Document: Dutch (NL) input on ECB SecuRePay consultation

June 18th 2012

ECB Recommendations for the Security of Internet Payments, SecuRe Pay Consultation

Background:

On 20 April 2012, the ECB published the document "Recommendations for the Security of Internet Payments" and announced the opening of a two month consultation.

Name and organisation:

- **Donald Kohen; Dutch Payments Association**
- **Michael Samson; Dutch Banking Association**

Donald Kohen
Dutch Payments Association
Productmanagement Cards

t: +31 (0)20 3051980
m: +31 (0)6 39496011
e: d.kohen@betaalvereniging.nl
i: www.debetaalvereniging.nl

Address:
Beethovenstraat 300
1077 WZ Amsterdam

Michael Samson
Dutch Banking Association
Advisor information technology and information security
t: +31 (0)20 5502 837
m: +31 (0)6 5572 0696
e: samson@nvb.nl
i: www.nvb.nl

Address:
Gustav Mahlerplein 29-35
1082 MS Amsterdam

General Part Comment:

- The Dutch Payments Association and the Dutch Banking Association welcome 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 suggested security recommendations should apply and be enforced in the same way all over Europe. Moreover, these recommendations should apply to all payments service providers involved in the internet payment chain, meaning not only to PSPs but also to acquirers, 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).
- We note that the recommendations are addressing the current threats and vulnerabilities. The Dutch Payments Association and the Dutch Banking Association strongly recommend that also next generation threats and vulnerabilities will be addressed in the document.
- We would emphasize the difference in the current approach to deal with threats and the next generations threats (for instance advanced persistent threats). The differences in security measures are quite different in protecting your assets, a traditional criminal will go for the easiest target, an APT attacker wants a specific firm or target, so the absolute security measurements are important, not the relative. A financial Stuxnet might be developed in the future.
- Although we support new guidelines on internet security, we think that these recommendations are quite generic and do not take into account the different roles that acquirers or issuers have. Furthermore the role of internet PSP's (as intermediate between payer and payee)is not taken into account.
- Time frame for realization (midst of 2014) seems to be (much too) tight to realize.
- It is not clear what the relation is of mobile payments with this paper, this needs clarification. The environment in which the transactions are initiated could make a difference.
- We suggest that the procedure for breach notification will be kept in place according to the current way of working. In the Dutch procedure reporting is to the Dutch Central Bank
- Rules on security measures should be consistent with other regulated domains such as cybercrime, data protection, anti-money laundering, etc. Furthermore, we 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. Important aspects are: the legal framework, possibilities to exchange (fraud detection and forensic) information, simple and effective procedures for declaration and prosecution of criminal acts and blocking and recovering (potentially) fraudulent (cross border) transactions.

- We think that the security rules should apply and be enforced in the same way for every party that provides payment services in Europe. Moreover those rules should apply to all providers involved in the internet payment chain, not only to PSPs but also to non-regulated service providers, etc. where and when relevant.
- Many players essential for the security of payments (non-licensed institutions), are currently not subject to supervision and oversight. We believe that all providers of e-payment services should be subject to oversight and supervision.
- The current legal framework in e.g. the Netherlands facilitates the possibility of exchange of information on a confidential basis. Freedom of information Act does not apply meanwhile allowing the supervisory authority on an anonymous or aggregated basis to inform other government bodies were relevant.
  We recall that the current system of security measures has a sound legal basis in EU directives and EBA guidelines.
  We advocate to continue this situation of open however confidential exchange of information between PSP and supervisory authority. This should be the case for information about the state of security as well as security breaches and personal data related accidents.
- We deem 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.
- 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 and security.
- All means (depending on risk) of payment need to be subject to the same minimum security requirements irrespective of the instrument, scheme or channel involved.
- There should be a harmonised interpretation of the various concepts, definitions and classifications used throughout the document, e.g. classification of authentication instruments.
- Data protection
  Current legislation as well as the proposed data protection regulation restricts the processing and exchange of data relating to criminal offenses. To facilitate the fight against misuse of the internet payment infrastructure it is inevitable 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 the reverse of fraud 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 misuse of the internet payment system. Obstacles for the exchange of data relating to criminal offenses (including convictions related to these offenses) should be removed.

