EUROPEAN CENTRAL BANK

EUROSYSTEM

RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

APRIL 2012

EUROPEAN CENTRAL BANK

EUROSYSTEM

In 2012 all ECB publications feature a motif taken from the €50 banknote.

RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

APRIL 2012

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

CONTENTS

I 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 or by providers located in the EU/EEA.

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, can make recommendations. The ultimate aim is to foster the establishment of a harmonised EU/EEA-wide minimum level of security, as well as to facilitate a common understanding between the relevant authorities.

The authorities participating in the work of the Forum are listed in Annex 4.

In 2011 the Forum's work focused on developing recommendations for the security of internet payments. The current experience of regulators, legislators, PSPs and the general public is that payments made over the internet are subject to higher rates of fraud than traditional payment methods.[1]

In preparing the recommendations, the Forum carried out a fact-finding exercise and consulted with PSPs, technical service providers and e-merchants in order to gain a better understanding of the relevant issues. The recommendations reflect the experience of overseers and supervisors in their home countries and the information obtained through the consultation process.

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 recommendations also include some best practices, which PSPs 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,[2] providing internet payment services. For the purposes of this report, internet payment services include:

– [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";

– [CT/e-mandate] the execution of credit transfers on the internet, or direct debit electronic mandates,[3] i.e. a framework contract providing for a series of payment transactions, where the payer authorises its

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.

2 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.

3 Since one-off direct debit transactions are initiated and executed through the mechanism of the direct debit scheme concerned, rather than over the internet, these transactions fall outside the scope of this report.

PSP over the internet using web-based technology (as, for example, in e-banking).

Owing to the specific nature of card payments, some recommendations are addressed to PSPs offering acquiring and/or issuing services, as well as to the governance authority[4] of the respective card payment scheme.

Excluded from the scope of the recommendations, key considerations and best practices are:[5]

- other internet services provided by a PSP via its payment website (e.g. e-brokerage, online contracts);
- non-internet-based payments where the instruction is given by post, telephone order, voice mail or using SMS-based technology;
- transfers of electronic money between two e-money accounts;
- credit transfers where a third-party accesses the customer's payment account;
- redirections, i.e. where the payer is redirected to the PSP by a third party in the context of a credit transfer and/or direct debit, the redirection itself is excluded;
- payment transactions made by an enterprise via dedicated networks;
- card payments using corporate cards, i.e. cards issued to an enterprise for use by its employees or agents acting on its behalf;
- card payments using anonymous, non-rechargeable physical or virtual pre-paid cards where there is no ongoing relationship between the issuer and the virtual cardholder;
- the clearing and settlement of internet payment transactions, as this typically takes place via (designated) mechanisms other than the internet.

GUIDING PRINCIPLES

The recommendations are based on four guiding principles.

First, PSPs 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. Some risks in this area have been identified in the past, for example by the Bank for International Settlements in 2003[6] or the Federal Financial Institutions Examination Council in 2005 and 2011.[7] 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 internet payment services provided by PSPs should be initiated by means of strong customer authentication.

Strong customer authentication is a procedure that enables the PSP to verify the identity of a customer. The use of two or more of the following elements – categorised as knowledge, ownership and inherence – is required:

- *something only the user knows, e.g. password, personal identification number;*
- *something only the user possesses, e.g. token, smart card, mobile phone;*

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.

5 Some of these items may be the subject of a separate report at a later stage.

6 Bank for International Settlements (2003), *Risk Management Principles for Electronic Banking*, July.

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

– *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 to mitigate the risks related to 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 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 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 relevant authorities' expectations in the areas of data protection and business continuity. Where the recommendations indicate solutions, PSPs may achieve the same result through other means.

The recommendations outlined in this report constitute minimum expectations. They are without prejudice to the responsibility of PSPs 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 key considerations (KC) or need to be able to explain and justify any deviation from them upon the request of their national overseers and/or supervisory authorities ("comply or explain" principle). In addition, the report describes some best practices (BP) which the relevant market participants are encouraged to adopt.

The legal basis for implementation of the recommendations by the national authorities may be 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. The Forum will also strive to ensure effective and consistent implementation across jurisdictions and may cooperate with other competent authorities for this purpose.

The implementation process will, depending on the relevant existing national legal frameworks, be monitored by those authorities that are members of the Forum (supervisors of PSPs and/or overseers), with the potential involvement of other competent authorities.

The recommendations outlined in this report should be implemented by PSPs and card payment schemes by 1 July 2014. National authorities may wish to define a shorter implementation 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.

