EUROPEAN CENTRAL BANK

EUROSYSTEM

RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

FINAL VERSION AFTER PUBLIC CONSULTATION

1 GENERAL PART

This report presents a set of recommendations to improve the security of internet payments. These recommendations were developed by the European Forum on the Security of Retail Payments, SecuRe Pay (the "Forum"). The Forum was set up in 2011 as a voluntary cooperative initiative between authorities. It aims to facilitate common knowledge and understanding, in particular between supervisors of payment service providers (PSPs) and overseers, of issues related to the security of electronic retail payment services and instruments provided within the European Union (EU)/European Economic Area (EEA) Member States. The Forum's work focuses on the whole processing chain of electronic retail payment services (excluding cheques and cash), irrespective of the payment channel. The Forum aims to address areas where major weaknesses and vulnerabilities are detected and, where appropriate, makes recommendations. The ultimate aim is to foster the establishment of a harmonised EU/EEA-wide minimum level of security. The authorities participating in the work of the Forum are listed in the annex.

Given the current experience of regulators, legislators, PSPs and the general public that payments made over the internet are subject to higher rates of fraud than traditional payment methods,[1] the Forum decided to develop recommendations for the security of internet payments. These reflect the experience of overseers and supervisors in their home countries and take into account the feedback obtained in a public consultation.[2]

The establishment of harmonised European recommendations for the security of internet payments is expected to contribute to fighting payment fraud and enhancing consumer trust in internet payments. The report also includes some best practices, which PSPs, governance authorities of payment schemes and other market participants, such as e-merchants, are encouraged to adopt. These best practices are important as the safety of internet payments depends on the responsible behaviour of all actors.

SCOPE AND ADDRESSEES

Unless stated otherwise, the recommendations, key considerations and best practices specified in this report are applicable to all PSPs, as defined in the Payment Services Directive,[3] providing internet payment services, as well as to governance authorities (GAs) of payment schemes[4] (including card payment schemes, credit transfer schemes, direct debit schemes, etc.). The purpose

1 Currently, publicly available EU-wide data on fraud is limited. However, according to the UK financial services industry's body, Financial Fraud, Action UK, and the French Observatory for Payment Card Security (*Observatoire de la sécurité des cartes de paiement*) card-not-present fraud has become the most prevalent type of payment fraud. See also European Central Bank (2012), *Report on card fraud*, July.

2 The public consultation on the draft recommendations was carried out from mid-April to June 2012.

3 Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, OJ L 319, 5.12.2007, p. 1.

4 The governance authority is accountable for the overall functioning of the scheme that promotes the payment instrument in question and ensuring that all the actors involved comply with the scheme's rules. Moreover, it is responsible for ensuring the scheme's compliance with oversight standards. European Central Bank (2009), *Harmonised oversight approach and oversight standards for payment instruments*, February.

of this report is to define common minimum requirements for the internet payment services listed below, irrespective of the access device used:

– [cards] the execution of card payments on the internet, including virtual card payments, as well as the registration of card payment data for use in "wallet solutions";

– [credit transfers] the execution of credit transfers (CTs) on the internet;

– [e-mandate] the issuance and amendment of direct debit electronic mandates;

– [e-money] transfers of electronic money between two e-money accounts via the internet.

Payment integrators[5] offering payment initiation services are considered either as acquirers of internet payment services (and thus as PSPs) or as external technical service providers of the relevant schemes. In the latter case, the payment integrators should be contractually required to comply with the recommendations.

Excluded from the scope of the recommendations, key considerations and best practices are:[6]

– other internet services provided by a PSP via its payment website (e.g. e-brokerage, online contracts);

– payments where the instruction is given by post, telephone order, voice mail or using SMS-based technology;

– mobile payments other than browser-based payments;[7]

– CTs where a third-party accesses the customer's payment account;

– payment transactions made by an enterprise via dedicated networks;

– card payments using anonymous and non-rechargeable physical or virtual pre-paid cards where there is no ongoing relationship between the issuer and the cardholder;

– clearing and settlement of payment transactions.