- Waiver
  The PSP's are encouraged to intervene in potential fraudulent transaction and to stop such payments temporarily or definitively. PSP's should be protected against financial claims of customers on the basis if it appears ex post that there was no fraudulent attack at stake.
- Legal basis for reversal of payment orders
  The interests of PSP and customers are served by broadening the possibilities to domestically as well as cross border reverse fraudulent payments. At this moment the originating PSP is depending of the preparedness of the beneficiary bank to cooperate in the reversal of a fraudulent payment order. Legislation should facilitate a mandatory process of reversing the payment. The definition of fraudulent payments however should well be described. Disputes between merchants and consumers about for example quality and delivery of the goods should not be in scope of fraudulent transactions.
- Consumer protection
  Currently the PSD protects the interests of consumers by establishing severe burden of proof and liability for PSP's. 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 consumer interests where the banking supervisory law should be enabled to protect the public trust and confidence.
- Security
  It is not clear how a level playing field for all (also non-European) payment solutions is secured. This should be addressed.
  The total level of security depends on the weakest link and in that sense it's strange that overlay services are out of scope of this document. SecuRe Pay works on a separate document regarding "Access to payment accounts over the internet by third party providers". The outcome of that project could weaken the security measures which are recommended in this more generic document.
  We are not able to inform our customers about correct implemented overlay services and fraudulent overlay services. Customers are never able to recognize the difference between correct and fraudulent overlay services. By supporting the initiation of transactions by overlay services all kind of implemented security measures will become more or less useless.
- From OBEP (online banking e-payments) point of view we remark that credit transfers where a third-party accesses the customer's payment and redirections should be brought in scope of the document. Also in these situations vulnerabilities exists which should be mitigated with EU-widely adopted security measurements.
- In general we concur with the view that effective risk management is required to maintain the trust in the internet payment business. We would like to emphasise that the current proposal gives on a broad spectrum recommendations which could be read as requirements which the PSP's are obliged to follow (rule based approach). This means that as new control measures emerge this document has to change with that. It would help to have a policy document that refrains from mentioning technical solutions).
- The scope of the document is set to internet payments, Other instructions flowing from client to PSP are excluded from the proposal which limits its effectiveness.

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 Comment:

- We state that all involved parties providing a function or role in the domain of internet payments should implement a formal internet security payment policy.

1.1 KC:

- Security measures should apply to all payment providers in the value chain, including non-licensed institutions.

1.1 BP:

- It should not be laid down in only one dedicated document. In order to minimise administrative burdens it should be possible to lay down security policy in a (related) set of documents.

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 Comment:

- In order to secure the complete end to end value chain in internet payments all payment service providers are responsible for thorough risk identification and vulnerability assessments.

2.1 KC:

- Clients (business and consumer) should be held responsible for the security of and use of their own (internet) payment environment. A fair and sound balance should be reached with the responsibility of the PSPs and its service providers

2.3 KC:

- It is not only sensitive data, but also all payment transaction related data should be secured with respect to its integrity and origin.

2.4 KC:

- Risk scenario's and security measures are carried out yearly on a product level. 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.

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 Comment:

- The current implementation of central monitoring, handling and follow-up of security incidents might differ within the several members of the Dutch Payments Association and the Dutch Banking Association. We recognize the statement from ECB, that the implementation process differs within each member and is depending on the security policy of a bank. The risk analysis done and consequently the necessary minimum level of implementation for monitoring can be decided depending on that security policy and risk analysis.
- In order to secure the complete end to end value chain in internet payments all payment service providers (including acquirer and issuer) are responsible for the detection and acting upon security incidents.
- We address the importance of sharing and exchanging security threats and attacks in order to prevent and act on cybercrime. (investigation on modus operandi, analysis and measurements.)
- We suggest that the procedure for breach notification will be kept in place according the current way of working. In the Dutch procedure reporting is done to the Dutch Central Bank. Additional law is currently developed in the Netherlands were security breaches and incidents involving customer data must be registered and reported.

3.1 KC:

- Monitoring and reporting of security incidents on payment products is already done, but not from a specific internet payments perspective. Transaction/security monitoring is done in general.

3.2 KC:

- Monitoring and reporting of e-payments security incidents to the various public authorities should be streamlined in order to avoid duplication.
- Cooperation with competent authorities and law enforcement agencies is already in place ,in general terms and not focused specifically on internet payments.

3.3 KC:

- We recommend generalising this to all major security incidents.
- Monitoring and reporting of e-payments security incidents to the various public authorities should be streamlined in order to avoid duplication.
- Cooperation with competent authorities and law enforcement agencies is already done. But in general and not focused on internet payments.

