GEMALTO draft comments on ECB Recommendations for Security of Internet Payments

Gemalto welcomes the opportunity to comment on the European Central Bank Draft Document « Recommendations for the security of Internet payments » , a constructive basis for discussion with stakeholders in order to agree on a common baseline to build effective Internet fraud-prevention solutions, safer and convenient.

Better information about internet payment practices, including privacy and security aspects, would allow EU regulators to assess more effectively the possible need for new legal framework fine-tune. Annex I of the document suggests that existing legislation as set forth in the Payment Services Directive (2007) may not adequate for innovative Internet payments. A perceived high degree of security and privacy is of utmost importance to the future regulation. The failure to gain and maintain the user's confidence in one particular internet payment system could ultimately undermine the credibility of the whole market offer. Because of the very dynamic nature of Internet Payments Market, a heterogeneous set of different solutions are available for users, who are not always aware of the consequences and responsibilities in case of payment fraud.

Internet Payments have been identified as an increasing source of fraud. An EU harmonized set of security recommendations, that could be enforced by National Authorities as a condition to provide an "Internet Payment Provider" license could help to tackle down fraud.

COMMENTS ON GENERAL PART I

As a general comment, the key recommendations (“KCs”) set forth in the document are consistent with the “good practices” usually enforced by the relevant means of payment authorities, be there domestic or international. They are close to PCI rules, and have anyway to be followed in order for a processor to be qualified by the different schemes, according to each one’s specific agenda.

As for card payment systems, Internet Payment schemes are a two side-market, meaning that for generate a sufficient number of transactions, both online merchants and online consumers/payers have to be captured. The Internet Payments Provider intermediates between online merchants and consumers/payers. It means that the three parties involved have security requirements that should coexist. Thus recurrent marketing studies have proved that concerns for the use of online payments include:

1. Lack of confidence in Internet payment methods
2. Lack of trust in the web merchant.
3. Privacy concerns. Avoiding to provide additional private information to complete a transaction is a good incentive to pay online.
4. Simplicity and a common user experience. Internet Payment solutions are fragmented, and payers have to repeat security procedures for paying online over and over again.

Of course, ideally, unauthorized payments should be impossible, even if the customer/payer has proceeded to previous legitimate internet payments with the same provider. This means that the Internet Service Provider should be in possession of unforgeable evidence that the legitimate payer has authorized the payment, prior to provide an unforgeable transaction authorization to the merchant, a key condition for the merchant prior to deliver the good/service purchased.

From the online payment prospective, merchants and internet payment providers have to be concerned with the security of connecting with (authenticate the customer) , securing the transfer of (**transaction integrity and confidentiality**) and the ongoing safeguarding of (security and privacy concerns) of sensitive payer data.

With this respect we notice that the Draft Document provides with Key Concerns for User Authentication but :

1. **Does not provide security requirements for the integrity of the transaction itself**.
2. Does not address the requirements for the **generation and verification of "unforgeable evidence"** for authorization messages (either by the user or by the Payment Service Provider)
3. Lack of recommendations to **link the user authentication data with the payment transaction data**.

We encourage therefore the ECB, to complete this initial Draft with these additional security recommendations.

Gemalto points out that the above security requirements might be achieved by extending the successful experience of card payments to Internet Payments. **Migrating "Card-Not-Present" transactions towards a context "Card-Present" transactions** in an Unattended terminal" is the best way to tackle down Internet payment fraud. Moreover, the use of the card for Internet payments would **make feasible the deadline of mid 2014 for system migration**, in a timeline consistent with the adoption of the other SEPA payment instruments.

In contrast with our vision, we outline that the present definition of **"strong authentication"** might introduce some ambiguity for "general purpose" payment cards even if we don't think this is the purpose of the document. In this respect, we believe that the "strong authentication" definition might be further clarified**.**

Therefore, instead of :

"In addition, the elements selected must be mutually independent, i.e. the breach of one does not compromise the other(s)"

we propose the following formulation:

"In addition, the elements selected must be mutually independent **from the security point of view**, *Meaning* ***the breach or the loss of possession of one authenticating element*** *shall not compromise the other(s).* ***As an example, the loss of the card, the token or the mobile phone shall not compromise any stored personal authenticator"****.*

Because the next paragraph mentions the term " weak authentication" . A sentence such as

" Any customer authentication procedure failing to meet the above conditions is considered as a weak authentication. A weak authentication does not protect the customer against unauthorized payments, and therefore in case of repudiation, the customer cannot be liable for any financial loss resulting from a claimed misuse of his payment instrument "

could be introduced. As an example , of "weak authentication" 8.2 KC could be introduced here.