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 executed.

The report also contains a glossary of some core definitions. Three annexes are attached. Annex 1 outlines a number of points for the European Commission to consider in the forthcoming review of the Payment Services Directive. Annex 2 provides information on broader issues concerning the security of internet payments. Annex 3 provides some background information on the architecture for cardholder authentication via the internet. Finally, Annex 4 lists the Forum members.

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 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 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.

8 Such as the susceptibility of the system to payment session hijacking, SQL injection, cross-site scripting, buffer overflows, etc.

9 Such as risks associated with using multimedia applications, browser plug-ins, frames, external links, etc.

3.2 KC PSPs and card payment schemes should have a procedure for notifying the competent authorities (i.e. supervisory, oversight and data protection authorities) immediately in the event of major incidents with regard to the services provided.

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

Recommendation 4: Risk control and mitigation

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

10 "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.

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 5: Traceability

PSPs should have processes in place ensuring that all transactions can be appropriately traced.

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

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

5.3 KC *PSPs should query and analyse the transaction data and ensure that any log files 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.*

SPECIFIC CONTROL AND SECURITY MEASURES FOR INTERNET PAYMENTS

Recommendation 6: Initial customer identification, information

Customers should be properly identified and confirm their willingness to conduct internet payment transactions before being granted access to such services. PSPs should provide adequate "prior" and "regular" information to the customer about the necessary requirements (e.g. equipment, procedures) for performing secure internet payment transactions and the inherent risks.

6.1 KC *PSPs should ensure that the customer has undergone the necessary identification procedures and provided adequate identity documents and related information before being granted access to the internet payment services.*

6.2 KC *PSPs should ensure that the prior information*[11] *supplied to the customer contains specific details relating to the internet payment services. These should include, as appropriate:*

- *clear information on any requirements in terms of customer equipment, software or other necessary tools (e.g. antivirus software, firewalls);*
- *guidelines for the proper and secure use of personalised security credentials;*
- *a step-by-step description of the procedure for the customer to submit and authorise a payment, including the consequences of each action;*
- *guidelines for the proper and secure use of all hardware and software provided to the customer;*
- *the procedures to follow in the event of loss or theft of the personalised security credentials or the customer's hardware or software for logging in or carrying out transactions;*
- *the procedures to follow if an abuse is detected or suspected;*
- *a description of the responsibilities and liabilities of the PSP and the customer respectively with regard to the use of the internet payment service.*

6.3 KC *PSPs should ensure that the framework contract with the customer includes compliance-related clauses enabling the PSP to fulfil its legal obligations relating to the prevention of money laundering, which may require it to suspend execution of a customer's payment transaction pending the necessary regulatory checks and/or to refuse to execute it. The contract should also specify that the PSP may block a specific transaction or the payment instrument on the basis of security concerns. It should set out the method and terms of the customer notification and how the customer can contact the PSP to have the service "unblocked", in line with the Payment Services Directive.*

6.4 KC *PSPs should also ensure that customers are provided, on an ongoing basis and via appropriate means (e.g. leaflets, website pages), with clear and straightforward instructions explaining their responsibilities regarding the secure use of the service.*

6.1 BP *It is desirable that the customer signs a dedicated service contract for conducting internet payment transactions, rather than the terms being included in a broader general service contract with the PSP.*

Recommendation 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*

11 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.

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

PSPs should limit the number of authentication attempts, define rules for payment session "time out" and set time limits for the validity of authentication.

9.1 KC *When using a one-time password for authentication purposes, PSPs should ensure that the validity period of such passwords is limited to the strict minimum necessary (i.e. a few minutes).*

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

9.3 KC *PSPs should set down the maximum period after which inactive payment sessions are automatically terminated, e.g. after ten minutes.*

Recommendation 10: Transaction monitoring and authorisation

Security monitoring and transaction authorisation mechanisms aimed at preventing, detecting and blocking fraudulent payment transactions before they are executed should be conducted in real time; suspicious or high risk transactions should be subject to a specific screening and evaluation procedure prior to execution.

10.1 KC *PSPs should use real-time fraud detection and prevention systems to identify suspicious transactions, for example based on parameterised rules (such as black lists of compromised or stolen card data), abnormal behaviour patterns of the customer or the customer's access device (change of Internet Protocol (IP) address[12] or IP range during the internet payment session, sometimes identified*

12 An IP address is a unique numeric code identifying each computer connected to the internet.

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 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.*

13 A "Geo-IP" check verifies whether the issuing country corresponds with the IP address from which the user is initiating the transaction.