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 Comment:

- All payment service providers should execute the necessary vulnerability management steps to protect their assets. Focus should be on these assets which carry the most critical data and are most vulnerable.
- All PSP's should also have in place the mentioned audit procedures
- We state that the suppliers of Java, Flash and other Active Browser Components provide their customers with clear instructions on the necessity of patching and updating in order to prevent breaches.

4.2 KC:

- From OBEP point of view we remark that there is no watertight protection possible from the server (PSP) side against man in the browser attacks. It is almost impossible for a PSP to adequately identify any difference between actions performed by a man in the browser or the actual customer itself.

- We state that the most effective protection against man in the browser attacks should reside at the client/customer side. Consumer education to establish and understand how to protect the customer device against malware and phishing should be considered here.
- It is technically not possible to exclude all risks concerning Man in the Middle / Man in the Browser (but it can be mitigated by setting procedures).

4.4 KC:

- While testing is a necessary step, the way it is organised should be left to the discretion of each PSP. The recommendations should make clear what is needed and leave the way of realising it to the PSP.

4.5 KC:

- How independent should experts be who carries out the required audits?

4.7 KC:

- Merchant security requirements should be harmonised across Europe. Merchants are responsible for complying with these requirements.
- Merchants have their own responsibility for security. PSP's are enablers of payments, 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 fi les 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 fi 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 Comment:

- The current implementation of logging transaction data might differ within the several members of the Dutch Payments Association and Dutch Banking Association. We recognize the statement from ECB and add that the implementation date may differ.
- We think this is for both issuer and acquirer a responsible role. An authorisation is always granted by the issuer. Other data is also forwarded from issuer (or merchant) to acquirer. The question is how (and who) to judge the integrity of the data, when in the value chain different interpretation of the data is presented.
- Detailed logging of information is OK but the way to make transactions traceable doesn't have to be described and should be more flexible.
- Traceability is in place but not only for internet payments. Reporting is in general, not based on only internet payments as several kinds of payments are more broadly used.

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 Comment:

6.2 KC:

- We fully agree with this statement. The customer should be well informed how to act in order to authorise transactions securely. It is though of the utmost importance that third parties offering "access to account services" don't offer that service in such a way, that this would weaken the security measures of a PSP and makes the information a PSP is offering to its customer more diffuse. Also, 6.3 KC relating to compliance related clauses should be valid also for third parties offering access to account services.
- This is a role that can only be preformed by the issuer. It is not the role of an acquirer to identify the customer. The acquirer is responsible for the identification of the merchant and routes the consumer to the point of the identification and authorisation. We suggest that identification of the customer is the sole responsibility of the issuer.

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:

- This best practice is far reaching: a separate client contract would mean a large scale client contract operation.
- 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 Comment:

- We state that the usage of a strong authentication mechanism (at least two factor) should be promoted. However, current experiences with two factor based token or reader devices in the Netherlands demonstrates that this is not the Holy grail in order to prevent fraudulent transactions. Current malware introducing man-in-the-middle attacks and incidents show that two factor authentication mechanisms can be breached. New threats (especially malware) explore current vulnerabilities and will perform fraudulent transaction even with solid two factor authentication. It is the combination of awareness, vulnerability management, authentication, authorisation and security monitoring which is necessary to prevent and act upon cybercrime and thus creating a trustworthy internet payment environment.
- This is a role that can only be preformed by the issuer. It is not the role of an acquirer to identify the customer. The acquirer should authenticate the merchant is a secure way and routes the consumer to the point of the identification and authorisation.
- The customer should only be allowed to enter his/her credentials and authentication codes by him/herself in the (secure) banking environment as indicated and approved by the issuing bank.
- We support strong customer authentication as a general principle, but the necessity should always be established in relation to the actual risk at hand, the acceptance by the users and the feasibility. E.g., the used/ suggested method must be designed in a way that makes the payment flow as fluid and easy as possible. This implies that the use of 'strong customer authentication' (as defined in the Guiding Principles) is not always feasible; there should be room for other authentication procedures, possibly accompanied with other, adequate risk mitigating measures.
- For credit card payments over the internet, the migration to 3D-secure with static passwords is now being taken up, which results in a great improvement in security. A 'mandate' for 'strong authentication' could stop this migration in exchange for a longer migration to a better method, and thus resulting in a longer period before the security level of current PAN-based (possibly CVCx-based) transactions is improved.

