

COMMISSION de SURVEILLANCE du SECTEUR FINANCIER

En cas de divergence entre les textes français et anglais, le texte anglais prévaut

Luxembourg, le 9 février 2015

À tous les prestataires de services de paiement tels que définis à l'article 1 (37) de la loi du 10 novembre 2009 relative aux services de paiement¹

CIRCULAIRE CSSF 15/603

Concerne : Sécurité des paiements sur internet

Mesdames, Messieurs,

1. L'Autorité bancaire européenne (ABE-EBA) a publié ses Orientations sur la sécurité des paiements sur internet (EBA/GL/2014/12) en date du 19 décembre 2014. Ces Orientations établissent les exigences minimales en matière de sécurité que les prestataires de services de paiement (PSP) de l'UE sont appelés à mettre en œuvre au plus tard le 1^{er} août 2015. Soucieuse de l'augmentation des fraudes relatives aux paiements sur internet, l'EBA a décidé qu'il était nécessaire d'instaurer un cadre plus sûr pour les paiements sur internet à travers l'UE.
2. Les Orientations s'appliquent à la fourniture de services de paiement sur internet tels que spécifiés dans les Orientations sous le « Titre I – Champ d'application et définitions ».
3. Les Orientations sont basées sur les recommandations qui ont été élaborées et publiées par le *European Forum on the Security of Retail Payments (SecuRe Pay)* (Forum européen sur la sécurité des paiements de détail) en janvier 2013. Créé en 2011 à l'initiative de la Banque centrale européenne (BCE), le SecuRe Pay est une plateforme de coopération volontaire entre les autorités compétentes pour la

¹ Loi du 10 novembre 2009 relative aux services de paiement, à l'activité d'établissement de monnaie électronique et au caractère définitif du règlement dans les systèmes de paiement et les systèmes de règlement des opérations sur titres.

supervision des prestataires de services de paiement et les autorités compétentes pour la surveillance des systèmes de paiement et des schémas/instruments de paiement au sein de l'UE/EEE. Cette plateforme vise à faciliter une connaissance et une compréhension commune entre ces autorités en matière de sécurité des services et instruments de paiement électronique.

4. La conversion des Recommandations SecuRe Pay en Orientations de l'EBA vise à fournir une base légale solide pour la mise en œuvre cohérente des exigences à travers les 28 États membres de l'UE.
5. La présente circulaire met en œuvre les Orientations de l'EBA en droit luxembourgeois. Conformément à l'article 16 (3) du Règlement de l'EBA², les autorités compétentes et les établissements financiers mettent tout en œuvre pour respecter ces Orientations, à compter de la date d'application indiquée dans les Orientations, à savoir le 1^{er} août 2015.
6. Les Orientations sont annexées à la présente circulaire. Elles sont également disponibles sur le site de l'EBA sous :

<https://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-the-security-of-internet-payments>
7. Les prestataires de services de paiement, tels que définis à l'article 1 (37) de la loi du 10 novembre 2009 relative aux services de paiement, doivent appliquer les Orientations de l'EBA à partir du 1^{er} août 2015.

Veillez recevoir, Mesdames, Messieurs, l'assurance de nos sentiments très distingués.

COMMISSION de SURVEILLANCE du SECTEUR FINANCIER

Claude SIMON
Directeur

Andrée BILLON
Directeur

Simone DELCOURT
Directeur

Jean GUILL
Directeur général

Annexe : Orientations de l'EBA sur la sécurité des paiements sur internet

² Règlement (UE) n° 1093/2010 du Parlement européen et du Conseil du 24 novembre 2010 instituant une Autorité européenne de surveillance (Autorité bancaire européenne), modifiant la décision n° 716/2009/CE et abrogeant la décision 2009/78/CE de la Commission (le « Règlement de l'EBA »).

EBA/GL/2014/12

19 December 2014

Final guidelines

on the security of internet payments

Contents

1. Executive summary	3
2. Background and rationale	4
Background	4
Rationale	5
3. Guidelines on the security of internet payments	8
Status of these guidelines	8
Reporting requirements	8
Title I – Scope and definitions	9
Scope	9
Definitions	11
Title II – Guidelines on the security of internet payments	13
General control and security environment	13
Specific control and security measures for internet payments	16
Customer awareness, education, and communication	22
Annex 1: Best practice examples	25
General control and security environment	25
Specific control and security measures for internet payments	25
4. Accompanying documents	27
4.1 Cost-benefit analysis/impact assessment	27
Introduction	27
Problem definition	27
Objective	28
Baseline scenario	28
4.2 Views of the Banking Stakeholder Group (BSG)	30
4.2.1 Summary of the BSG’s opinion	30
4.2.2 EBA feedback on the BSG’s opinion	30
4.3 Feedback on the public consultation	31
Summary of key issues and the EBA’s response	31
5. Confirmation of compliance with guidelines and recommendations	42

1. Executive summary

On 20 October 2014, the EBA published a Consultation Paper (CP) on draft guidelines for the security of internet payments. The guidelines were based on the recommendations that had been developed and published by the European Forum on the Security of Retail Payments (SecuRe Pay) in January 2013. The conversion into EBA guidelines is intended to provide a solid legal basis for the consistent implementation of the requirements across the 28 EU Member States.