14 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 would help PSPs to analyse the fraud risk of a transaction.

CUSTOMER AWARENESS, EDUCATION AND COMMUNICATION

Recommendation 12: Customer education and communication

PSPs should communicate with their customers in such a way as to reassure them of the integrity and authenticity of the messages received. The PSP should provide assistance and guidance to customers with regard to the secure use of the internet payment service.

12.1 KC *PSPs should provide at least one secured channel*[15] *for ongoing communication with customers regarding the correct and secure use of the internet payment service. PSPs should inform customers of this channel and explain that any message on behalf of the PSP via any other means, such as e-mail, which concerns the correct and secure use of the internet payment service, is not reliable. The PSP should explain:*

- *the procedure for customers to report to the PSP (suspected) fraudulent payments, suspicious incidents or anomalies during the internet payment session and/or possible social engineering*[16] *attempts;*
- *the next steps, i.e. how the PSP will respond to the customer;*
- *how the PSP will notify the customer about (potential) fraudulent transactions or warn the customer about the occurrence of attacks (e.g. phishing e-mails).*

12.2 KC *Through the designated channel, PSPs should keep customers informed about updates in procedures and security measures regarding internet payment services. Any alerts about significant emerging risks (e.g. warnings about social engineering) should also be provided via the designated channel.*

12.3 KC *Customer assistance should be made available by PSPs for all questions, complaints, requests for support and notifications of anomalies or incidents regarding internet payments, and customers should be appropriately informed about how such assistance can be obtained.*

12.4 KC *PSPs and, where relevant, card payment schemes should initiate customer education and awareness programmes designed to ensure customers understand, at a minimum, the need:*

- *to protect their passwords, security tokens, personal details and other confidential data;*
- *to manage properly the security of the personal device (e.g. computer), through installing and updating security components (antivirus, firewalls, security patches);*
- *to consider the significant threats and risks related to downloading software via the internet if the customer cannot be reasonably sure that the software is genuine and has not been tampered with;*
- *to use the genuine internet payment website.*

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

Recommendation 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*

15 Such as by letter with acknowledgement of receipt signed by the customer, a dedicated mailbox on the PSP's website, or a secured website.

16 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.

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 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.*

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 incident	An incident which has or may have a material impact on the security, integrity or continuity of the PSP's 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.
Sensitive payment data	Data which could be used to carry out fraud. These include data allowing a payment order to be initiated; data used for authentication; data used for ordering payment instruments or authentication tools sent to customers; or data which may affect the customer's ability to verify transactions or control the account, such as a postal address, e-mail address, "black" and "white" lists, customer-defined limits, etc.
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 cards in order to make e-money or card payments with several e-merchants.

ANNEX 1: THE REVIEW OF THE PAYMENT SERVICES DIRECTIVE: POINTS TO CONSIDER

Article 87 of the Payment Services Directive requires the European Commission to present a report giving a full economic and legal assessment of the implementation and impact of the Directive, accompanied, where appropriate, by a proposal for its revision, no later than 1 November 2012. In the light of this review, some aspects of the recommendations laid down in this report deserve further clarification from a legal perspective.

1) ACQUIRING SERVICES SHOULD ONLY BE PROVIDED BY LICENSED PROVIDERS

In the forthcoming review, greater clarity should be given to the meaning of "acquiring services", including the services provided by payment integrators. In particular, any provider offering acquiring services should be authorised or acting as an agent for an authorised entity. Currently not all providers are regulated and the competent authorities are therefore unable to review their security arrangements.

2) THE LEGAL FRAMEWORK FOR REPUDIATION AND RELATED LIABILITIES WITH RESPECT TO TRANSACTIONS VIA THE INTERNET SHOULD PROVIDE SUFFICIENT CLARITY TO ENHANCE TRUST IN THESE PAYMENT SERVICES

The Forum submits that:

- the option in Article 61(3) of the Directive for a Member State to reduce the payer's liability for unauthorised payment transactions has led to very diverse liability regimes across countries for such transactions, including internet payment transactions;
- more clarity is needed regarding the burden of proof (Article 59(1)) and consumer liability (see above, Article 61(3));
- different payer liability regimes should be introduced for internet payment transactions taking into account whether or not strong authentication is used.

The option in Article 61(3) has not been transposed by 14 Member States.[17] For these countries, the payer's maximum liability in the event of an unauthorised payment transaction, including internet payment transactions is, in principle, limited to € 150 (or national currency equivalent).

The option has been transposed in 13 Member States. For unauthorised card transactions, seven countries[18] have reduced the maximum amount borne by the payer to zero. For three Member States, the payer's liability never exceeds € 100 or national currency equivalent.[19] In Portugal the payer's liability is limited to the balance available or the associated credit line. Austrian legislation reduces the payer's liability by providing for it to be shared.

Some of these countries apply these reductions only under certain conditions:

- payment executed without electronic identification (i.e. without personalised security features): Belgium, Denmark;
- payment initiated by means of information technology or a telecommunication device: Hungary;
- payment initiated in connection with a distance contract: United Kingdom (there is no payer liability);
- Italy and Romania apply the same conditions as for physical card payment transactions;
- consumer card payments made with a lost or stolen card: Latvia (there is no payer liability).

This situation generates different incentives or disincentives for the implementation of authentication of card transactions by e-merchants, acquirers, issuers and cardholders.

17 Bulgaria, Czech Republic, Germany, Estonia, Greece, Spain, Cyprus, Lithuania, Luxembourg, Malta, Netherlands, Poland, Slovenia and Finland.
18 Belgium, Denmark, France, Italy, Latvia, Hungary and the United Kingdom.
19 € 75 for Ireland, € 100 for Slovakia and the equivalent in leu of € 50 for Romania.

The Forum concludes that where there is no or weak authentication procedure in place, in the event of a disputed transaction, PSPs cannot provide proof that the customer has authorised the transaction. When strong authentication is used, it is for the issuer to prove that the cardholder has acted with gross negligence or intent. An incentive (e.g. liability shift) in the Directive for PSPs and e-merchants to use strong authentication would be welcome. Different payment liability regimes could be introduced harmonising the payer's liability in the event of unauthorised internet payment transactions.

3) COMMUNICATION OF DATA BREACHES

The European Commission could consider setting up a structure to facilitate the exchange of information and cooperation between PSPs, supervisory authorities/overseers and data protection authorities with regard to data breaches in order to help limit the financial consequences.

4) SCOPE OF THE DIRECTIVE

Currently the rules apply where the PSPs of both the payer and the payee are located in the EU/EEA and where the transaction is in euro or in the currency of a non-euro area Member State. However, the internet is a worldwide network and threats and frauds affecting customers and PSPs may of course arise from outside the EU/EEA. The Commission noted in the preamble[20] to the Directive that, "with regard to the global integration of financial services and harmonised consumer protection ... focal points of the review should be the possible need to expand the scope of application with regard to ... payment transactions where only one PSP concerned is located in the Community". The Forum believes that where a payer's PSP is located in the EU/EEA, this alone should bring the transaction under the scope of the Directive. A customer's liability for fraud should not be dependent on the location of the payee's service provider.

20 Recital 54.

ANNEX 2: SECURITY OF THE ENVIRONMENT UNDERPINNING INTERNET PAYMENTS

Payment security is the result of the complex interaction of all actors playing a role in the payments industry, such as PSPs, cardholders, technical service providers and e-merchants.

Mitigating the risk of fraud requires that each actor makes a continuous effort to implement and maintain security "best practices" in its own domain. The level of security depends not only on the behaviour of each actor but also on the larger environment underpinning the payments industry, such as, for example the role of infrastructure providers, technology and regulation.

Efforts to improve the level of security of internet payments should take into account internet infrastructure and technology, sound software packages for users and the importance of global standards on cybercrime.

These aspects are beyond the Forum's mandate and are therefore not addressed in the recommendations. However, they represent a potential point of failure in the payment chain and therefore require attention.

INTERNET INFRASTRUCTURE AND TECHNOLOGY

Without secure internet infrastructures and reliable technology providers behind them, PSPs would not be able to provide secure internet payment services to their customers. A sound global infrastructure is crucial for shoppers to navigate online and purchase items safely and securely. In a general sense, each market operator implements security requirements covering its own domain, but the security level of the payment transaction chain overall also depends on external factors.

Examples include the following.

1) SSL Protocol: implements encryption techniques designed to protect data from being intercepted over insecure networks and to prove that a website is authentic rather than a counterfeited impostor. The protocol is implemented by the popular browsers (such as MIE, Firefox, Google Chrome, Opera, Safari) which, de facto, set the standard for secure connections between personal computers and web servers. E-merchants and financial institutions develop their websites following the protocol evolutions set by browser developers (Microsoft, Mozilla, etc.). An incorrect implementation of the SSL protocol can lead to security vulnerabilities.

2) SSL Certificates: SSL protocol provides website authentication based on a "digital certificate" issued by a certification authority such as VeriSign, Entrust, Comodo and Global Sign. In order to obtain such a certificate, the website's owner needs to give the authority documentary proof of entitlement to receive it. Authorities issuing SSL certificates are generally private multinational companies that are not subject to a specific oversight regime. The most popular browsers have an embedded list of approximately one hundred certification authorities which they use to verify websites' SSL digital certificates. The list of "recognised" authorities for an SSL connection is therefore indirectly defined by browser developers.

3) Device tokens: strong authentication procedures are based on specific products like hardware tokens generating one-time passwords. These products have been launched on the market by few specialised manufacturers, such as RSA and Vasco, targeting a variety of sectors (financial, industry, governmental agencies, etc.) with the same technology and management procedures. However, the market is characterised by a few large suppliers and security breaches experienced recently by a single manufacturer have led to potential security risks for millions of users.

Based on the above-mentioned examples, it is clear that a few critical players have a "systemic role" in realising a global "security infrastructure". This infrastructure is used by market operators to interact and carry out specific security procedures. In 2011 the

financial industry experienced a variety of security incidents, related to weaknesses in these critical players and internet infrastructures more generally.

The following aspects are crucial for the security of internet payments: i) "diversity" of technology providers in the market in order to avoid risk concentration; ii) secure internet infrastructures (SSL, DNS and DN Registrar, etc); and iii) promoting the soundness of critical technology providers.

SOFTWARE

Very often an attacker's intrusion is successful because of weaknesses or defects in software packages installed in users' devices (e.g. smart phones, computers), web servers and network equipments.

Users' devices are especially vulnerable, given that:

- generally users have neither a clear awareness of internet risks, nor the required technical skills to protect their device;
- software manufacturers usually disclaim liability for defects;
- users might have difficulty in promptly installing "patches" on the device.

The user device, for the most part, is an insecure environment where sensitive data, like authentication codes, are managed with high levels of risk. However users should only assume responsibility for risks that they can, to some extent, control in terms of risk avoidance and risk mitigation. Indeed there are weaknesses in the systems that the user cannot influence. As a result, users who are victims of fraud or other security breaches need assistance as well as effective prevention and control systems based on safe and easy-to-use solutions.

In line with the recommendations, financial institutions, e-merchants and card payment schemes should help users through awareness programmes, providing user support services on IT security and giving advice on recommended security tools.

As an additional step, the financial industry could promote the development of specific tools for carrying out financial transactions on the internet, such as secure customised browsers, operating systems, and authentication methods specifically designed to mitigate the risk of "man in the middle", "man in the browser" and "man in the application" attacks perpetrated via malicious code.

A crucial issue is the "intrinsic" security of commercial software packages which are not specifically designed for internet payment services. In this context, authorities and regulators could encourage the software industry to develop more secure software products tailored to the network-connected equipment to be used in payment transactions.

Suggestions for action points in this sector include the following.

1) Self certification and liability: a requirement for software vendors to certify that their products are secure "by default" when used in the context of internet payment services. The vendor could simply "self-certify" the product, but would be liable in the event of security incidents if the certification turns out to have been erroneous.

2) "Patch" management: a requirement for vendors to adopt an adequate "vulnerability disclosure model" and an efficient policy on developing and issuing patches for disclosed vulnerabilities. This could also be promoted through introducing vendor liability in the event of a slow reaction.

3) Security breach notification: a requirement that actors managing sensitive data promptly inform users in the event of security incidents compromising their personal data. This would help users who are victims of fraud to find out who is responsible for the disclosure.

4) Infected machine policies: defining specific security rules related to infected network-connected machines. Infected machines could, for example, host a "phishing" website[21] or be part of a botnet,[22] thus polluting the digital environment. Security rules in this sector could require internet service providers[23] to disconnect compromised machines.

LEGISLATION ON CYBERCRIME

Measures aimed at reducing vulnerabilities in IT products and payment services, together with specific supervision and oversight, should be complemented by appropriate legislation to discourage fraudulent attacks (comprising provisions on sanctions and penalties, wide investigative powers, international cooperation, etc.). The deterrent effect of criminal penalties for payment fraud offences is a key element in fighting against payment fraud.

