EPC185-12
Version 1.0

20 June 2012
EPC
Final

# ECB Recommendations for the Security of Internet Payments
# SecuRe Pay
# EPC response

**Circulation to: ECB**
**Restricted: No**



**General Part Comments:**

- The EPC welcomes the Forum's initiative to publish security measures for internet payments.
- The total level of security depends on the weakest link, and in that sense, the EPC would like to propose that the suggested security recommendations should apply and be enforced in the same way all over Europe. Moreover, these recommendations should apply to all players involved in the internet payment chain, meaning not only to PSPs but also to e-merchants, non-regulated service providers, etc. when relevant and through appropriate mechanisms (for example, the "General Part" in section 1, paragraph 6, mentions the applicability to e-merchants, however they are nowhere mentioned in the "Scope and addressees" later on in this section).
- EPC notes that 'third party access to customer accounts' is out of scope of this document and understands that SecuRe Pay is currently working on a separate document regarding "Access to payment accounts over the internet by third party providers". The outcome of that project should not weaken the security measures which are recommended in this more generic document. Moreover, the EPC deems it necessary that national supervisors and overseers 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.
- In addition, many providers that are playing a key role in the payment chain and hence are relevant when it comes to the topic of security in payments (e.g. non-licensed institutions), are currently not subject to supervision and oversight. The EPC believes that all providers in the field of e-payment services should be subject to oversight and supervision.
- Rules on security measures should be consistent with other regulated domains such as cybercrime, data protection, anti-money laundering, etc. Furthermore, the EPC would like to stress the need for improving and harmonising European law and procedures in respect of the domains mentioned above so that liabilities and responsibilities, as defined in the corresponding legislation, are consistent with and reflect internet payment security requirements.
- In some cases, the EPC considers that recommendations go into too much detail which creates the risk that these measures could become either inappropriate to some contexts, or obsolete as a result of innovation. Recommendations should be restricted to technology

independent security requirements, rather than prescribing specific technical solutions.

- Recommendations enforced only by European supervision and oversight bodies would not necessarily apply to non-European players which could be detrimental to a level playing field for internet payments due to differentiated security requirements.
- All means of payment need to be subject to a similar security level irrespective of the instrument, scheme or channel involved. This should be reflected in specific sets of minimum requirements. Generally, the EPC is of the opinion that the scope of the document should be more precise and comprehensive (e.g. in many instances in the document, references are made to card payment schemes whereas many of the statements may also be valid for other payment schemes using the internet).
- There is a need for clarification concerning risk management on one hand and audit functions/processes on the other.
- The EPC would also like to observe that the document focuses merely on customer authentication aspects thereby overlooking the security of the payment transaction (e.g. the integrity) and the link of the consumer authentication to the securing of the payment transaction.
- With respect to the two or more elements involved in strong authentication, special care needs to be taken to precisely define the "mutually independent" concept to ensure that current practices, e.g. involving cards and PINs, are not ruled out.
- There should be a harmonised interpretation of the various concepts, definitions and classifications used throughout the document.
- In general, the EPC assumes that these recommendations have undergone an impact assessment which has taken into consideration the various situations and points of view of the parties concerned.
- Finally, the timeframe for implementation of mid 2014 appears rather ambitious.

## 2 RECOMMENDATIONS

### GENERAL CONTROL AND SECURITY ENVIRONMENT

**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.*

**Recommendation 1 Comments:**

1.1 KC: Security measures should apply to all players, including non licensed institutions

1.2 KC: The concept of "independent" should be clarified because, unlike for the audit function, some degree of integration of the risk management function seems desirable for efficiency and effectiveness reasons.

**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 [8] and the customer.[9]*

*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.*

**Recommendation 2 Comments:**

2.1 KC: Customers should be responsible for the security and use of their own (internet) payment environment. In order to secure the whole value chain, the security measures proposed by the ECB should also apply to customers and e-merchants through proper legal and contractual arrangements.

2.3 KC: Not only sensitive data (including credentials), but also all payment transaction related data should be secured in terms of its integrity and origin.

**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.*

**Recommendation 3 Comments:**

When reporting to authorities, currently available channels should be used as much as possible. These security measures should apply to all service providers, not only PSPs.

3.2 KC and 3.3 KC: Monitoring and reporting of e-payments security incidents to the various

public authorities should be streamlined in order to avoid duplication.
3.3 KC: The EPC recommends generalising this to all major security incidents.