GUIDING PRINCIPLES

The recommendations are based on four guiding principles.

First, PSPs and GAs of payment schemes should perform specific assessments of the risks associated with providing internet payment services, which should be regularly updated in line with the evolution of internet security threats and fraud mechanisms. Some risks in this area have been identified in the past, for example by the Bank for International Settlements in 2003[8] or the Federal

5 Payment integrators provide the payee (i.e. the e-merchant) with a standardised interface to payment initiation services provided by PSPs.
6 Some of these items may be the subject of a separate report at a later stage.
7 Specific recommendations applying to the release and maintenance of software applications will be the subject of a separate work stream on mobile payments.
8 Bank for International Settlements (2003), *Risk Management Principles for Electronic Banking*, July.

Financial Institutions Examination Council in 2005 and 2011.[9] However, in view of the speed of technological advances and the introduction of new ways of effecting internet payments, along with the fact that fraudsters have become more organised and their attacks more sophisticated, a regular assessment of the relevant risks is of utmost importance.

Second, as a general principle, the initiation of internet payments as well as access to sensitive payment data should be protected by strong customer authentication. For the purpose of this report, sensitive payment data are defined as data which could be used to carry out fraud. These include data enabling a payment order to be initiated, data used for authentication, data used for ordering payment instruments or authentication tools to be sent to customers, as well as data, parameters and software which, if modified, may affect the legitimate party's ability to verify payment transactions, authorise e-mandates or control the account, such as "black" and "white" lists, customer-defined limits, etc.

Strong customer authentication is a procedure based on the use of two or more of the following elements – categorised as knowledge, ownership and inherence: i) something only the user knows, e.g. static password, code, personal identification number; ii) something only the user possesses, e.g. token, smart card, mobile phone; iii) something the user is, e.g. biometric characteristic, such as a fingerprint. In addition, the elements selected must be mutually independent, i.e. the breach of one does not compromise the other(s). At least one of the elements should be non-reusable and non-replicable (except for inherence), and not capable of being surreptitiously stolen via the internet. The strong authentication procedure should be designed in such a way as to protect the confidentiality of the authentication data.

From the Forum's perspective, PSPs with no or only weak authentication procedures cannot, in the event of a disputed transaction, provide proof that the customer has authorised the transaction.

Third, PSPs should implement effective processes for authorising transactions, as well as for monitoring transactions and systems in order to identify abnormal customer payment patterns and prevent fraud.

Finally, PSPs and GAs of payment schemes should engage in customer awareness and education programmes on security issues related to the use of internet payment services with a view to enabling customers[10] to use such services safely and efficiently.

The recommendations are formulated as generically as possible to accommodate continual technological innovation. However, the Forum is aware that new threats can arise at any time and will therefore review the recommendations from time to time.

This report does not attempt to set specific security or technical solutions. Nor does it redefine, or suggest amendments to, existing industry technical standards or the authorities' expectations in the areas of data protection and business continuity. When assessing compliance with the security recommendations, the authorities may take into account compliance with the relevant international standards. Where the recommendations indicate solutions, the same result may be achieved through other means.

9 Federal Financial Institutions Examination Council (2005), *Authentication in an Internet Banking Environment*, October. See also the Supplement to the 2005 guidance, June 2011.

10 Customers include both consumers and companies to which a payment service is provided.

The recommendations outlined in this report constitute minimum expectations. They are without prejudice to the responsibility of PSPs, GAs of payment schemes and other market participants to monitor and assess the risks involved in their payment operations, develop their own detailed security policies and implement adequate security, contingency, incident management and business continuity measures that are commensurate with the risks inherent in the payment services provided.

