V1.0

EACB position on Eurosystem recommendations for the security of internet payments

June 2012

The **European Association of Co-operative Banks** (EACB) is the voice of the co-operative banks in Europe. It represents, promotes and defends the common interests of its 28 member institutions and of co-operative banks in general. Co-operative banks form decentralised networks which are subject to banking as well as co-operative legislation. Democracy, transparency and proximity are the three key characteristics of the co-operative banks' business model. With 4.000 locally operating banks and 65.000 outlets co-operative banks are widely represented throughout the enlarged European Union, playing a major role in the financial and economic system. They have a long tradition in serving 181 million customers, mainly consumers, retailers and communities. The co-operative banks in Europe represent 51 million members and 750.000 employees and have a total average market share of about 20%.

For further details, please visit www.eurocoopbanks.coop

EACB AISBL – Secretariat • Rue de l'Industrie 26-38 • B-1040 Brussels
Tel: (+32 2) 230 11 24 • Fax (+32 2) 230 06 49 • Enterprise 0896.081.149 • lobbying register 4172526951-19
www.eurocoopbanks.coop • e-mail : secretariat@eurocoopbanks.coop

General remarks

EACB welcomes the Forum's initiative to publish security measures for internet payments and to seek feedback on them. The system of internet payments represents an important contribution to the functioning of the economy. General and specific control and security measures are required in order to establish a secure environment for internet payments. Such measures contribute to the reduction of systemic risk in the payment area, and aim at the establishment of public trust and confidence in the financial system. In this context, the EACB carefully evaluated the recommendations and would like to make a number of remarks contained below, which we trust will be considered.

- **Role of financial supervisory authorities, central banks, legislators and PSPs**

Financial supervisory authorities and in particular central banks play a particular role in the management of payment systems through the mandate laid down in article 3 and 22 of the Statutes of the European System of Central Banks and the oversight role subsequently developed. As a result, they are well acquainted with the functioning of payment systems and their inherent risks. In case of incidents they are able to efficiently and adequately intervene from the perspective of the interests of the market. In our view it is therefore important that financial supervisory authorities, central banks and PSP's regularly exchange on a confidential basis on the security measures in place, on their effectiveness and on the threats observed. At these occasions, information should be shared about the state of security as well as security breaches and personal data related accidents.

In addition, where not already the case, we would recommend that banking supervisory authorities and central banks do periodical and incident driven evaluations of the state of security of internet payment systems. It is extremely important that an environment is ensured where PSP and supervisory authorities can continue to commonly analyze, assess and resolve internet payment related risks, while maintaining public trust and confidence.

Although the scope of Eurosystem recommendations is the 'technical' security, the EACB would like to remark that this is only one side of 'secure payments' and that the legal and regulatory framework is as important as the technical one. We would like to quote Daniela Russo's speech "Challenges for retail payment systems" made at the hearing on card, internet and mobile payments in Brussels on 4 May 2012:
"The current legal and regulatory framework does not consistently meet the challenges that arise relating to access to payment accounts required by those entities. For example, non-bank providers offering overlay services in various EU countries are not currently considered to fall under the Payment Services Directive (PSD) and are thus not regulated or supervised. It is important that the current legal vacuum will be addressed in the revision of the PSD."
From the perspective of the EACB it is as important to close this "vacuum" as it is to provide technical security.

- **Need for consistency in implementation of recommendations**

The EACB would call for national supervisors and central banks to apply, interpret and enforce the proposed security measures in a uniform manner, thereby creating a level playing field, a consistent consumer experience and an environment conducive to the development of e-commerce. There should be a harmonised interpretation of the various concepts, definitions and classifications used throughout the document, e.g. classification of authentication instruments, and also a harmonised legal basis in the different national legislations incl. civil law.

- **Need for consistency with other measures**

Furthermore, we would like to stress the need for consistency between legislative measures in the area of cybercrime, data protection, anti-money laundering, consumer protection, and payments in general (e.g. the PSD) on the one hand, and the recommendations under consideration on the other, to ensure that liabilities and responsibilities can effectively be implemented:

- Data protection

The directive on the protection of personal data and the framework decision on protection of personal data processed in the framework of police and judicial cooperation in criminal matters are presently under review, and new legislative proposals are on the table. To facilitate the fight against misuse of the internet payment infrastructure it is necessary to process and exchange data about suspicious transactions, suspicious IP-addresses, suspicious accounts. The processing and exchange is necessary to detect, analyze, prevent and stop malicious attacks on the infrastructure. The exchange also facilitates reversing fraudulently initiated payments. We would welcome initiatives to analyze and remove obstacles emerging from current or coming data protection law that hinder an efficient approach to the prevention of the misuse of the internet payment system.

- Need for waivers to be introduced limiting liabilities in case of follow-up to the recommendations

The recommendations encourage PSPs to intervene when they detect potentially fraudulent transactions and to stop such payments temporarily or definitively. Legislation (such as the PSD) should be adapted so as to protect PSPs against financial claims of customers on the basis that ex-post it appears that there was no fraudulent attack at stake.

- Legal basis for reversal of payment orders

The interests of PSPs and customers are served by broadening the possibilities to reverse fraudulent payment both on a domestic and cross border level. At present, the originating PSP is dependent on the willingness of the beneficiary bank to cooperate in the reversal of a fraudulent payment order. Legislation could facilitate a mandatory process for reversing fraudulent payments. The definition of fraudulent payments however should be sufficiently prescriptive. Disputes between merchants and consumers about, for example, the quality and delivery of the goods should not be in the scope of fraudulent transactions.

- Consumer protection

Consumer protection as regards the occurrence of unauthorized fraudulent payments is ruled by the PSD which puts the burden of proof largely on the part of the PSPs. We strongly recommend to keep the system of security measures confidential and not to make them part of the civil law relationship between PSP and consumer. The PSD already protects the consumers' interests while the banking supervisory law should enable to protect the public trust and confidence.

- Security measures to be respected by other parties

Various players active on the market for internet payments such as the non-PSD licensed institutions, currently seem not to be subjected to supervision and oversight. In the context of the present recommendations it would seem important that all providers of internet payment services, whether PSD licensed or not, should be subject to the same oversight,supervision and recommendations ('level playing field'). After all, the total level of security depends on the weakest link. In addition, not doing so would seem contradictory in particular to KC 2.1.

The EACB is aware that the SecuRe Pay is working on a separate document regarding "Access to payment accounts over the internet by third party providers". Care should be taken so as to avoid that the outcome of that project would create a situation that would weaken the security measures which are recommended in this more generic document. It should be noted in this context that banks will not be able to control, nor be made responsible for the security arrangements of such third party service providers in the payment chain outside the control of the banks, nor can banks be expected to protect their clients towards those parties. A discussion on access to payment accounts over the internet by third party providers should duly consider the risk such access may bring to the effectiveness of the recommendations under consideration in this document.

➢ Scope and Addressees

The EACB takes note of the fact that the Recommendations formulated by the Eurosystem would only be enforced by European supervision and oversight bodies but would not necessarily apply to non-European players. We would encourage the Eurosystem to promote similar practices with their peers outside Europe so as to ensure a level playing field and maximum security.
As far as intra-EU is concerned, the EACB would believe that the security rules should apply and be enforced in the same way all over Europe.
In addition, the EACB has some reservations as to some carve-outs made in the general introduction. It believes that:

- Fraud is not limited to one particular payment channel, scheme or instrument. All means of payment need to be subject to the same minimum security requirements irrespective of the instrument, scheme or channel involved. We do not necessarily understand why payments mentioned under point 2, 3, 4, 7 and 8 are excluded from the recommendations.
- The recommendations should apply to all players involved in the internet payment chain, not only to PSPs but also to e-merchants, to non-PSD licensed payment service providers, etc., where and when relevant.

- **Guiding principles**

The EACB remarks that – as far as the guiding principles are concerned – there are a number of principles for which parallels can be found either in the area of anti-money laundering and terrorist financing legislation or in the way PSPs manage their payments in general. Where this is the case, and where specific recommendations are formulated on the subject of internet payments, the EACB would consider that it should be possible to incorporate the implementation of these recommendations in the overall policies already in place. In some areas, alignment may have to be sought between practices so as to avoid unnecessarily overlap and inefficiency. You will find more detailed comments below.

On the second general principle, i.e. on the need for strong customer authentication, we have to note that the third party access to the customer payment account that is excluded from the scope of these recommendations, may in fact affect the ability of the PSP to confirm the authentication of the customer.

Finally, we would like to observe that security solutions continue to evolve. The EACB would therefore recommend caution in making references to specific security solutions that are in place at the moment and would encourage taking an independent approach in formulating the recommendations.

- **Implementation**

The EACB would consider the timelines for implementation and adoption of the recommendations as rather ambitious.

General control and security environment

Recommendation 1: Governance

PSPs should implement and regularly review a formal internet payment services security policy.

The EACB would consider that the proposed security recommendations should apply to all players in the value chain, including non-PSD licensed service providers (see also the general remarks above).

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.

The EACB would consider the timing and frequency of the reviews and risk assessments as part of the security policy. It would be recommended to qualify what is meant with "regular", at least by specifying a maximum term and leaving PSPs the freedom to do a more frequent review based on their own risk analysis.
Another question is whether the timeline of 1 year referred to under KC 2.4 should be understood to be indicative.

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.

The concept of "independent" should be clarified because, unlike for the audit function, some degree of integration of the risk management function with the actual payments design and processing functions seems desirable for efficiency and effectiveness reasons.
It would be helpful if some criteria could be formulated on what is considered as "independent". This could e.g. be aligned to the Basel Committee's advice concerning Operational Risk Management with three lines of defence: (i) business line, (ii) central Op. Risk Management, and (iii) audit.

1.1 BP.
The internet payment services security policy could be laid down in a dedicated document.

In order to minimise administrative burdens it should be possible to lay down the security policy related to the payment service offer in general in a set of related documents (e.g. the bank's general security policy) of which the internet payment services security policy document could be one.

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.

This can be agreed with the following caveats:

- Clients (business and consumer) should be held responsible for the security of and use of their own (internet) payment (internet) environment. A fair and sound balance should be reached between the responsibility of the PSPs and its service providers.
- In order to secure the whole value chain, similar security recommendations should also apply to customers and e-merchants through proper legal and contractual arrangements.
- In order to minimise administrative burdens it should be possible to integrate this "internet payment services security risk" in the existing risk management of a bank (e.g. Op. Risk management).

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.

This can be agreed with the following caveat:
In order to minimise administrative burdens it should be possible to integrate this "internet payment services security change management" in the existing management of a bank's security management process for online-banking, cards payments etc..

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.

It would be our view that all payment transaction related and personal data would need to be protected and secured, not just the sensitive ones, as otherwise "sensitive" has to be defined ex ante.

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.

Risk scenario's and security measures are carried out regulary as part of the banks' Operational Risk Management processes. Integration of these assessments of risk scenario's and measures for internet payments will not enhance the results of these existing assessments.
The timing and frequency of the reviews and risk assessments is part of the security policy.

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.

- These security measures should apply to all service providers, not only PSPs.
- Exchange of such non-competitive and anonymised information between PSPs would be effective in addressing and preventing security threats.
- There should be no need to have separated report lines. Information as part of an existing report line should be sufficient (especially Operational Risk Management reporting and Client Claims Management).

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.

This could be acceptable, as long as such monitoring and reporting of security incidents on payment products can be done as part of the overall policy on transaction/security monitoring which also addresses internet payments and does not have to be seperated out into a specific process for internet payments alone.

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.

Co-operation arrangements with the various authorities are already in place for various issues but not necessarily specifically targeting internet payments. The notification processes targeted under this recommendation should be streamlined with already existing notification processes towards these authorities so as to avoid unnecessary duplication.

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

See our comments under 3.2

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 as the basis for a sound identity and access management.

The "least privileged" principle is already in place for various issues, as this is part of the data protection procedures in banks incl. segregated IT system environments.

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.

This requirement is related to Online-Banking services in general, with "internet payments" being only a sub-set of those services.

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.

This is already part of banks' general IT security concepts, with "internet payments" being only one service of many others.

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.

While testing is a necessary step, the way it is organised and the choice of the responsible organisational unit in a PSP should be left to the discretion of each PSP.

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.

While auditing is a necessary step, the way it is organised and the choice of the responsible organisational unit in a PSP should be left to the discretion of each PSP, as both - IT systems and payment processes in general - are already part of a bank's audit processes.

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.

While the EACB appreciates and recognises the importance of requiring e-merchants to implement the proposed security measures, it has to warn against making PSPs responsible for the implementation of them by merchants. PSP's are enablers of payment services, not security authorities.

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 les 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.

Traceability and reporting are in place for all payments, not just internet payments.

Specific control and security measures for internet payments

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 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.