Given that the negotiations on the revision of the existing Payment Services Directive (PSD) were ongoing, and that SecuRe Pay had already consulted on the substance of the guidelines, the CP sought input solely from stakeholders with regard to how the potentially higher security standards required by the forthcoming PSD 2 as of 2017/18 should be catered for by the EBA: through a one-step approach in which the EBA anticipates and ‘frontloads’ future requirements from the implementation date of the guidelines on 1 August 2015 onwards, or a two-step approach that will see the guidelines implemented as consulted on 1 August 2015, with potentially more stringent requirements necessary under the PSD 2 being implemented at a later stage, as set by the PSD 2.

The EBA received 45 responses to the CP, including a response from the EBA’s Banking Stakeholder Group (BSG). The majority of responses stated that they would be able to agree with the two-step approach, although a significant number of these respondents did so only as a second-best solution, should their first choice — the EBA delaying the issuing of the guidelines until the transposition of the PSD 2 — not come to pass. Two responses expressed a preference for the one-step approach. A large minority of responses were against either option and proposed instead that the EBA should not issue the guidelines at all and instead wait until the transposition of the PSD 2 and its security requirements in 2017/18.

The EBA has assessed the responses and concludes that, due to the continually high levels of fraud observed on internet payments, a delay in the implementation of the guidelines until the transposition of the PSD 2 in 2017/18 is not a plausible option. Furthermore, given the preferences expressed by respondents, the EBA concludes that a one-step approach is not desirable. The EBA is therefore issuing the final guidelines with the substance as consulted, i.e. a conversion of the original SecuRe Pay recommendations, with an implementation date of 1 August 2015, and the implementation of any potentially more stringent requirements under the PSD 2 at a later stage — by the date set in the PSD 2. Finally, in response to some questions asking for clarification, the EBA made a few minor modifications to the guidelines and the surrounding text, in particular deleting two remaining and erroneous references to payment schemes; clarifying the meaning of ‘strong authentication’; confirming the continued relevance of the SecuRe Pay assessment guide; and re-numbering the best practice examples.

2. Background and rationale

Background

1. 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. At the time, the implementation date of the recommendations was set as 1 February 2015.
2. During a stock-take in summer 2014 of the progress of the implementation, 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. To that end, the EBA, as a member of SecurePay, agreed to convert the SecurePay recommendations into EBA guidelines under Article 16 of the EBA Regulation No 1093/2010 of the European Parliament and of the Council of 24 November 2010, with some minor deviations to bring them in line with the existing PSD as a legal basis.
3. On 20 October 2014, the EBA published a CP on draft guidelines for the security of internet payments.¹ The guidelines were based on the recommendations that had been developed and published by the SecuRe Pay forum in January 2013. The conversion into EBA guidelines is intended to provide a solid legal basis for the consistent implementation of the requirements across the 28 EU Member States.
4. Given that the negotiations on the revision of the PSD were ongoing, the CP asked stakeholders for views on how the potentially higher security standards required by the forthcoming PSD 2 as of 2017/18 should be catered for by the EBA. Two options were presented and respondents were asked to express their preference on whether the final EBA guidelines under the PSD should:
 - enter into force, as consulted, on 1 August 2015 with the substance set out in this CP, which would mean that they would apply during a transitional period until stronger requirements enter into force at a later date under the PSD 2 (i.e. a two-step approach); or
 - anticipate these stronger PSD 2 requirements and, once the PSD 2 negotiations have concluded, include them in the final guidelines under the PSD that enter into force on

¹ See <http://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-the-security-of-internet-payments>

1 August 2015, the substance of which would then continue to apply under the PSD 2 (i.e. a one-step approach).

5. The consultation period closed on 14 November 2014. The EBA received 45 responses to the CP, including a response from the EBA's BSG. 38 of these responses gave permission for the EBA to publish them on the EBA website.
6. The majority of responses stated that they would be able to agree with the two-step approach, although a significant number of these respondents did so only as a second-best solution, should their first choice— the EBA delaying the issuing of the guidelines until the transposition of the PSD 2—not come to pass. One of the main reasons stated by respondents was that they did not think the alternative of a one-step approach was feasible, because it would be impossible to anticipate the final conclusions of the on-going PSD 2 debate on the definition of 'strong authentication'. This, so respondents continued, would therefore leave no time for payment service providers to adapt their IT platforms and payment system interfaces.
7. None of the responses that preferred the two-step approach raised an issue with the 1 August 2015 implementation deadline, and some reiterated that they would be ready for the 1 February 2015 deadline that had been set by the original SecuRe Pay recommendations.
8. Two responses expressed a preference for the one-step approach.
9. Finally, a large minority of responses were against either option and proposed instead that the EBA should not issue the guidelines at all and instead wait until the transposition of the PSD 2 and its security requirements in 2017/18. One of the main reasons given in these responses was that this would avoid additional costs for financial institutions before PSD 2 implementation. There were also concerns about an August 2015 implementation deadline.