IMPLEMENTATION

The report outlines 14 recommendations to promote the security of internet payments. Each recommendation is specified through key considerations (KC). The latter must be read along with the recommendations in order to achieve a full understanding of what is expected as a minimum in order to comply with the security recommendations. Addressees are expected to comply with both the recommendations and the KCs or need to be able to explain and justify any deviation from them upon the request of the relevant competent authority (**"comply or explain" principle**). In addition, the report describes some best practices (BP) which PSPs, GAs of payment schemes and the relevant market participants are encouraged to adopt.

The legal basis for implementation of the recommendations by the national authorities is provided by the domestic legislation transposing the Payment Services Directive and/or the existing oversight and supervisory competence of the relevant authorities. The members of the Forum are committed to supporting the implementation of the recommendations in their respective jurisdictions and will integrate them in existing supervisory/oversight frameworks. The Forum will also strive to ensure effective and consistent implementation across jurisdictions and may cooperate with other competent authorities for this purpose.

The recommendations should be implemented by PSPs and GAs of payment schemes by 1 February 2015. National authorities may wish to define a shorter transition period where appropriate.

OUTLINE OF THE REPORT

The recommendations are organised into three categories.

1. **General control and security environment** of the platform supporting the internet payment service. As part of their risk management procedures, PSPs should evaluate the adequacy of their internal security controls against internal and external risk scenarios. Recommendations in the first category address issues related to governance, risk identification and assessment, monitoring and reporting, risk control and mitigation issues as well as traceability.

2. **Specific control and security measures for internet payments.** Recommendations in the second category cover all of the steps of payment transaction processing, from access to the service (customer information, enrolment, authentication solutions) to payment initiation, monitoring and authorisation, as well as the protection of sensitive payment data.

3. **Customer awareness, education and communication.** Recommendations in the third category include customer protection, what customers are expected to do in the event of an unsolicited request for personalised security credentials, how to use internet payment services safely and, finally, how customers can check that the transaction has been initiated and executed.

The report also contains a glossary of some core definitions. The annex lists the Forum members.

2 RECOMMENDATIONS

GENERAL CONTROL AND SECURITY ENVIRONMENT

Recommendation 1: Governance

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

1.1 KC The security policy should be properly documented, and regularly reviewed (in line with 2.4 KC) and approved by senior management. It should define security objectives and the risk appetite.

1.2 KC The security policy should define roles and responsibilities, including the risk management function with a direct reporting line to board level, and the reporting lines for the internet payment services provided, including management of sensitive payment data with regard to the risk assessment, control and mitigation.

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

Recommendation 2: Risk assessment

PSPs and payment schemes should carry out and document thorough risk assessments with regard to the security of internet payments and related services, both prior to establishing the service(s) and regularly thereafter.

2.1 KC PSPs and payment schemes, through their risk management function, should carry out and document detailed risk assessments for internet payments and related services. PSPs and payment schemes should consider the results of the ongoing monitoring of security threats relating to the internet payment services they offer or plan to offer, taking into account: i) the technology solutions used by them, ii) services outsourced to external providers and, iii) the customers' technical environment. PSPs and payment schemes should consider the risks associated with the chosen technology platforms, application architecture, programming techniques and routines both on their side[11] and the side of their customers,[12] as well as the results of the security incident monitoring process (see Recommendation 3).

2.2 KC On this basis, PSPs and payment schemes 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 and payment schemes should take into account the time required to implement the changes (including customer roll-out) and take the appropriate interim measures to minimise security incidents and fraud, as well as potential disruptive effects.

2.3 KC The assessment of risks should address the need to protect and secure sensitive payment data.

2.4 KC PSPs and payment schemes should undertake a review of the risk scenarios and existing security measures after major incidents affecting their services, before a major change to the infrastructure or procedures and when new threats are identified through risk monitoring activities. In addition, a general review of the risk assessment should be carried out at least once a year.

11 Such as the susceptibility of the system to payment session hijacking, SQL injection, cross-site scripting, buffer overflows, etc.
12 Such as risks associated with using multimedia applications, browser plug-ins, frames, external links, etc.