**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.*

**Recommendation 4 Comments:**

4.2 KC: Finding the appropriate balance between fraud prevention and ease of use for consumers is critical to ensure effective authentication of PSP websites.
4.4 KC: Whilst testing is a necessary step, the way it is organised should be left to the discretion of each PSP.
4.7 KC: Merchants should be made contractually responsible for complying with these security requirements, which should be harmonised across Europe. This would allow a proper allocation of liability amongst all parties involved.

**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.*

**Recommendation 5 Comments:**

No specific comments.

## 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[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 Comments:**

6.2 KC: This consideration should read "... use of all up-to-date hardware ..." In addition, customers should be made aware of any updates to address new security threats in order to prevent fraud. Furthermore, national transpositions of the Payment Services Directive (PSD) in this regard should be harmonised across SEPA. This should be considered during the current review of the PSD.

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

6.1 BP: Whilst it is legitimate that internet payments be subject to contractual arrangements, individual institutions should be allowed 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.*

***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 Comments:**

Customers should only be allowed to enter their credentials and authentication codes by themselves in a secure environment as indicated and approved by the issuing PSP.

With respect to authentication, protection against for example a "Man in the Middle" attack should also be effective. Here it is impossible for the issuing PSP to distinguish between the actual fraudulent and (supposedly) non-fraudulent use of authentication codes not initiated by PSP customers and/or in the secure banking environment. PSPs are not able to inform their customers whether or not these services are genuine and trustworthy. Customers themselves are also not able to recognise the difference between genuine and fraudulent services.

7.1 KC: White lists can be created by customers or their PSP.
7.2 KC: The first sentence should read "...strong customer authentication...."
7.3 KC: It should be clarified what is meant by "such services".
7.6 KC:

- As there is no contractual relationship between the e-merchant and the issuer, it should read "i.e. from the acquirer to the issuer".
- Great care has to be taken in order not to harm European merchants, acquirers, PSPs and ultimately cardholders. For example, asymmetrical liability shifts for EMV have been prejudicial towards European players. The cross border and cross region nature of internet payments will amplify the effects of an inequitable liability strategy.
- The EPC recommends that the ECB enters into a dialogue with its non-European counterparts in order to ensure a global level playing field.

**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.*

**Recommendation 8 Comments:**

8.1 KC: Has a detailed analysis of the various means of communicating security credentials been undertaken to support the recommendation made? For instance, delivery by e-mail is not always considered to be a bad practice. Another example is card-based authentication devices used in some countries for internet payments. Since these devices are not personalised and do neither contain credentials nor secret key material, secure delivery should not be required (in view of the associated costs).
8.2 KC: 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 9 Comments:**

9.3 KC: An example does not seem to be appropriate in this context as it could potentially be misinterpreted as being a recommendation.

**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.*[14]

***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.*

**Recommendation 10 Comments:**

10.1 KC: The level of monitoring should be proportionate to the level of security required and 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 detecting fraudulent activity, the acquirers can also help their customer base in the reduction of potential fraud.

**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.*

**Recommendation 11 Comments:**

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

11.3 KC: 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 e-merchants to adopt the same measures as those required of PSPs".

## 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 [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 Comments:**

Education of customers is the responsibility of the PSPs (amongst others). They need to educate their customers on the right level of security including the correct URLs and websites.

12.4 KC: Education is important but it does not exempt customers from their responsibility to keep their own environment and credentials secure. There is also a role for public authorities and legislators in this area.

**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.*

**Recommendation 13 Comments:**

13.1 KC: Managing spending limits should be left to the responsible market PSPs in relation with their customers.
13.3 BP: This can 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.*
***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.*

**Recommendation 14 Comments:**

No specific comments.

| |
|---|
| **Legislation on cybercrime**<br>**ANNEX 3: ARCHITECTURE FOR CARDHOLDER AUTHENTICATION VIA THE INTERNET**<br>**ANNEX 4: LIST OF AUTHORITIES PARTICIPATING IN THE WORK OF THE EUROPEAN FORUM ON THE SECURITY OF RETAIL PAYMENTS** |
| **Annex Comment:** |
| No specific comments. |

| |
|---|
| **ANY OTHER ASPECT** |
| **Other Comment:** |
| No specific comments. |