Rationale

10. The EBA has assessed all of the responses and has arrived at the following conclusions. Firstly, given the high level of fraud observed on internet payments and its increasing trend over recent years², the EBA does not consider the preference of some respondents to delay the implementation of the guidelines until the transposition of the PSD 2 in 2017/18 to be a plausible option. Fraud figures on card internet payments alone, with EUR 794 million in fraud losses in 2012 (up by 21.2% from the previous year) for card-not-present fraud, illustrate that a lack of security is continuing to undermine the confidence of market participants in payment systems and therefore that a timely and consistent regulatory

² See, for example, the third card fraud report of the ECB, which underlines that with €794 million in fraud losses in 2012, card-not-present fraud was not only the largest category in absolute value, but also the one with the highest growth (up 21.2% from 2011) (<http://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201402en.pdf>)

response is required. The EBA is therefore publishing these final guidelines, with an implementation date of 1 August 2015, as consulted.

11. Secondly, given that a significant majority of the other respondents expressed a preference for a two-step approach, the EBA concludes that a one-step approach is not desirable. The EBA is therefore issuing the final guidelines with the substance as consulted, i.e. a conversion of the original SecuRe Pay recommendations. The implementation of any potentially more stringent requirements necessary under the PSD 2 will occur at a later stage, by the date set in the PSD 2.
12. Finally, some responses asked for explanations on particular aspects of the guidelines. By way of a response, the EBA is providing the following clarifications:
 - A few responses challenged the definition of 'strong authentication' in the CP, asking for it to be aligned with the definition in the PSD 2. The EBA is of the view that the working definition of strong authentication used in the guidelines was already discussed during the SecuRe Pay consultation, incorporates well-known security concepts and is not intended to anticipate or second guess the future PSD 2 regulation. Any potential legal definition of the concept in the PSD 2 would replace the working definition used here, as of the transposition date of the PSD 2 onwards. As 'strong customer authentication' was not defined in the CP on the draft guidelines and only referred to in the background and rationale sections, the final guidelines now define this concept in the section on 'Definitions'.
 - Some respondents remarked that guidelines 7.6 and 10.2 should be deleted since they address payment schemes that are not covered by the PSD 1. The EBA confirms that these two guidelines had erroneously been retained in the CP and has corrected the final guidelines accordingly.
 - Some respondents remarked that the CP contained two misleading references to the 'report' of the original SecuRe Pay recommendations. The EBA agrees with this view and has removed these references in the final guidelines.
 - Other responses noted that the numbering in the annex was confusing. The EBA agrees and has changed the numbering as a result.
 - Several respondents also asked for clarification regarding the status of the 'Assessment guide for the security of internet payments', which had been published by SecuRe Pay in February 2014, once the EBA publishes the final guidelines. To aid the consistent implementation of its recommendations, SecuRe Pay had published the assessment guide for staff in supervisory and oversight authorities as a non-prescriptive tool to help them assess firms' compliance with the recommendations. The EBA encourages competent authorities to continue using the guide for the intended purpose.

13. Finally, some members of the EBA's BSG questioned the effectiveness of the guidelines as a basis for EU-wide implementation of stringent payment security standards and suggested the implementation of an effective monitoring mechanism as a part of these guidelines. The EBA sees merit in this view and believes that the assessment guide is one means of ensuring consistent implementation.

3. Guidelines on the security of internet payments

Status of these guidelines

This document contains 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 guidelines.

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 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, within two months of the translations of the final guidelines being published. 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/2014/12'. 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).

Title I – Scope and definitions

Scope

1. These 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/EC³ ('Payment Services Directive', PSD) 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 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 PSD under their supervision.
4. In addition, competent authorities may decide to require PSPs to report to the competent authority that they are complying with the guidelines.
5. These guidelines do not affect the validity of the European Central Bank 'Recommendations for the security of internet payments' (the 'Report').⁴ The Report in particular continues to represent the document against which central banks in their oversight function for payment systems and instruments should assess compliance with regards to the security of internet payments.
6. 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.
7. The purpose of the guidelines are to define common minimum requirements for the internet payment services listed below, irrespective of the access device used:

³ Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, OJ L 319, 05.12.2007,

⁴ http://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html

- [cards] the execution of card payments on the internet, including virtual card payments, as well as the registration of card payment data for use in 'wallet solutions';
 - [credit transfers] the execution of credit transfers (CTs) on the internet;
 - [e-mandate] the issuance and amendment of direct debit electronic mandates;
 - [e-money] transfers of electronic money between two e-money accounts via the internet.
8. Where the guidelines indicate an outcome, the outcome may be achieved through different means. 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.
9. 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.
10. Payment integrators⁵ 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.
11. 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;

⁵ Payment integrators provide the payee (i.e. the e-merchant) with a standardised interface to payment initiation services provided by PSPs.