The results of the risk assessments and reviews should be submitted to senior management for approval.

Recommendation 3: Incident monitoring and reporting

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

3.1 KC PSPs and payment schemes should have a process in place to 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 payment schemes should have a procedure for notifying immediately the competent authorities (i.e. supervisory, oversight and data protection authorities), where they exist, in the event of major payment security incidents with regard to the payment services provided.

3.3 KC PSPs and payment schemes should have a procedure for cooperating on major payment security incidents, including data breaches, with the relevant law enforcement agencies.

3.4 KC Acquiring PSPs should contractually require e-merchants that store, process or transmit sensitive payment data to cooperate on major payment security incidents, including data breaches, both with them and the relevant law enforcement agencies. If a PSP becomes aware that an e-merchant is not cooperating as required under the contract, it should take steps to enforce this contractual obligation, or terminate the contract.

Recommendation 4: Risk control and mitigation

PSPs and payment schemes should implement security measures in line with their respective security policies 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 and payment schemes 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 privilege" principle[13] as the basis for a sound identity and access management.

4.2 KC PSPs and payment schemes should have appropriate security solutions in place to protect networks, websites, servers and communication links against abuse or attacks. PSPs and payment schemes should strip the servers of all superfluous functions in order to protect (harden) them and eliminate or reduce 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 privilege" 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.

13 "Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job." See Saltzer, J.H. (1974), "Protection and the Control of Information Sharing in Multics", *Communications of the ACM*, Vol. 17, No 7, pp. 388.

4.3 KC PSPs and payment schemes should have appropriate processes in place to monitor, track and restrict access to: i) sensitive payment 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 In designing,[14] developing and maintaining internet payment services, PSPs should ensure that data minimisation[15] is an essential component of the core functionality: the gathering, routing, processing, storing and/or archiving, and visualisation of sensitive payment data should be kept at the absolute minimum level.

4.5 KC Security measures for internet payment services should be tested under the supervision of the risk management function to ensure their robustness and effectiveness. All changes should be subject to a formal change management process ensuring that changes are properly planned, tested, documented and authorised. 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.

4.6 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 payment 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 (internal or external) 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.

4.7 KC Whenever PSPs and payment schemes outsource 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.

4.8 KC PSPs offering acquiring services should contractually require e-merchants handling (i.e. storing, processing or transmitting) sensitive payment data to implement security measures in their IT infrastructure, in line with KCs 4.1 to 4.7, in order to avoid the theft of those sensitive payment data through their systems. If a PSP becomes aware that an e-merchant does not have the required security measures in place, it should take steps to enforce this contractual obligation, or terminate the contract.

4.1 BP PSPs could provide security tools (e.g. devices and/or customised browsers, properly secured) to protect the customer interface against unlawful use or attacks (e.g. "man in the browser" attacks).

Recommendation 5: Traceability

PSPs should have processes in place ensuring that all transactions, as well as the e-mandate process flow, are appropriately traced.

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

14 Privacy by design.
15 Data minimisation refers to the policy of gathering the least amount of personal information necessary to perform a given function.

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

5.3 KC PSPs should query and analyse the transaction and e-mandate data and ensure that they have tools to evaluate the log files. The respective applications should only be available to authorised personnel.

5.1 BP PSPs offering acquiring services could contractually require e-merchants who store payment information to have adequate processes in place supporting traceability.

SPECIFIC CONTROL AND SECURITY MEASURES FOR INTERNET PAYMENTS

Recommendation 6: Initial customer identification, information

Customers should be properly identified in line with the European anti-money laundering legislation[16] and confirm their willingness to make internet payments using the services before being granted access to such services. PSPs should provide adequate "prior", "regular" or, where applicable, "ad hoc" 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 customer due diligence procedures, and has provided adequate identity documents[17] and related information before being granted access to the internet payment services.[18]

6.2 KC PSPs should ensure that the prior information[19] 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 transaction and/or obtain information, 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;

16 For example, Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. OJ L 309, 25.11.2005, pp. 15-36. See also Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of 'politically exposed person' and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis. OJ L 214, 4.8.2006, pp. 29-34.

17 For example, passport, national identity card or advanced electronic signature.

18 The customer identification process is without prejudice to any exemptions provided in existing anti-money laundering legislation. PSPs need not conduct a separate customer identification process for the internet payment services, provided that such customer identification has already been carried out, e.g. for other existing payment-related services or for the opening of an account.

19 This information complements Article 42 of the Payment Services Directive which specifies the information that the PSP must provide to the payment service user before entering into a contract for the provision of payment services.

– 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 specifies that the PSP may block a specific transaction or the payment instrument[20] 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 internet payment transaction or service "unblocked", in line with the Payment Services Directive.

6.4 KC PSPs should also ensure that customers are provided, on an ongoing or, where applicable, ad hoc 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 The customer could sign 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

The initiation of internet payments, as well as access to sensitive payment data, should be protected by strong customer authentication.

7.1 KC [CT/e-mandate/e-money] PSPs should perform strong customer authentication for the customer's authorisation of internet payment transactions (including bundled CTs) and the issuance or amendment of electronic direct debit mandates. However, PSPs could consider adopting alternative customer authentication measures for:

– outgoing payments to trusted beneficiaries included in previously established white lists for that customer;

– transactions between two accounts of the same customer held at the same PSP;

– transfers within the same PSP justified by a transaction risk analysis;

– low-value payments, as referred to in the Payment Services Directive.[21]

7.2 KC Obtaining access to or amending sensitive payment data (including the creation and amending of white lists) requires strong customer 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 assessment.

7.3 KC [cards] For card transactions, all card issuing PSPs should support strong authentication of the cardholder. All cards issued must be technically ready (registered) to be used with strong authentication.

20 See Article 55 of the Payment Services Directive on limits of the use of the payment instrument.
21 See the definition of low-value payment instruments in Articles 34(1) and 53(1) of the Payment Services Directive.

7.4 KC [cards] 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 solutions allowing the issuer to perform strong authentication of the cardholder for card transactions via the internet. The use of alternative authentication measures could be considered for pre-identified categories of low-risk transactions, e.g. based on a transaction risk analysis, or involving low-value payments, as referred to in the Payment Services Directive.

7.6 KC All payment schemes should promote the implementation of strong customer authentication by introducing a liability regime[22] for the participating PSPs in and across all European markets.

7.7 KC [cards] For the card payment schemes accepted by the service, providers of wallet solutions should require strong authentication by the issuer when the legitimate holder first registers the card data.

7.8 KC Providers of wallet solutions should support strong customer authentication when customers log in to the wallet payment services or carry out card transactions via the internet. The use of alternative authentication measures could be considered for pre-identified categories of low-risk transactions, e.g. based on a transaction risk analysis, or involving low-value payments, as referred to in the Payment Services Directive.

7.9 KC [cards] For virtual cards, the initial registration should take place in a safe and trusted environment[23]. Strong customer authentication should be required for the virtual card data generation process if the card is issued in the internet environment.

7.10 KC PSPs should ensure proper bilateral authentication when communicating with e-merchants for the purpose of initiating internet payments and accessing sensitive payment data.

7.1 BP [cards] E-merchants could support strong authentication of the cardholder by the issuer in card transactions via the internet.

7.2 BP For customer convenience purposes, PSPs could consider using a single strong customer authentication tool for all internet payment services. This could increase acceptance of the solution among customers and facilitate proper use.

7.3 BP Strong customer authentication could include elements linking the authentication to a specific amount and payee. This could provide customers with increased certainty when authorising payments. The technology solution enabling the strong authentication data and transaction data to be linked should be tamper resistant.

22 The liability regime should provide that a PSP must refund other PSPs for any fraud resulting from weak customer authentication.

23 Environments under the PSP's responsibility where adequate authentication of the customer and of the PSP offering the service and the protection of confidential/sensitive information is assured include: i) the PSP's premises; ii) internet banking or other secure website, e.g. where the GA offers comparable security features inter alia as defined in Recommendation 4; or iii) automated teller machine (ATM) services. (In the case of ATMs, strong customer authentication is required. Such authentication is typically provided by chip and PIN, or chip and biometrics.)

Recommendation 8: Enrolment for and provision of authentication tools and/or software delivered to the customer

PSPs should ensure that customer enrolment for and the initial provision of the authentication tools required to use the internet payment service and/or the delivery of payment-related software to customers is carried out in a secure manner.

8.1 KC Enrolment for and provision of authentication tools and/or payment-related software delivered to the customer should fulfil the following requirements.

– The related procedures should be carried out in a safe and trusted environment while taking into account possible risks arising from devices that are not under the PSP's control.

– Effective and secure procedures should be in place for the delivery of personalised security credentials, payment-related software and all internet payment-related personalised devices. Software delivered via the internet should also be digitally signed by the PSP to allow the customer to verify its authenticity and that it has not been tampered with.

– [cards] For card transactions, the customer should have the option to register for strong authentication independently of a specific internet purchase. Where activation during online shopping is offered, this should be done by re-directing the customer to a safe and trusted environment.

8.2 KC [cards] Issuers should actively encourage cardholder enrolment for strong authentication and allow their cardholders to bypass enrolment only in an exceptional and limited number of cases where justified by the risk related to the specific card transaction.

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

PSPs should limit the number of log-in or authentication attempts, define rules for internet payment services 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.

9.2 KC PSPs should set down the maximum number of failed log-in or authentication attempts after which access to the internet payment service is (temporarily or permanently) blocked. They should have a secure procedure in place to re-activate blocked internet payment services.

9.3 KC PSPs should set down the maximum period after which inactive internet payment services sessions are automatically terminated.

Recommendation 10: Transaction monitoring

Transaction monitoring mechanisms designed to prevent, detect and block fraudulent payment transactions should be operated before the PSP's final authorisation; suspicious or high risk transactions should be subject to a specific screening and evaluation procedure. Equivalent security monitoring and authorisation mechanisms should also be in place for the issuance of e-mandates.

10.1 KC PSPs should use fraud detection and prevention systems to identify suspicious transactions before the PSP finally authorises transactions or e-mandates. Such systems should be based, for example, on parameterised rules (such as black lists of compromised or stolen card data), and monitor

abnormal behaviour patterns of the customer or the customer's access device (such as a change of Internet Protocol (IP) address[24] or IP range during the internet payment services session, sometimes identified by geolocation IP checks,[25] atypical e-merchant categories for a specific customer or abnormal transaction data, etc.). Such systems should also be able to detect signs of malware infection in the session (e.g. via script versus human validation) and known fraud scenarios. The extent, complexity and adaptability of the monitoring solutions, while complying with the relevant data protection legislation, should be commensurate with the outcome of the 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 PSP's authorisation message conveyed to the issuer.[26]

10.3 KC Acquiring PSPs should have fraud detection and prevention systems in place to monitor e-merchant activities.

10.4 KC PSPs should perform any transaction screening and evaluation procedures within an appropriate time period, in order not to unduly delay the initiation and/or execution of the payment service concerned.

10.5 KC Where the PSP, according to its risk policy, decides to block a payment transaction which has been identified as potentially fraudulent, the PSP should maintain the block for as short a time as possible until the security issues have been resolved.

Recommendation 11: Protection of sensitive payment data

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

11.1 KC All data used to identify and authenticate customers (e.g. at log-in, when initiating internet payments, and when issuing, amending or cancelling e-mandates), 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 exchanging sensitive payment data via the internet, secure end-to-end encryption[27] is applied between the communicating parties throughout the respective communication session, in order to safeguard the confidentiality and integrity of the data, using strong and widely recognised encryption techniques.