Finally, we would like to highlight:

1. The need to share the final document provisions with other supervisory/regulatory authorities for adoption. Indeed the security of internet payments is an international concern and the protection of the internet payer should be guaranteed regardless the location of the online retailer payment provider.

2. The fact that some of the provisions of this document (electronic identification and authentication) may come within the scope of other regulations. With this respect the European Commission adopted a proposal for a Regulation on ***"electronic identification and trust services for electronic transactions in the internal market".*** The proposal intends to ensure mutual recognition and acceptance of electronic Identification across borders and to establish a common framework for essential electronic trust services, namely electronic signatures, electronic seals, time stamping, electronic document acceptability, certified electronic delivery and website authentication.

3. Other than monetary loss in case of fraud, reputation risks is probably a more serious concern for online merchants. Meaning that there is a strong incentive for the online retailer to work with an Internet PSP which protects against payment incidents and in particular minimizes the risk of chargebacks.

4. The fact that ,the KC & BPs hereafter are defining objectives to be reached, and not the technical means used to achieve them. Therefore this document of requirements should be completed with a " guidelines for implementation" that could be drafted by the European Central Bank or written in collaboration with the EPC Card Stakeholders Group.

NOTA : Gemalto has no filled the "Comment" column for those sections we don’t have any particular comment to suggest

Clause	Content	Comment
General control and security environment		
Recommendation 1: Governance		
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	Upon request of the competent authority , ie audit during an accreditation process, the Internet Payment Service Provider shall provide documented evidence that these KC's are fulfilled. In case that some security services are outsourced (eg, Customer Identification Management) , the Internet Payment Service Provide is responsible for the proper fulfillment of these KC's by any subcontractor. In particular the Internet Service Provider is expected to audit and accredit their subcontractors and verify that only properly security certified components are used during the processing of any payment transaction.
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.	
Specific control and security measures for internet payments		
Recommendation 2: Risk identification and assessment		
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	When applicable,this risk assessment should include a vulnerability analysis of possible misuse of the offered services or the underlying infrastructure for the purpose of money laundering or financial crime. As a result of this risk identification analysis, a program for the security certification of all the payment system components, whose compromise might put the security system at risk should be performed.

	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	
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 KC can be expected to be fulfilled, prior to the design of the system security architecture. The changes referred in this KC, should be the result of either identified security breaches as result of payment incidents or for new attack patterns typically as a result of technological innovation made available to attackers.
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	In particular, the Internet Service Provider should conduct a " Consumer Privacy Risk Analysis". Security countermeasures to mitigate privacy risks shall be properly documented and made available for audit purposes by the relevant authority.
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	The Internet Service Provide shall implement and document corrective actions for root causes identified as the source for major payment incidents or regular minor payment incidents. The efficiency of these corrective measures shall be monitored and properly documented for auditing purposes.
Recommendation 3: Monitoring and reporting		
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 4: Risk control and mitigation		
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.	It is unclear what the "least privileged " principle refers to.
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 provisionsr e quiring 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 5: Traceability		
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	In particular, traceability data elements should be incorporated during the protocol designed for the customer authentication.
5.2 KC	PSPs should implement log files allowing any addition, change or deletion of transaction data to be traced. .	Implementation of this KC shall comply with the provisions of the applicable Data Protection laws.
5.3 KC	PSPs should query and analyse the transaction data and ensure that any log fi les can be evaluated using special tools. The respective	In particular, special tools might be used for the identification of suspicious transactions.

	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	Same comment than for 5.2 KC
Recommendation 6: Initial customer identification, information		
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.	"PSPs should ensure that the customer has undergone the necessary identification procedures and provided adequate identity documents and related information, or is already registered by the used trusted scheme, before being granted access to the internet payment services." Rationale: It could be possible to use a debit/credit payment card issued by a Bank for Internet Payments
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); – 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 7: 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	The formulation of this KC is unclear and the first requirement " should be initiated using strong authentication" seems to contradict the remainder of the KC (a "lighter" customer authentication could be acceptable for a pre-established list of beneficiaries) and be inconsistent with the example: "a customer-created list of trusted counterparties and beneficiary accounts with strong authentication" . It seems that the this sentence could be rewritten as "a customer-created list of trusted counterparties and beneficiary accounts without requiring strong authentication". However the process of creation of this list of exemptions to the general rule, should be highly secured. A non-repudiation mechanism using an electronic signature should be used so that the customer signs the list of exemptions.