- 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

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

- *Authentication* means a procedure that allows the PSP to verify a customer's identity.
- *Strong customer authentication* is, for the purpose of these guidelines, 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.
- *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 possession of a 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 – Guidelines on the security of internet payments

General control and security environment

Governance

1. 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

2. 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 side⁶ and the side of their customers,⁷ 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.

⁶ Such as the susceptibility of the system to payment session hijacking, SQL injection, cross-site scripting, buffer overflows, etc.

⁷ Such as risks associated with using multimedia applications, browser plug-ins, frames, external links, etc.

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

3. 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

4. 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.⁸

- 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,⁹ developing and maintaining internet payment services, PSPs should ensure that data minimisation¹⁰ 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.

⁸ '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, p. 388.

⁹ Privacy by design.

¹⁰ Data minimisation refers to the policy of gathering the least amount of personal information necessary to perform a given function.

- 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 these guidelines.
- 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 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

5. 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

6. Customers should be properly identified in line with the European anti-money laundering legislation¹¹ 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.

¹¹ 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.

- 6.1 PSPs should ensure that the customer has undergone the customer due diligence procedures, and has provided adequate identity documents¹² and related information before being granted access to the internet payment services.¹³
- 6.2 PSPs should ensure that the prior information¹⁴ 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 instrument¹⁵ 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 PSD.

¹² For example, passport, national identity card or advanced electronic signature.

¹³ 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.

¹⁴ This information complements Article 42 of the PSD 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.

¹⁵ See Article 55 of the PSD on limits of the use of the payment instrument.

Strong customer authentication

7. 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 these guidelines .
- 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:
- 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 PSD.¹⁶
- 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 PSD.
- 7.6 [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.

¹⁶ See the definition of low-value payment instruments in Articles 34(1) and 53(1) of the PSD.

- 7.7 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 PSD.
- 7.8 [cards] For virtual cards, the initial registration should take place in a safe and trusted environment.¹⁷ Strong customer authentication should be required for the virtual card data generation process if the card is issued in the internet environment.
- 7.9 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

8. 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.

¹⁷ 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).

- 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

9. PSPs should limit the number of log-in or authentication attempts, define rules for internet payment services session ‘time out’ and set time limits for the validity of authentication.
 - 9.1 When using a one-time password (OTP) 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

10. 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) address¹⁸ or IP range during the internet payment services session, sometimes identified by geolocation IP checks,¹⁹ 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.

¹⁸ An IP address is a unique numeric code identifying each computer connected to the internet.

¹⁹ A ‘Geo-IP’ check verifies whether the issuing country corresponds with the IP address from which the user is initiating the transaction.

- 10.2 Acquiring PSPs should have fraud detection and prevention systems in place to monitor e-merchant activities.
- 10.3 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.
- 10.4 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

11. 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 encryption²⁰ 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.

²⁰ 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

12. 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 channel²¹ 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 engineering²² 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;

²¹ Such as a dedicated mailbox on the PSP's website or a secured website.

²² 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

13. 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 limits²³ 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

14. 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 time²⁴ 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-

²³ Such limits may either apply globally (i.e. to all payment instruments enabling internet payments) or individually.

²⁴ Excluding exceptional non-availability of the facility for technical maintenance purposes, or as a result of major incidents.

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

Annex 1: Best practice examples

In addition to the requirements set out above, these guidelines describes some best practices which PSPs and the relevant market participants are encouraged, but not required, to adopt. For ease of reference, the chapters to which these best practices apply are stated explicitly.

General control and security environment

Governance

BP 1: The security policy could be laid down in a dedicated document.

Risk control and mitigation

BP 2: 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).

Traceability

BP 3: PSPs offering acquiring services could contractually require e-merchants who store payment information to have adequate processes in place supporting traceability.

Specific control and security measures for internet payments

Initial customer identification, information

BP4: 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.

BP5: 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.

Strong customer authentication

BP6: [cards] E-merchants could support strong authentication of the cardholder by the issuer in card transactions via the internet.

BP7: 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.

BP8: 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.

Protection of sensitive payment data

BP 9: It is desirable that e-merchants handling sensitive payment data appropriately train their fraud management staff and update this training regularly to ensure that the content remains relevant to a dynamic security environment.

Customer education and communication

BP 10: It is desirable that PSPs offering acquiring services arrange educational programmes for their e-merchants on fraud prevention.

Notifications, setting of limits

BP 11: 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.

BP 12: 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.

BP 13: 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.

4. Accompanying documents

4.1 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.²⁵ 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.²⁶ 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.²⁷ 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,

²⁵ See ECB Blue book at <https://www.ecb.europa.eu/paym/intro/book/html/index.en.html>

²⁶ 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.

²⁷ 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>

compromising the smooth operation of payment systems, decreasing efficiency throughout the economy, and undermining firms' efforts to realise cost efficiencies.