11.3 KC PSPs offering acquiring services should encourage their e-merchants not to store any sensitive payment data. In the event e-merchants handle, i.e. store, process or transmit sensitive payment data, such PSPs should contractually require the e-merchants to have the necessary measures in place to protect these data. PSPs should carry out regular checks and if a PSP becomes aware that an e-merchant handling sensitive payment data does not have the required security measures in place, it should take steps to enforce this contractual obligation, or terminate the contract.

24 An IP address is a unique numeric code identifying each computer connected to the internet.
25 A "Geo-IP" check verifies whether the issuing country corresponds with the IP address from which the user is initiating the transaction.
26 E-merchant categories refer to the classification of merchants according to sector of business activity. Currently the e-merchant categories are not yet standardised across card payment schemes and not always conveyed in the authorisation message. The harmonised classification of e-merchant categories (based, for example, on the European NACE classification) would help PSPs to analyse the fraud risk of a transaction.
27 End-to-end-encryption refers to encryption within or at the source end system, with the corresponding decryption occurring only within or at the destination end system. ETSI EN 302 109 V1.1.1. (2003-06).

11.1 BP It is desirable that e-merchants handling sensitive payment data appropriately train their 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

PSPs should provide assistance and guidance to customers, where needed, with regard to the secure use of the internet payment services. PSPs should communicate with their customers in such a way as to reassure them of the authenticity of the messages received.

12.1 KC PSPs should provide at least one secured channel[28] 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 services session and/or possible social engineering[29] 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 their non-initiation, or warn the customer about the occurrence of attacks (e.g. phishing e-mails).

12.2 KC Through the secured channel, PSPs should keep customers informed about updates in security procedures regarding internet payment services. Any alerts about significant emerging risks (e.g. warnings about social engineering) should also be provided via the secured 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 related services, and customers should be appropriately informed about how such assistance can be obtained.

12.4 KC PSPs, and, where relevant, 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 of the PSP.

28 Such as a dedicated mailbox on the PSP's website or a secured website.

29 Social engineering in this context means techniques of manipulating people to obtain information (e.g. via e-mail or phone calls), or retrieving information from social networks, for the purposes of fraud or gaining unauthorised access to a computer or network.

12.5 KC Acquiring PSPs should require e-merchants to clearly separate payment-related processes from the online shop in order to make it easier for customers to identify when they are communicating with the PSP and not the payee (e.g. by re-directing the customer and opening a separate window so that the payment process is not shown within a frame of the e-merchant).

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

Recommendation 13: Notifications, setting of limits

PSPs should set limits for internet payment services and could provide their customers with options for further risk limitation within these limits. They may also provide alert and customer profile management services.

13.1 KC Prior to providing a customer with internet payment services, PSPs should set limits[30] applying to those services, (e.g. a maximum amount for each individual payment or a cumulative amount over a certain period of time) and should inform their customers accordingly. PSPs should allow customers to disable the internet payment functionality.

13.1 BP Within the set limits, PSPs could provide their customers with the facility to manage limits for internet payment services in a safe and trusted environment.

13.2 BP PSPs could implement alerts for customers, such as via phone calls or SMS, for suspicious or high risk payment transactions 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 and related services, e.g. that they will only initiate payments from certain specific countries and that payments initiated from elsewhere should be blocked, or that they may include specific payees in white or black lists.

Recommendation 14: Customer access to information on the status of payment initiation and execution

PSPs should confirm to their customers the payment initiation and provide customers in good time with the information necessary to check that a payment transaction has been correctly initiated and/or executed.

14.1 KC [CT/e-mandate] PSPs should provide customers with a near real-time facility to check the status of the execution of transactions as well as account balances at any time[31] in a safe and trusted environment.

14.2 KC Any detailed electronic statements should be made available in a safe and trusted environment. Where PSPs inform customers about the availability of electronic statements (e.g. regularly when a periodic 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 communications or, if included, they should be masked.

30 Such limits may either apply globally (i.e. to all payment instruments enabling internet payments) or individually.
31 Excluding exceptional non-availability of the facility for technical maintenance purposes, or as a result of major incidents.

GLOSSARY OF TERMS

The following terms are defined for the purpose of this report.

Term	Definition
Authentication	A procedure that allows the PSP to verify a customer's identity.
Authorisation	A procedure that checks whether a customer or PSP has the right to perform a certain action, e.g. the right to transfer funds, or to have access to sensitive data.
Credentials	The information – generally confidential – provided by a customer or PSP for the purposes of authentication. Credentials can also mean the physical tool containing the information (e.g. one-time-password generator, smart card), or something the user memorises or represents (such as biometric characteristics).
Major payment security incident	An incident which has or may have a material impact on the security, integrity or continuity of the PSP's payment-related systems and/or the security of sensitive payment data or funds. The assessment of materiality should consider the number of potentially affected customers, the amount at risk and the impact on other PSPs or other payment infrastructures.
Transaction risk analysis	Evaluation of the risk related to a specific transaction taking into account criteria such as, for example, customer payment patterns (behaviour), value of the related transaction, type of product and payee profile.
Virtual cards	A card-based payment solution where an alternative, temporary card number with a reduced validity period, limited usage and a pre-defined spending limit is generated which can be used for internet purchases.
Wallet solutions	Solutions that allow a customer to register data relating to one or more payment instruments in order to make payments with several e-merchants.

ANNEX: LIST OF AUTHORITIES PARTICIPATING IN THE WORK OF THE EUROPEAN FORUM ON THE SECURITY OF RETAIL PAYMENTS

	Members
BE	Nationale Bank van België/Banque Nationale de Belgique
BG	Българска народна банка (Bulgarian National Bank)
CZ	Česká národní banka
DK	Danmarks Nationalbank Finanstilsynet
DE	Deutsche Bundesbank Bundesanstalt für Finanzdienstleistungsaufsicht
EE	Eesti Pank Finantsinspektsioon
IE	Central Bank of Ireland
GR	Bank of Greece
ES	Banco de España
FR	Banque de France Autorité de Contrôle Prudentiel
IT	Banca d'Italia
CY	Central Bank of Cyprus
LV	Latvijas Banka Finanšu un kapitāla tirgus komisija
LT	Lietuvos bankas
LU	Banque centrale du Luxembourg Commission de Surveillance du Secteur Financier
HU	Magyar Nemzeti Bank Pénzügyi Szervezetek Állami Felügyelete

	Members
MT	Central Bank of Malta
NL	De Nederlandsche Bank
AT	Oesterreichische Nationalbank Österreichische Finanzmarktaufsicht
PL	Narodowy Bank Polski Komisja Nadzoru Finansowego
PT	Banco de Portugal
RO	Banca Națională a României
SI	Banka Slovenije
SK	Národná banka Slovenska
FI	Suomen Pankki – Finlands Bank Finanssivalvonta
SE	Sveriges Riksbank Finansinspektionen
UK	Financial Services Authority
	European Banking Authority European Central Bank

	Observers
IS	Central Bank of Iceland Fjármálaeftirlitið
LI	Liechtensteinische Landesbank 1861 Finanzmarktaufsicht Liechtenstein
NO	Norges Bank Finanstilsynet – The Financial Supervisory Authority of Norway
	European Commission Europol

© European Central Bank, 2013

Address: Kaiserstrasse 29, 60311 Frankfurt am Main, Germany

Postal address: Postfach 16 03 19, 60066 Frankfurt am Main, Germany

Telephone: +49 69 1344 0; Website: http://www.ecb.europa.eu; Fax: +49 69 1344 6000

All rights reserved. Reproduction for educational and non-commercial purpose is permitted provided that the source is acknowledged.

ISSN 978-92-899-0866-5 (online)
EU catalogue number QB-30-13-188-EN-N (online)