■ www.savings-banks.eu

Published by ESBG, June 2012