However, the cross-border nature of the internet means that identifying the applicable regulations and competent jurisdictions in the event of a security breach is not a straightforward matter. There are often significant cross-border components in payment fraud while law enforcement authorities are limited by traditional territorial constraints: card data is generally obtained in one country but exploited in another. It should be underlined that attacks against critical infrastructures and the provision of payment services can be carried out by people based in countries with no cybercrime regulation, implying a serious problem of jurisdiction. For the time being, only some countries consider cyber fraud and illegally accessing sensitive data to be criminal offences under domestic law. Cyber fraud is a global offence which needs a global and harmonised response.

The Council of Europe's "Convention on Cybercrime", which entered into force in 2004, is to date the only binding international instrument covering this field. The main aim of the Convention, set out in the preamble, is to "pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international cooperation".[24] However, for the time being, only 32 countries have ratified the Convention.

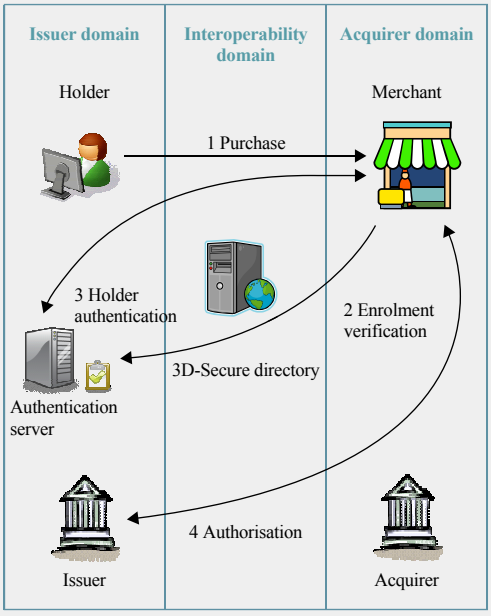
21 Phishing e-mails trick users into revealing sensitive data via "fake" websites imitating genuine companies.
22 The term "botnet" describes a network of computers that have been infected by malicious software (computer virus).
23 Organisations that provide access to the internet.
24 See the section on cybercrime on the Council of Europe's website at http://www.coe.int

ANNEX 3: ARCHITECTURE FOR CARDHOLDER AUTHENTICATION VIA THE INTERNET

With regard to card transactions via the internet, some card payment schemes have introduced architectures enabling e-merchants to request the issuer to authenticate the cardholder. One example of this kind of solution is "3-D Secure".[25] Following a request by the e-merchant's server, the cardholder's PSP is contacted in order to authenticate the cardholder,[26] approve the terms of the transaction, notably the amount, and prepare a record or certificate as evidence of the transaction. This authentication solution provides additional security, and use of the service results in a shift of liability in the event of fraud. Indeed, when an e-merchant is the victim of a fraudulent payment, and the transaction was processed using 3-D Secure, it is the issuer rather than the e-merchant that is liable.

The success of 3-D Secure will depend on its widespread introduction by card payment schemes and the related liability shift attached to it.

Overview of 3-D Secure



The steps of a "3-D Secure" enabled card payment transaction are as follows.

1) The e-merchant receives via its website a purchase request from a customer. After choosing to pay by card, the customer is asked to enter his card data (number, expiry date and card verification code (CVx2)[27]).

2) Where the e-merchant is 3-D Secure compliant – i.e. the issuer provides a solution for additional customer authentication – the customer will be directed, via the 3-D Secure Directory, to the issuer's authentication server. Note that the customer must have been enrolled by the issuer (enrolment verification) and informed about the authentication procedure prior to the first authenticated payment transaction.

3) A separate window will be opened where the customer is asked to enter his password, which is subsequently verified by the issuer. The level of security offered by the password depends on the nature of the password required by the service, i.e. static or dynamic. Static passwords provide weak authentication.

4) Once the cardholder has been authenticated, the e-merchant is informed via its acquirer. The e-merchant then sends the issuer an authorisation request, incorporating the digital proof of successful cardholder authentication, after which the issuer finally authorises the transaction. Once the e-merchant has received the final authorisation message, the transaction can be finalised.

25 3D-Secure is an industry communication protocol linking the e-merchant, the acquiring PSP and the issuing PSP. It is offered to clients under the name "Verified by Visa". Services based on the protocol are offered by MasterCard under the name "MasterCard SecureCode" and by JCB International as "J/Secure".

26 The authentication method – weak or strong – is chosen by the issuer PSP.

27 The card verification code is not always requested.

ANNEX 4: 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 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
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 Naţăionalã a României
SI	Banka Slovenije
SK	Národná banka Slovenska
FI	Suomen Pankki – Finlands Bank Finanssivalvonta
SE	Sveriges Riksbank Finansinspektionen
UK	Bank of England 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