7.1 KC:

- White lists restricted to customer-created should be extended to also bank-created white list possibilities.

7.2 KC:

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

7.3 KC:

- All cards must be technical ready; We assume that this is only applicable if and when they will be used for internet payments.

7.5 KC:

- The described interpretation freedom for compliance with this recommendation is one of the examples in this paper where the level playing field between (acquiring) competitors is threatened.

7.6 KC:

- Liability shifts from the e-merchant to the issuer are not possible. An e-merchant doesn't have a contractual relation with the card payment scheme. Liability shifts are always in accordance with the relation Issuer vs. Acquirer.

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 Comment:

- As stated in recommendation 7 the usage of strong authentication tools is only part of the chain to create a safe and secure internet payment environment. We agree that the handling of critical security devices should be executed in a secure matter, however the way this is performed is up to the involved parties. In addition to this is the fact that in the Netherlands most card readers are non personalized and do not contain any confidential data, secure delivery of these devices is not required.
- We do support strong customer authentication. However, the used/ suggested method must be designed in a way that makes the payment flow as fluid and easy as possible. Which is at least disruptive as possible and maintaining healthy conversion rates at the merchant.
- The responsibility of authentication must be between issuer and consumer.

8.1 KC:

- In the Netherlands CAP-like card readers are used for internet payments. Since these readers are not personalised and do not contain credentials nor secret key material, secure delivery should not be required. This would make the procedure very costly and it is not necessary from a security standpoint.
  Has a detailed analysis of the various means of communicating security credentials been undertaken to support the recommendation made?

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 Comment:

- No Comments

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 Comment:

- The level of monitoring should be proportionate to the level of risk and 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.

10.1 KC:

- Real time must be related to the moment of payment guarantee and/or finalising (clearing and settlement). Only by a real time payment guarantee a real time fraud detection is needed. Furthermore we agree very much with the statement that the extent of the monitoring solution should be commensurate with the outcome of the fraud risk assessment.
- The prime responsibility for detection of potential fraudulent transaction resides at the issuer. Next to this the acquirers can help their customer base in 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 Comment:

- In general terms, transaction monitoring implemented should be proportional to the risk for the specific PSP. These measures depend on the size of the PSP and in how far the PSP is under attack.
- We do agree on this, and welcome standards on how the review and set levels of protection have to be adopted.

11.3 KC:

- Complies with PCI requirements in Scheme rules for acquirers/merchants of Maestro eCommerce. Compliance to the Scheme requirements is also a way to have the necessary measures implemented by the merchant . An approval by as well a PSP as a Scheme owner is double work with no effect.
- The actual implementation of the requirements by merchants is hard to verify by the PSP's.

11.1 BP:

- Is it realistic to expect that all e-merchants will have dedicated fraud management staff?

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 Comment:

12.4 KC:

- Large scale security awareness training programs for customers are very costly for PSP's. Clients have their own responsibilities for the security of their own payment environment
- Education is important but it doesn't exempt customers from their (contract based) responsibility to keep their own environment and security credentials secure. It is not to be expected that banks will be able to secure the customers computer. The end user is responsible for the initial and continuous hardening of the devices used for internet banking.
- The education of consumers is primarily the responsibility of issuers. They need to educate their customers on the right levels of security. Including the correct url and websites.
- Prerequisite is that customers use the secure (internet) channel for information in an active way otherwise the recommendation has no effect.

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 Comment:

- We agree with the direction from ECB to give customers certain risk limitation possibilities. However the implementation and possibilities to achieve this might differ between the various PSP.
- We do agree with this. It is the role of the issuer. However, to lower risks of merchants, we suggest the possibility that a merchant can set limits as well. We state that this is not applicable for OBEP schemes where the issuer sets the limits.

13.1 KC:

- Maximum payment amounts over a certain period of time should apply to all payments and not only to internet payments.
- Managing spending limits should be left to the responsible market players involved with the relation to customers.

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 Comment:

14.1 KC: We advise to mention a secure procedure instead of secure environment as the scope of the recommendation can be seen broader than internet payments only.

Annex Comment:

We do support the arguments for the increase of (internet) infrastructure and international cybercrime legislation. The harmonisation of cybercrime legislation and investigation possibilities would be an effective development in the challenge against internet crime.

ANY OTHER ASPECT

Other Comment: