EBA/CP/2014/31

20 October2014

Consultation Paper

On the implementation of draft EBA Guidelines on the security of internet payments prior to the transposition of the revised Payment Services Directive (PSD2)

Contents

Responding to this Consultation 3

Executive Summary 4

Background and rationale 5

Background 5

Rationale 8

Structure of the draft guidelines 10

Draft Guidelines on the security of internet payments 11

Status of these Guidelines 11

Reporting Requirements 11

Title I – Scope and definitions 12

Title II – Draft guidelines on the security of internet payments 15

Consultation Question 27

Accompanying documents 28

Annex 1: Best practice examples 28

Annex 2: List of authorities participating in the work of the SecuRe Pay forum 30

Annex 3: Cost-Benefit Analysis / Impact Assessment 32

Responding to this Consultation

The EBA invites comments on all proposals put forward in this paper and in particular on the specific question stated in the paper.

Comments are most helpful if they:

- respond to the question stated;
- indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence to support the views expressed/ rationale proposed; and
- describe any alternative regulatory choices the EBA should consider.

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by **14.11.2014.** Please note that comments submitted after this deadline, or submitted via other means may not be processed.

Publication of responses

Please clearly indicate in the consultation form if you wish your comments to be disclosed or to be treated as confidential. A confidential response may be requested from us in accordance with the EBA's rules on public access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by the EBA's Board of Appeal and the European Ombudsman.

Data protection

The protection of individuals with regard to the processing of personal data by the EBA is based on Regulation (EC) N° 45/2001 of the European Parliament and of the Council of 18 December 2000 as implemented by the EBA in its implementing rules adopted by its Management Board. Further information on data protection can be found under the Legal notice section of the EBA website.

Executive Summary

On 31 January 2013, the European Central Bank (ECB) released final recommendations for the security of internet payments. The publication followed a two-month public consultation carried out in 2012, and represented the first output of SecuRe Pay forum. SecuRe Pay was set up in 2011 as a voluntary cooperative initiative between relevant authorities from the European Economic Area (EEA), including national supervisors of payment service providers and overseers. Its objective is to facilitate common knowledge and understanding of issues related to the security of electronic retail payment services and instruments and to issue recommendations.

During a stock-take in summer 2014 of the progress of the implementation of the recommendations, the SecuRe Pay forum concluded that the implementation would benefit from a more solid legal basis, to ensure a consistent implementation by financial institutions across all Member States, and to provide confidence to financial institutions that the required investments and system changes are not carried out in vain.

The EBA, as a member of the SecurePay forum, agreed to develop EBA guidelines that are based on the SecuRe Pay recommendations, with minor deviations as explained in the background section of the paper. Using the existing Payment Services Directive (PSD) as a legal basis, and in accordance with Article 16 of the EBA regulation, competent authorities and financial institutions must make every effort to comply with EBA guidelines.

The entry of force date of the draft guidelines will be 1 August 2015, which constitutes an extension by six months compared to the implementation date that had been set for the SecuRe Pay recommendations. The EBA is consulting in October/November 2014 and will be publishing the final guidelines including the feedback statement soon thereafter.

At the time of publishing this consultation paper, the negotiations on the revision of the existing PSD were ongoing. One of the more recent developments in the negotiations indicate that the final PSD2 text may potentially include provisions that require stronger security standards than the EBA guidelines, which would come into force with the transposition date of the PSD2 or later. If this scenario were to materialise, the EBA would like to hear respondents' views on the question whether the final EBA guidelines under PSD 1 should

- enter into force, as consulted, on 1 August 2015 with the substance set out in this consultation paper, which would mean that they would apply during a transitional period until stronger requirements enter into force at a later date under PSD 2 (i.e. a two-step approach); or
- should anticipate these stronger PSD 2 requirements and, once the PSD2 negotiations have concluded, include them in the final guidelines under PSD 1 that enter into force on 1 August 2015, the substance of which would then continue to apply under PSD 2 (i.e. a one-step approach).