		Whilst reformulated this KC could be understandable, it raises liability shift concerns in case of repudiation of a transaction whose beneficiary is in the "white list".
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	As a general principle governing customer authentication: Authentication should be proportionate to the risk of the transaction and therefore the assertion is correct. However, "pure consultative" services are out of the scope of the recommendations. We therefore recommend to add "consultative services" to the first bullet in paragraph of the SCOPE AND ADDRESSES clause "Excluded from the scope of ... and best practices are - other internet services provided by a PSP via its payment website (eg, e-brokerage, online contracts, pure consultative services" and remove this KC.
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.)	This KC focuses on PSPs "offering issuing services" and so is not, in principle, a concern for Gemalto. According to our principle of translating face to face or unattended experience for card payments, it is not indispensable to implement such internet-specific mechanisms in payment cards. We would propose following : "If specific Internet mechanisms are necessary to achieve strong authentication, 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)".
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	Same remark and proposal than **7.3 KC**

	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	Same remark and proposal than **7.3 KC**
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	In a consistent way with our comment for 7.3 KC, we propose that **7.6 KC** be completed as follows: "All card payment schemes should promote the usage or, if necessary, 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	The concept of "wallet solution" should be clarified. Add a note with a definition for "wallet solution". As an example: " In this context, a wallet is a client-server payment solution made up of (1) client card-resident applications implementing a remote payment instrument and (2) of server facilities intended to manage the connection with associated payment accounts as well as the remote administration of the wallet client"
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	We suppose that the" initial registration", refers to a new enrolled customer of the service. We suppose that this "strong authentication" refers to the new enrolled customer authentication. The text as written could be interpreted as authentication of the data required for the generation of the virtual card. If so replace " strong authentication" by "strong customer authentication"

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	The CVx2 authenticates the support, nor the cardholder.
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	A balance is to be found between convenience and strong security. In principle the authentication procedure to be used should be proportionate to the risks intrinsic to a particular payment service. Meaning that this authentication mechanism should mitigate the highest risk service. The use of an authentication mechanism designed for a high-risk transaction for low-risk transactions (eg, more frequent) weakens the security of the high-risk payment service.
Recommendation 8: Enrolment for and provision of strong authentication tools		
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.	Refer to 7.3 KC
Recommendation 9: Log-in attempts, session time-out, 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)	From a practical point of view and in order to ensure compliance with this KC , this KC should be completed. When a One-Time Password (OTP) is generated as the " next OTP without including in its calculation an information on time it was generated and/or a challenge at authentication time , it's not possible to assign a "limited time " to the OTP. Complete the KC by adding: " The calculation of the OTP should incorporate a data element, that enables the OTP verifier to ensure that the OTP is authenticated within a given validity period"
9.2 KC	PSPs should set down the maximum number of	The customer of the service should be well informed of conditions restricting access to the

	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	service.
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 authorization		
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,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	Complete this KC by adding a conclusive outcome " The PSP may decide to block a payment transaction identified as suspicious with regards the PSP risk policy . In that case, BP2 applies ".
10.2 KC	Card payment schemes in cooperation with acquirers should elaborate a harmonized definition of e-merchant categories and require acquirers to implement it accordingly in the authorisation message conveyed to the issuer.	T
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	This BP should be transformed into a KC. " The PSP shall notify the customer ..... have been resolved".
Recommendation 11: Protection of sensitive payment data		
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	Further clarification on what "strong encryption" means could be precised in a " implementation guideline document" complementing these recommendations.
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	
CUSTOMER AWARENESS, EDUCATION AND COMMUNICATION		
Recommendation 12: Customer education and communication		
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 13: Notifications, setting of limits		
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	Clauses 13 and 14, seem to focus on PSPs "offering issuing services", but it is not clearly said… We would propose to complete : "For PSPs offering issuing services […] " ;

	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 14: Verification of payment execution by the customer		
14.1 KC	PSPs should provide customers with a facility to check transactions and account balances at any time in a secure environment	Idem to Clause 13
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	