Objective

The 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 payments, a thorough assessment of risks, incident monitoring and reporting;
- to implement appropriate tracing of transactions and e-mandates;
- to implement a sound Know Your Customer (KYC) and provide essential information to the customer;
- to ensure a secure enrolment for and provision of authentication 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 e-mail account hacked. 7% have been the victim of credit card or banking fraud online.²⁸

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

²⁸ EU Commission (2013), *Special Eurobarometer 404 – Cyber security*, p. 52, at http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf

misusing personal data (mentioned by 37% of internet users in the EU) and security of online payments (35%).²⁹

The guidelines aim markedly to reduce these figures after implementation.

²⁹ EU Commission (2013), Special Eurobarometer 404 – Cyber security, p. 4.

4.2 Views of the Banking Stakeholder Group (BSG)

4.2.1 Summary of the BSG's opinion

The BSG welcomes the plans outlined in the CP for the EBA to address the issue of security of internet payments. In particular, the BSG was in support of providing a solid legal basis for consumer protection in this area rather than relying on the to-date voluntary arrangements for consumers to have maximum trust and confidence in the use of internet facilities for payments.

A specific emphasis was placed on the need for better consumer information regarding security incidents, as well as incident reporting to authorities. The French 'Observatoire de la securite des cartes de paiement'³⁰ and 'Financial Fraud Action UK'³¹ were cited as good practices for the information provided to consumers on relevant risks and instructions on security measures.

The BSG also expressly requested a monitoring mechanism for the implementation of these guidelines, and expressed the view that clarity was required on guidelines mainly related to risk assessments performed by PSPs, including the external assessment of these internal risk assessments.

4.2.2 EBA feedback on the BSG's opinion

The EBA welcomes the opinion of the BSG. With regard to the monitoring of the implementation of these guidelines, as well as the additional clarity desired regarding the risk assessments requested for PSPs, the EBA underlines the existence of an assessment guide for the security of internet payments, which was published by SecuRe Pay in February 2014³². This assessment guide will help National Competent Authorities to assess compliance of financial institutions with these guidelines on a harmonised basis.

³⁰ <https://observatoire.banque-france.fr/accueil.html>

³¹ <http://www.financialfraudaction.org.uk/>

³² <http://www.ecb.europa.eu/pub/pdf/other/assessmentguidesecurityinternetpayments201402en.pdf>

4.3 Feedback on the public consultation

The EBA publicly consulted on the draft proposal contained in this paper. The consultation period started on 20 October 2014 and ended on 14 November 2014. 45 responses were received, of which 39 were published on the EBA website.

This chapter, and the appended table, presents a summary of the key points and other comments made in response to the consultation and the EBA's feedback to these responses, including any actions taken to address them, if applicable.

In many cases, several industry bodies made similar comments or the same body repeated its comments in response to different questions. In such cases, the comments — and EBA analysis — are included in the section of this paper where the EBA considers them most appropriate.

Summary of key issues and the EBA's response

The EBA posed a single consultation question in the CP: If the scenario were to materialise in which the PSD 2 requires stronger security requirements from 2017/18 onwards, would respondents prefer for the final EBA guidelines under the PSD 1:

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

The majority of responses stated that they would be able to agree with the two-step approach, although a significant number of these respondents did so only as a second-best solution should their first choice — the EBA delaying the issuing of the guidelines until the transposition of the PSD 2 — not come to pass. Amongst the main reasons stated, respondents held the view that the alternative of a one-step approach was not feasible because it would be impossible to anticipate, at this stage, the final conclusions of the on-going PSD 2 debate on the definition of 'strong authentication'. This, so respondents continued, would therefore leave no time left for PSPs to adapt their IT platforms and payment systems interfaces.

None of the responses raised an issue with the 1 August 2015 implementation deadline, and some reiterated that they would be ready for the 1 February 2015 deadline set by the original SecuRe Pay recommendations.

Two responses expressed a preference for the one-step approach, while a large minority of responses were against either option and proposed instead that the EBA delay issuing the guidelines until the transposition date of the PSD 2 and its security requirements in 2017/18. One

of the main reasons given in these responses was that this would avoid additional costs for financial institutions before PSD 2 implementation. There were also concerns about an August 2015 implementation deadline.

The consultation deliberately did not ask for views on the substance of the guidelines, as these had already been consulted on by SecuRe Pay in 2012/13. However, some responses asked for clarification on some aspects of the guidelines.

A significant number of respondents used the opportunity of this consultation to express their views on what the future PSD 2 legislation should include. These remarks were not taken into account by the EBA.

Some respondents called for very limited supervision of internet payments to avoid hindering innovation, allowing each PSP to define the measures to be implemented to fight against fraud or even to leave consumers to decide what level of security they are willing to use.

A few responses challenged the definition of 'strong authentication' in the CP, asking for it to be aligned with the definition in the PSD 2. The EBA is of the view that the definition of strong authentication used in the guidelines was already discussed during the SecuRe Pay consultation, incorporates well-known security concepts and is not intended to anticipate the future PSD 2 regulation as a two-step approach will be implemented. Against this background, the definition of strong authentication remains in the guidelines as in the CP but will be amended when reviewing the guidelines following the implementation of the PSD 2.