Background and rationale

This section summarises the work that has been carried out and that has led to these proposed guidelines; compares the proposed guidelines with the recommendations of the European Forum on the Security of Retail Payments (SecuRe Pay); elucidates the interaction between the proposed guidelines and the ongoing PSD2 negotiations and the consultation question that results from it regarding the implementation; and sets out the rationale of the substance as well as the structure of the guidelines

Background

The work that has been carried out so far

On 31 January 2013, the European Central Bank (ECB) released final recommendations for the security of internet payments (the Report).[1] The publication followed a two-month public consultation carried out in 2012, and represented the first output of SecuRe Pay.

SecuRe Pay was set up in 2011 as a voluntary cooperative initiative between relevant authorities from the European Economic Area (EEA), including national supervisors of payment service providers and overseers. Its objective is to facilitate common knowledge and understanding of issues related to the security of electronic retail payment services and instruments and, where necessary, to issue recommendations.

Comments from 17 European Union countries had been received during the SecuRe Pay public consultation. The resultant harmonised, minimum security recommendations constituted a set of measures in the fight against payment fraud and aimed to increase consumer trust in internet payment services. The main recommendations included:

- protecting the initiation of internet payments, as well as access to sensitive payment data, by strong customer authentication;
- limiting 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;
- establishing transaction monitoring mechanisms designed to prevent, detect and block fraudulent payment transactions;
- implementing multiple layers of security defences in order to mitigate identified risks;
- providing assistance and guidance to customers about best online security practices, set up alerts and provide tools to help customers monitor transactions.

[1] see http://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html

The recommendations were considered as common minimum requirements for internet payment services and the members of SecuRe Pay agreed to implement the recommendations within their jurisdictions, where possible, on the basis of the existing powers under EU or national law by 1 February 2015.[2]

During a stock-take in summer 2014 of the progress of the implementation of the recommendations, the SecuRe Pay forum concluded that, while the majority of national authorities and financial institutions are progressing as planned, the implementation would benefit from a more solid legal basis, to ensure a consistent implementation by financial institutions across all 28 Member States of the European Union, and to provide confidence to financial institutions that the required investments and system changes are not carried out in vain.

The SecuRe Pay forum brought this issue to the attention of the EBA as one the forum members. The EBA agreed to develop EBA guidelines that are based on the SecuRe Pay recommendations, pursuant to Article 16 of Regulation (EU) No 1093/2010 (the EBA Regulation),[3] and are aimed at establishing a framework for PSPs with regards to the security of internet payments. In accordance with Article 16(3) of the EBA regulation, competent authorities and financial institutions must make every effort to comply with EBA guidelines by the date of entry into force provided.

The entry of force date of the draft guidelines will be 1 August 2015, which constitutes an extension by six months compared to the implementation date that had been set originally for the SecuRe Pay recommendations. The extension is aimed at providing some competent authorities and financial institutions with extra time to comply with the EBA guidelines but is also driven by the EBA being required by its regulation publicly to consult on its draft guidelines, to assess the responses, and to develop a feedback statement and the final guidelines after consultation.

Competent authorities and financial institutions that are already on track with implementing the SecuRe Pay recommendations to the original date of 1 February 2015 are not affected by the extension and should continue with their plans.

The EBA is consulting in September/October 2014 and would publish the final guidelines including the feedback statement soon thereafter. From the publication of the final guidelines onwards, competent authorities will have to notify the EBA within two months as to whether they comply or intend to comply, or otherwise with reasons for non-compliance. Competent authorities, as well as financial institutions, will have to comply with the guidelines by the entry into force date of 1 August 2015.

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

[3] See http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02010R1093-20131030&from=EN

Comparison between the draft EBA guidelines and the SecuRe Pay recommendations

The draft EBA guidelines stated in this document are identical to the Recommendations and the Key Considerations of the SecuRe Pay Report, with the following substantive exceptions:

i. Recommendation 6.4 of the SecuRe Pay report, which requires payment service providers (PSPs) to ensure that customers are provided with instructions explaining their responsibilities regarding the secure use of payment services, has been incorporated in the draft EBA guidelines only as a best practice, because in the EBA's view the provisions in PSD1 do not allow for such a requirement to be imposed.

ii. References to payment schemes, their Governance Authorities (GAs), and the oversight thereof have not been incorporated in the draft EBA guidelines, as payment schemes are not covered by PSD1. However, the validity of the recommendations in the SecuRe Pay report remain intact in this regard since these aspects fall under the responsibility of Central Banks with an oversight function on payment instruments, which should assess compliance with regards to the security of internet payments[4].

In addition, the following layout changes have been made:

iii. All Best Practices of the Report – which represented a model application of the SecurRe Pay Recommendations, but not a requirement – have been moved to Annex 1 of the draft EBA guidelines.

iv. The content of the 'glossary' of the Report has been moved to the 'definitions' section in the draft EBA guidelines; the 'general part' has been moved to the 'background', and the 'guiding principles' are now stated in the 'rationale' section.

Interaction between the draft EBA guidelines and PSD 2, and consultation question

As explained in more detail in the scope section of the draft guidelines further below, the draft EBA guidelines are based on the provisions in PSD1. They were developed keeping in mind the European Commission's legislative proposal, published on 24 July 2013, for a revision of PSD1,[5] as well as the changes subsequently proposed by the revised texts produced by the Council of the EU and the European Parliament, during the legislative procedure.

At the time of publishing the consultation paper on the draft EBA guidelines in October 2014, the PSD2 negotiations were still ongoing. One of the more recent developments in the negotiations

[4] For example, on the side of the Eurosystem, harmonised implementation of the recommendations is ensured through their approval in January 2013 by the Governing Council and their integration into the Eurosystem oversight framework.

[5] See http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52013PC0547

indicate that the final PSD2 text may potentially include provisions that require stronger security standards than the EBA guidelines, which would come into force with the transposition date of the PSD2 or later. In particular, payment service providers may be required to apply an enhanced version of strong customer authentication, so called "strong transaction authorisation", for all types of electronic payment transactions. Strong transaction authorisation links authentication data to payment-specific amount and payee and is already one of the 70+ provisions in the SecuRe Pay Report and listed in the draft EBA guidelines as a best practice example (7.3 in the Annex).

If the scenario were to materialise that the final text of the PSD2 includes such stronger requirements, the EBA would like to hear respondents' views on the question whether the final EBA guidelines under PSD 1 should

a) enter into force, as consulted, on 1 August 2015 with the substance set out in this consultation paper, which means they would apply during a transitional period until stronger requirements enter into force at a later date under PSD 2 (i.e. a two-step approach); or

b) anticipate these stronger PSD 2 requirements and include them in the final guidelines under PSD 1 that enter into force on 1 August 2015, the substance of which would then continue to apply under PSD 2 (i.e. a one-step approach).

Either option would result in the guidelines coming into force on 1 August 2015, albeit with a different respective substance, depending on the option eventually chosen by the EBA. During November and December 2014, the EBA will review the responses to this consultation question; monitor the development of the PSD2 negotiations; amend the guidelines in light of both; and then publish the *final* EBA guidelines as soon as possible thereafter.

Rationale

Akin to the rationale of the SecuRe Pay recommendations, EBA guidelines for the security of internet payments are expected to contribute to fighting payment fraud and enhancing consumer trust in internet payments. The draft guidelines 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 mechanisms. 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. 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.

[6] Bank for International Settlements (2003), Risk Management Principles for Electronic Banking, July

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 these draft Guidelines, 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 EBA'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[7] to use such services safely and efficiently.

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

These draft guidelines do not attempt to set specific security or technical solutions. Nor do they 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 guidelines, the authorities may take into account compliance with the relevant international standards.

[7] Customers include both consumers and companies to which a payment service is provided.