From the EACB's point of view, the PSPs should also provide clear and transparent information about the contractual relationship between customer/payer and the PSP, including the liability of the PSP and the obligations of the customer. Any "ad-hoc" contracts concluded by simply clicking on a "payment button" should be avoided to protect the customer.

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.

Even though anti-money laundering is a sound legitimate objective, it does not seem to belong within a document on security requirements.

6.4 KC.
PSPs should also ensure that customers are provided, on an on-going 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.

Whilst the proposal to make internet payments subject to contractual arrangements is supported, the EACB would consider it too far reaching to prescribe that separate contracts should be signed for internet payments. It should be left to individual institutions to decide how they organise their contractual relationships with their customers.

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.

Based on the above mentioned risk assessment, such white lists could also be created by the customer's PSP.

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.

The first sentence should read "...strong *customer* authentication...."

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.)

It should be clarified what is meant by "such services"

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.

This could be supported, although there are limits to the implementation power that PSPs have over e-merchants.

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.

As there is no contractual relationship between the e-merchant and the issuer, it should read "i.e. from the acquirer to the issuer".

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.

It remains unclear whether 7.7 is related to (i) cards or to (ii) wallet solutions. This schould be clarified.

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.

See remark to 7.6 KC.

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 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.**

In the context of this recommendation, the EACB would like to ask whether card readers are considered as part of such safe and trusted environment. They are not personalised but they provide a strong authentication tools. These tools do not have to be part of a safe and trusted enrol environment, because they are not personalised.

As the future development of security solutions for strong authentication cannot be foreseen, all recommendations should be phrased in a principle based way to avoid prescription of a fixed technological solution, which could be outdated soon.

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.

Unless agreed by the issuer, bypassing of strong authentication by the cardholder should not be allowed and if it were to occur, it should be under the latter's responsibility.

Recommendation 9: Log-in attempts, session time-out, validity of authentication

PSPs should limit the number of authentication attempts, define 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.

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) address12 or IP range during the internet payment session, sometimes identified by geolocation IP checks, 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.

- The level of monitoring should be proportionate to the level of security required and the strength of the customer authentication method used. For example, real time fraud detection and prevention systems are only indispensable in the case of real time authorisation, guarantee or settlement. It should also be clear that whilst the role of the issuer is key in detection of fraudulent activity, the acquirers can also help their customer base in the reduction of potential fraud.
- We question what is meant by the wording used here, and in particular it is not clear whether the risk analyses are the starting point for measurements to be taken or whether the ECB is asking for a minimum set of measurements.

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.

It is not clear what is meant by e-merchant "categories".

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.

It is not clear what is meant by "appropriate" and "unduly".

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.

It is not clear what "… until the security issues have been resolved …" means. If e.g. the customer itself is responsible for an eventual blocking of a payment transaction, the question arises as to who has to act and in which timeframe.

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.

It is unclear what is meant by "…throughout the entire duration of the internet payment service provided …",as PSPs are only a part of the whole end-to-end payment chain from

the customer to the e-merchant (with e.g. a webside payment entry solution) and parts of this chain can be outside the controll of the PSPs.

End to end security is only required when sensitive data has to travel the whole distance from endpoint to endpoint.

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.

- Instead of "such PSPs should require the e-merchants to have the necessary measures in place", we propose the following wording, "such PSPs should require the e-merchants *to adopt the same* measures *as those required of PSPs*".
- The actual implementation of the requirements by merchants is hard to verify by the PSP's or can be a very complex and costly process if e.g. checks of physical data security have to be performed at the location of the merchants IT systems.

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.

This can be a problem, as e-merchants are not obliged to have any "dedicated fraud management staff".

Customer awareness, education and communication

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 for on-going 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 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.**

The above recommendation in the EACB view addresses a responsibility that goes well beyond that of the PSPs. This concerns in particular, but not only, the third bullet. More in general, the EACB would consider that the issues raised under this recommendation require a shared effort both by PSPs and public policy in the form of financial education and education on internet use. Finally, the education provided should not exempt the customer from taking responsibility for the respecting the above obligations.

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

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.

- The offering and management of spending limits is put in place as part of the overall payment portfolio offered to clients.
- Managing spending limits should be left to the responsible market players involved in the relation with customers.

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.

- This could be extended to specific beneficiaries.

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.

It is not clear what "… to check transactions …" means. PSPs usually provide account balances (statement of accounts) with all relevant data about all transactions incl. online banking or e-business transactions.

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.