As far as harmonisation is concerned, several respondents called for global harmonisation of security requirements at an international level to avoid fraud still being able to be committed outside the European Union at the expense of European PSPs and consumers. The EBA is indeed supportive of this argument and will pursue international cooperation with other competent authorities in that regard whenever possible.

Some respondents also requested some clarification regarding the scope of application of these guidelines as well as their binding nature. On those aspects, the EBA clarified that all PSPs covered under the PSD are subject to these guidelines. These guidelines define minimum requirements that have to be fulfilled by PSPs covered under the PSD by 1 August 2015.

Several respondents also requested clarification regarding the status of the 'Assessment guide for the security of internet payments', which had been published by SecuRe Pay in February 2014, once the EBA publishes the final guidelines. To aid the consistent implementation of its recommendations, SecuRe Pay had published the assessment guide for staff in supervisory and oversight authorities as a non-prescriptive tool to help them assess firms' compliance with the recommendations. The EBA encourages competent authorities to continue using the guide for the intended purpose.

Table 3: Overview of responses to the consultation and the EBA's feedback

Consultation question	Summary of responses received	EBA feedback	Amendments to the proposals
Responses to questions in Consultation Paper EBA/CP/2014/31			
Question 1: Do you prefer for the EBA guidelines to enter into force on 1 August 2015 using a 1-step or 2-step approach?	<p>1) The majority of responses stated that they would be able to agree with the two-step approach, although a significant number of these respondents did so only as a second-best solution should their first choice — the EBA delaying the issuing of the guidelines until the transposition of the PSD 2 — not come to pass. Amongst the main reasons stated, respondents held the view that the alternative of a one-step approach was not feasible because it would be impossible to anticipate, at this stage, the final conclusions of the on-going PSD 2 debate on the definition of 'strong authentication'. This, so respondents continued, would therefore leave no time left for PSPs to adapt their IT platforms and payment systems interfaces.</p> <p>None of the responses raised an issue with the 1 August 2015 implementation deadline, and some reiterated that they would be ready for the 1 February 2015 deadline set by the original SecuRe Pay recommendations.</p>	The EBA takes note of this majority position.	Implementation of the guidelines as of 1 August 2015
	2) Only two responses expressed a preference for the one-step approach based on the PSD 2 proposal.	The EBA takes note of this minority position.	2) Implementation of the guidelines as of 1 August 2015
	3) Other responses were against either option and proposed instead that the EBA delay issuing the guidelines until the transposition date of the PSD 2 and its security requirements in 2017/18. One of the main reasons given in these responses was that this would avoid additional costs for financial institutions before PSD 2 implementation. There were also concerns about an August 2015 implementation deadline.	Given the high level of fraud currently observed on internet payments and its increasing trend over recent years, the EBA does not consider delaying the implementation of the guidelines until the transposition of the PSD 2 to be a conceivable option, because security issues in internet payments have continued to undermine	3) Implementation of the guidelines as of 1 August 2015.

Consultation question	Summary of responses received	EBA feedback	Amendments to the proposals
		the confidence in payment systems and therefore require timely and consistent mitigation through regulation.	
Miscellaneous comments			
Comments applicable to the entire document	Several respondents insisted on the need for the guidelines to remain technology neutral, not preventing innovations in security, and to preserve an appropriate balance between security and consumer convenience.	The EBA points out that the guidelines are based on a proper assessment by PSPs. enabling the security of most risky transactions to be improved while at the same time preserving user convenience. The guidelines are neutrals as regards the technology to be used.	None
	Several respondents emphasised that the current guidelines should not aim to build a ‘European fortress’ and should therefore take into account the global environment.	The EBA shares the objective of coordination at an international level with regard to the security of internet payments. However, this approach does not prevent a harmonised level of security from being created across the European Union.	None
Comment applicable to paragraph 1	Several respondents challenged the ability of the EBA to issue guidelines on the security of internet payments based on the PSD regulation.	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, and they are issued under Article 16 of the EBA Regulation.	None
Paragraphs 2 & 3	One respondent asked for clarity regarding the actual addressees of these guidelines since paragraph 2 of the scope section refers to PSPs as defined in Article 1 of the Directive while paragraph 3 of the same section only mentions financial institutions as defined in Article 4(1) of Regulation (EU) No 1093/2010.	These guidelines apply to the provision of payment services offered via the internet by PSPs as defined in Article 1 of the PSD. Competent authorities in the 28 Member States should ensure the application of these guidelines by PSPs as defined in Article 1 of the PSD under their supervision.	None