Structure of the draft guidelines

The draft guidelines are organised into the following three categories:

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. Guidelines 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.

Specific control and security measures for internet payments. Guidelines 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.

Customer awareness, education and communication. Guidelines 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 documents accompanying the above guidelines comprise some best practice examples that PSPs and the relevant market participants are encouraged, but not required, to adopt; a list of authorities participating in the work of the European Forum on the Security of Retail Payments; as well as an impact assessment.

Draft Guidelines on the security of internet payments

Status of these Guidelines

This document contains draft guidelines issued pursuant to Article 16 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (‘*the EBA Regulation*’). In accordance with Article 16(3) of the EBA Regulation, competent authorities and financial institutions must make every effort to comply with the draft guidelines by the date of entry into force provided for.

Guidelines set out the EBA’s view of appropriate supervisory practices within the European System of Financial Supervision or of how Union law should be applied in a particular area. The EBA therefore expects all competent authorities and financial institutions to whom guidelines are addressed to comply with guidelines. Competent authorities to whom guidelines apply should comply by incorporating them into their supervisory practices as appropriate (e.g. by amending their legal framework or their supervisory processes), including where guidelines are directed primarily at financial institutions.

Reporting Requirements

According to Article 16(3) of the EBA Regulation, competent authorities must notify the EBA as to whether they comply or intend to comply with these guidelines, or otherwise with reasons for non-compliance, by dd.mm.yyyy [here: publication date of final GL, plus 2 months]. In the absence of any notification by this deadline, competent authorities will be considered by the EBA to be non-compliant. Notifications should be sent by submitting the form provided at Section 5 to compliance@eba.europa.eu with the reference ‘EBA/GL/201x/xx’. Notifications should be submitted by persons with appropriate authority to report compliance on behalf of their competent authorities.

Notifications will be published on the EBA website, in line with Article 16(3).

Competent authorities may decide to impose additional compliance reporting requirements on the financial institutions that they supervise in their respective jurisdictions.

Title I – Scope and definitions

Scope

1. These draft guidelines establish a set of minimum requirements in the field of the security of internet payments. The guidelines build on the rules of Directive 2007/64/EC[8] ('Payment Services Directive', PSD1) concerning information requirements for payment services and obligations of payment services providers (PSPs) in relation to the provision of payment services. Furthermore, Article 10(4) of the Directive requires payment institutions to have in place robust governance arrangements and adequate internal control mechanisms.

2. The guidelines apply to the provision of payment services offered through the internet by payment services providers (PSPs) as defined in Article 1 of the Directive.

3. The guidelines are addressed to financial institutions as defined in Article 4(1) of Regulation (EU) No 1093/2010 and to competent authorities as defined in Article 4(2) of Regulation (EU) No 1093/2010. Competent authorities in the 28 Member States of the European Union should ensure the application of these guidelines by PSPs as defined in Article 1 of the Payment Services Directive under their supervision.

4. These guidelines do not affect the validity of the European Central Bank "Recommendations for the security of internet payments" (the 'Report').[9] The Report in particular continues to represent the document against which oversight authorities on payment systems and payment schemes should assess compliance with regards to the security of internet payments.

5. The guidelines constitute minimum expectations. They are without prejudice to the responsibility of PSPs 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.

6. The purpose of the guidelines are 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;

[8] 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,

[9] http://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html

- [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.

7. These guidelines, in addition to the requirements set out as follows, also provide examples of best practices (in Annex 1), which PSPs are encouraged, but not required, to follow.

8. Where the provision of payment services and instruments is offered through a payment scheme (e.g. card payment schemes, credit transfer schemes, direct debit schemes, etc.), competent authorities and relevant central bank with an oversight function on payment instruments should liaise to ensure a consistent application of the guidelines by the actors responsible for the functioning of the scheme.

9. Payment integrators [10] 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 or PSPs. In the latter case, the payment integrators should be contractually required to comply with the guidelines.

10. Excluded from the scope of the guidelines are:

- 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;

- 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.

Definitions

11. For the purpose of these guidelines, and in addition to the definitions provided in PSD1, the following definitions apply:

[10] Payment integrators provide the payee (i.e. the e-merchant) with a standardised interface to payment initiation services provided by PSPs.

- *Authentication* means a procedure that allows the PSP to verify a customer's identity.

- *Authorisation* means 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* mean 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* means 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* means 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* means 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* means solutions that allow a customer to register data relating to one or more payment instruments in order to make payments with several e-merchants.

Title II – Draft guidelines on the security of internet payments

General Control and Security Environment

Governance

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

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

1.2 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.

Risk assessment

PSPs 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. PSPs, through their risk management function, should carry out and document detailed risk assessments for internet payments and related services. PSPs 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 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 Guideline 3).

2.2. On this basis, 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 security incidents and fraud, as well as potential disruptive effects.

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

[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.

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

Incident monitoring and reporting

PSPs should ensure the consistent and integrated 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 payment security incidents, the competent authorities.

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

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

3.4 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.

Risk control and mitigation

PSPs 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 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 privilege” principle as the basis for a sound identity and access management.[13]

[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.

4.2 PSPs should have appropriate security solutions in place to protect networks, websites, servers and communication links against abuse or attacks. PSPs 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.

4.3 PSPs 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 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 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 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 Whenever PSPs outsource functions related to the security of the internet payment services, the contract should include provisions requiring compliance with the principles and guidelines set out in this report.

4.8 PSPs offering acquiring services should contractually require e-merchants handling (i.e. storing, processing or transmitting) sensitive payment data to implement security measures

[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

in their IT infrastructure, in line with guidelines 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.

Traceability

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

5.1 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.

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

5.3 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.

Specific control and security measures for internet payments

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 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]

[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.

6.2 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;

- 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 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.

Strong customer authentication

The initiation of internet payments, as well as access to sensitive payment data, should be protected by strong customer authentication. PSPs should have a strong customer authentication procedure in line with the definition provided in this report.

7.1 [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:

[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.

[20] See Article 55 of the Payment Services Directive on limits of the use of the payment instrument.

- 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 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 [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.

7.4 [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 [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 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 [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 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.

[21] See the definition of low-value payment instruments in Articles 34(1) and 53(1) of the Payment Services Directive.

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

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

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 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 [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.

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.

[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 Guideline 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).

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

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

[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.

10.4 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 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.

Protection of sensitive payment data

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

11.1 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 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 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.

[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).

Customer awareness, education, and communication

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 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 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 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 PSPs 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;

[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.

- 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.

12.5 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).

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 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.

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 [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 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,

[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.

sensitive payment data should not be included in such communications or, if included, they should be masked.

Consultation Question

Question: Do you prefer for the EBA guidelines

a) to enter into force, as consulted, on 1 August 2015 with the substance set out in this consultation paper, which means they would apply during a transitional period until stronger requirements enter into force at a later date under PSD 2 (i.e. a two-step approach); or

b) to anticipate these stronger PSD 2 requirements and include them in the final guidelines under PSD 1 that enter into force on 1 August 2015, the substance of which would then continue to apply under PSD 2 (i.e. a one-step approach).

Accompanying documents

Annex 1: Best practice examples

In addition to the requirements set out in the guidelines above, the report describes some best practices which PSPs and the relevant market participants are encouraged, but not required, to adopt. The numbering of the best practices mirrors the numbering of the guidelines to which they apply.

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

4.1 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).

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

6.1 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.

6.2 PSPs could 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.

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

7.2 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 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.

11.1 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.

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

13.1 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 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 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.

Annex 2: List of authorities participating in the work of the SecuRe Pay forum

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 et de Résolution
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
HR	Hrvatska narodna banka
HU	Magyar Nemzeti Bank
	Pénzügyi Szervezetek Állami Felügyelete (since then merged with Magyar Nemzeti Bank)
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 Naţională 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

Annex 3: Cost-Benefit Analysis / Impact Assessment

Introduction

A payment system consists of a set of instruments, banking procedures and, typically, interbank funds transfer systems that ensure the circulation of money.[32] Efficient payment systems reduce the cost of exchanging goods and services, and are indispensable to the functioning of the interbank, money, and capital markets, and are therefore core elements of the financial infrastructure.

Weak payment systems can be an impediment to the stability and developmental capacity of an economy, as they can result in an inefficient use of financial resources, inequitable risk-sharing among market participants, actual losses, and a reduction of confidence in the financial system and in the very use of money.[33] The technical efficiency of payment systems is therefore of concern to regulators.

Problem definition

Inadequate security is an important impediment to the efficiency of payment systems because, as the number and value of payment transactions has increased over time, the number of security incidents has increased as well.

The sophistication of security breaches has also developed, and continuously do so. Cybercriminals are no longer focused solely on attacks against users to gain access to personal information but increasing attention is applied to the service providers.[34] The increased number of security incidents causes problems for payment institutions, consumers, merchants, and regulators alike.

Consumers are affected because inadequate security diminishes their overall confidence in the online retail and banking sector. Such lack of confidence has a knock-on impact on the confidence in the security of e-commerce and the functioning of merchants and other commercial entities more generally.

Payment systems, in turn, are impacted because the perception of failing payment security affects the way in which consumers make payment choices. As consumer confidence in specific payment instruments is undermined, they may switch to alternative but less efficient forms of payments, compromising the smooth operation of payment systems, decreasing efficiency throughout the economy, and undermining firms' efforts to realise cost efficiencies.

[32] See ECB Blue book at https://www.ecb.europa.eu/paym/intro/book/html/index.en.html

[33] Biago Bossone and Massimo Cirasino, "The Oversight of the Payment Systems: A Framework for the Development and Governance of Payment Systems in Emerging Economies", The World Bank, July 2001, p.7

[34] Europol (2013), *SOCTA 2013 – EU Serious and Organised Crime Threat Assessment*, p. 28, see https://www.europol.europa.eu/sites/default/files/publications/socta2013.pdf

Objective

The draft guidelines constitute harmonised, minimum security recommendations in the fight against payment fraud and aim to increase consumer trust in internet payment services. The core recommendation is that the initiation of internet payments as well as access to sensitive payment data should be protected by strong customer authentication to ensure that it is a rightful user, and not a fraudster, initiating a payment. This will be achieved through the following provisions:

- to protect the initiation of internet payments, as well as access to sensitive payment data, by strong customer authentication;
- to 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;
- to establish transaction monitoring mechanisms designed to prevent, detect and block fraudulent payment transactions;
- to implement multiple layers of security defences in order to mitigate identified risks;
- to provide assistance and guidance to customers about best online security practices, set up alerts and provide tools to help customers monitor transactions;
- to have a formal security policy for internet payment, a thorough assessment of risks, incident monitoring and reporting;
- to implement appropriate tracing of transactions and e-mandates;
- to implement a sound KYC and provide essential information to the customer;
- to ensure a secure enrolment for and provision of authentications tools and or software delivered to the customer;

Baseline scenario

A survey of consumers in the EU has shown that 10% of internet users across the EU have experienced online fraud, and 6% have experienced identity theft. 12% have not been able to access online services because of cyber-attacks, and 12% have had a social media or email account hacked. 7% have been the victim of credit card or banking fraud online.[35]

At present, 28% of internet users across the EU are not confident about their ability to use the internet for services like online banking or buying things online. When using the internet for online banking or shopping, the two most common concerns are about someone taking or misusing personal data (mentioned by 37% of internet users in the EU) and security of online payments (35%).[36]

The draft guidelines aim markedly to reduce these figures after implementation.

[35] EU Commission (2013), *Special Eurobarometer 404 – Cyber security*, p. 52, at http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf

[36] EU Commission (2013), *Special Eurobarometer 404 – Cyber security*, p. 4,