Consultation question	Summary of responses received	EBA feedback	Amendments to the proposals
	A few respondents requested clarification regarding the exclusion of payment schemes under these guidelines as they can perform some of the security requirements set by the guidelines.	The 'Recommendations for the security of internet payments' continues to represent the document against which authorities with an oversight function for payment systems and payment schemes should assess compliance with regard to the security of internet payments. The guidelines also provide that 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 banks with an oversight function for payment instruments should liaise to ensure the consistent application of the guidelines by the actors responsible for the functioning of the scheme.	None
Paragraph 4	A few respondents asked for clarification regarding the implementation date of the SecuRe Pay recommendations as of 1 February 2015 and EBA guidelines as of 1 August 2015 and some of them emphasised the issue of ensuring a level playing field.	The date of entry into force for 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 intended to provide 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 to publicly consult on its draft guidelines, to assess the responses and to draw up 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 by the original	None

Consultation question	Summary of responses received	EBA feedback	Amendments to the proposals
		date of 1 February 2015 are not affected by the extension and should continue with their plans.	
Paragraph 5	Several respondents requested the introduction, as in the SecuRe Pay recommendations, of an explicit ‘comply or explain’ principle for the PSPs vis-à-vis their competent authority for the implementation of these guidelines.	Article 16 of Regulation (EU) No 1093/2010 provides a ‘comply or explain mechanism’ for competent authorities. 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 PSD under their supervision. All addresses shall make every effort to comply with the guidelines. In addition, competent authorities may require PSPs to report that they are complying with the guidelines. All addresses shall make every effort to comply with the guidelines.	None
	One respondent requested clarification regarding the nature of the guidelines, especially whether these guidelines should be considered as requirements or only expectations.	In light of Article 16 Regulation (EU) No 1093/2010, competent authorities and financial institutions shall make every effort to comply with the guidelines. These guidelines apply to the provision of payment services offered via the internet by PSPs as defined in Article 1 of the Directive and they establish a set of minimum requirements in the field of the security of internet payments.	None
Paragraph 7	Some respondents asked for the removal of some best practices as they should not be required to be implemented by PSPs, or asked for some of these best practices to remain as best practices under the future PSD 2 regulation	As explained in the annex of the guidelines, best practices are only encouraged and not required to be implemented. Regarding the link with the future PSD 2 regulation, this issue does not fall within the scope of the regulation.	None

Consultation question	Summary of responses received	EBA feedback	Amendments to the proposals
Paragraph 9	Some respondents asked for clarification regarding the inclusion or exclusion of payment account access services providers, also known as ‘third-party access providers’, from these guidelines as regards the reference to payment integrators.	Payment account access service providers, also known as ‘third-party access providers’, also do not fall within the scope of the guidelines because they are not covered by the PSD. Payment integrators referred to within the scope are entities that are either recognised as PSPs under the PSD or that have a contractual relationship with a PSP to offer its services. Under the last assumption, payment integrators can be seen as an outsourcer of a PSP and should then comply with the guidelines through the contractual agreement with the PSP.	None.
Paragraph 10	Some respondents asked for justification of the exclusions from the scope of the guidelines, underlying the need for a multi-channel approach. One respondent asked for mail order and telephone order transactions specifically to be covered.	These guidelines were issued to address the most urgent fraud issues related to internet payments. Current exclusions listed under paragraph 10, which were considered to be of lower priority, will deserve further attention under the future PSD 2 regulation.	None
Paragraph 11	Some respondents asked for clarification in the background and rationale section of the CP regarding the use of the undefined term ‘strong transaction authorisation’. Respondents in favour of delaying the guidelines with the PSD 2 implementation were particularly interested in the EBA aligning the definitions in the EBA guidelines — particularly regarding authentication and authorisation — with the PSD 2.	This term ‘strong transaction authorisation’ has been removed from the guidelines. The EBA is of the view that the definition of ‘strong authentication’ used in the guidelines was already discussed during the SecuRe Pay consultation, incorporates well-known security concepts and is not intended to anticipate the future PSD 2 regulation as a two-step approach will be implemented. Against this background, the definition of strong authentication remains in the guidelines as in the CP but will be amended when reviewing the guidelines with the	None. No amendment of the definition. As the definition of ‘strong customer authentication’ was in fact missing in the guidelines (the definition was only present in the background and rationale section of the CP), it was reintroduced

Consultation question	Summary of responses received	EBA feedback	Amendments to the proposals
		implementation of the PSD 2.	in the 'definitions' section of the final guidelines.
Paragraph 11 (cont.)	Two respondents underlined that credentials cannot be physical tools but rather the possession of physical tools.	The EBA agrees with this view and decided to correct the final guidelines accordingly.	Amendment: Credentials can also mean the possession of a physical tool containing the information (e.g. one-time-password generator, smart card), or something the user memorises or represents (such as biometric characteristics).
Guideline 2.1	One respondent requested to add that customers should be responsible for the security and use of their own (internet) payment environment. To secure the entire value chain, the security measures proposed by the guidelines should also apply to customers and e-merchants through proper legal and contractual arrangements.	Consumers and e-merchants are also addressed by this guideline through guideline 12.4 for the consumers and guidelines 4.8 and 11.3 for the e-merchants.	None
Guideline 2.3	One respondent requested that not only sensitive data (including credentials), but also all payment transaction-related data should be secured in terms of its integrity and origin.	As the definition of 'sensitive data' covers data enabling a payment order to be initiated, the EBA believes that this concern has been addressed.	None
Guideline 3.3	One respondent mentioned the impossibility of declaring security incidents to the relevant authority due to banking secrecy law.	Professional secrecy provisions apply to competent authorities, as provided for by the PSD.	None
Guideline 3.4	One respondent asked for clarification regarding the	Competent authorities in the 28 Member States	None

Consultation question	Summary of responses received	EBA feedback	Amendments to the proposals
	application of this guideline to existing customer agreements.	of the European Union should ensure the application of these guidelines by PSPs as defined in Article 1 of the PSD under their supervision. The issue raised in the question will be decided within the context of this supervision.	
Guideline 7.1	One respondent asked for there to be an option to add merchants with a trusted shop label to the list of trusted beneficiaries automatically.	The list of trusted beneficiaries is established by customers and is independent of any label.	None
Guideline 7.3	A few respondents requested clarity regarding the fact that PSPs should support strong authentication of the cardholder.	This guideline requests the issuer PSP to register all cards enabled for payment via the internet to be technically ready to be used with strong authentication if requested.	None
Guideline 7.6	Many respondents remarked that guideline 7.6 should be deleted since it addresses payment schemes, which do not fall within the scope of the EBA guidelines since they are not covered by the PSD.	The EBA agrees with this view and decided to correct the final guidelines accordingly.	Deletion
Guideline 7.10	One respondent asked how this guideline relates to the PCI requirements.	These draft guidelines do not attempt to define 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.	None
Guideline 8.1	One respondent asked for clarification as to whether this guideline applies to the enrolment of the consumer or the e-merchant.	Even if mainly directed at consumers, this guideline may also apply to the e-merchant if the latter is provided with an internet payment	None

Consultation question	Summary of responses received	EBA feedback	Amendments to the proposals
		authentication tool and/or payment-related software.	
Guideline 9.1	One respondent asked whether event-related OTPs, which by definition have no validity expiration, can be considered as strong authentication under these guidelines since it is not possible to limit the validity of OTPs to the strict minimum necessary.	Event-related OTPs are not excluded from the definition of strong authentication. When time-related OTPs are used, their validity should be limited to the strict minimum necessary.	None
Guideline 10.2	Many respondents remarked that guideline 10.2 should be deleted since it addresses payment schemes, which do not fall within the scope of the EBA guidelines since they are not covered by the PSD.	The EBA agrees with this view and decided to correct the final guidelines accordingly.	Deletion
Guideline 10.5	One respondent mentioned the need to have approval from the data protection authority before being able to block a transaction for security reasons.	The blocking of transactions for security reasons is already provided for under the PSD framework.	None
Guideline 12.4	A few respondents found guideline 12.4, which asks the PSP to initiate education to ensure that customers understand the need to protect their passwords, security tokens, personal details and other confidential data, to contradict the future proposed PSD 2 legislation regarding payment account access by third-party providers.	This document does not address pending or future legislation. Nevertheless, the possibility for third-party providers to access payment account information does not preclude the importance of customers' awareness concerning the security of their credentials.	None
Guideline 13.1	One respondent underlined that some internet payment transactions might be initiated in a face-to-face environment, which can make it difficult in practice to allow customers to disable the internet payment functionality.	The PSP must inform the customer that if he wishes to disable the internet payment functionality, he may not be able to pay in the situations referred to in the response.	None
	One respondent was of the view that it was not in the interest of the consumer to disable the internet payment	This guideline allows the consumer to have the option of disabling the internet payment functionality. It does not express any view with regard to whether it is in the interest of the	None

Consultation question	Summary of responses received	EBA feedback	Amendments to the proposals
Guideline 14.2	<p>functionality.</p> <p>One respondent asked for clarification as to whether this guideline would apply to transactions initiated by post, telephone order, voice mail or SMS, which do not fall within the scope of the guidelines.</p>	<p>consumer to use this option.</p> <p>No, if the underlying transaction is excluded from the scope of application of the guidelines, none of these guidelines apply.</p>	None

5. Confirmation of compliance with guidelines and recommendations

Date:

Member/EEA State:

Competent authority

Guidelines/recommendations:

Name:

Position:

Telephone number:

E-mail address:

I am authorised to confirm compliance with the guidelines/recommendations on behalf of my competent authority: Yes

The competent authority complies or intends to comply with the guidelines and recommendations: Yes No Partial compliance

My competent authority does not, and does not intend to, comply with the guidelines and recommendations for the following reasons³³:

Details of the partial compliance and reasoning:

Please send this notification to compliance@eba.europa.eu³⁴

³³ In cases of partial compliance, please include the extent of compliance and of non-compliance and provide the reasons for non-compliance for the respective subject matter areas.

³⁴ Please note that other methods of communication of this confirmation of compliance, such as communication to a different e-mail address from the above, or by e-mail that does not contain the required form, shall not be accepted as valid.