Security of Internet Payments: EBA issues new guidelines

January 2015

The Authors

Mark Woltman

Dario Rossa

Abstract

On the 19th of December 2014 the European Banking Authority (EBA) published its final Guidelines on the security of internet payments, which set the minimum security requirements that Payment Services Providers in the EU will be expected to implement by 1 August 2015.

Concerned about the increase in frauds related to internet payments, the EBA decided that the implementation of a more secure framework for internet payments across the EU was needed. Fraud levels on card internet payments have been rising in the last years and the EBA felt a regulatory response was necessary while waiting for the revision of the Payment Services Directive, which aims at creating more secure, competitive and consumer-friendly rules for payments in the EU.

These EBA guidelines specifically require that Payment Service Providers (PSPs) carry out strong customer authentication in order to verify the customer identity before proceeding with an on-line payment and also the clear protection of customer data, especially from a privacy perspective.

This Briefing Note presents an overview of regulatory impact for PSP's and customers, highlighting areas which should be carefully checked and implemented before the 1st of August 2015.

Security of Internet Payments: a brief history

In January 2013 the final recommendations for the security of internet payments were released by the ECB. In order to facilitate greater legal consistency as well as a more uniform implementation across the 28 EU member states the EBA agreed to convert those recommendations into EBA guidelines. The first consultation paper was published in October 2014, with incorporation of the original recommendations. Since the negotiations for the PSD2 were still ongoing a two-step approach was chosen for the implementation of the guidelines: Immediate implementation as of the 1st of August 2015 and (if necessary) an upgrade with the more stringent regulations derived from the PSD2 (planned for 2017/2018). The one step approach would try to implement new guidelines and include them later on in the PSD2.

The two step approach enables the incorporation of changes during the upcoming two years, while providing guidelines as soon as possible. With the quickly changing landscape in payments, privacy and regulatory requirements this seems to be the best choice.

There are 14 specific guidelines, each with a number of detailed sub-guidelines. We will briefly discuss these guidelines, as well as those sub-guidelines that could have a strong impact on PSPs and their customers.

Governance

PSPs should implement and regularly review a formal security policy for internet payment services. The security policy should be properly documented, and regularly reviewed. It should define security objectives, risk appetite, and roles and responsibilities, including risk management.

Risk assessment

Risk assessments with regards to internet payments and services should be carried out and documented on a regular basis, both prior as well as during the usage of those services. The assessment should also include the technical environment of the client and outsourcing parties, as well as paying specific attention to the security of sensitive payment data.

Incident monitoring & reporting

PSPs should ensure the consistent and integrated monitoring, handling and follow-up of security incidents, including security-related customer complaints. There should also be a procedure for reporting such incidents to management and, in the event of major payment security incidents, the competent authorities. These obligations also extend to e-merchants with whom the PSP is collaborating. It is important that the PSP takes an active role in this.

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. This is certainly one of the most critical points: networks, payment data, restricted access, outsourcing, and technology are all affected by this and should be thoroughly validated.

Traceability

PSPs should have the technology in place to trace all payment data, including that for e-mandate processes.

Initial customer identification and information

Customers should be properly vetted in line with the European anti-money laundering legislation and confirm their willingness to make internet payments using these services before being granted access to such services. Due diligence on customer identity has to have been performed, amongst other things, software and hardware requirements must be explained to the customers, and post detection or suspicion of abuse have to be clear and transparent.

Strong customer authentication

The initiation of internet payments, as well as access to sensitive payment data, should be protected by strong customer authentication. 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 (code, NFC without encryption, fingerprint) 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.

Enrolment for and provision of software and authentication tools to the customer

Effective and secure procedures should be in place for the delivery of personalized security credentials, payment-related software and all internet payment-related personalized 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.

Login attempts, session time out, authentication validation.

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. Procedures after failed login attempts and authentication have to be readily available.

Transaction monitoring

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

Protection of sensitive payment data

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 unauthorized access or modification. End-to-end encryption for

payments across the internet is a must as is the responsibility of the PSP for the enforcement of these measures by its e-merchants.

Customer education and communication

Guidance and assistance has to be given by the PSP's to their clients on how to manage transactions in a secure way via the internet. At least one secured channel should be available to communicate directly to the customers.

Notifications and setting of limits

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

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

PSPs should confirm the payment initiation to their customers and provide them in a timely manner with the necessary information to validate that a payment transaction has been correctly initiated and/or executed. Any detailed electronic statements should be made available in a safe and trusted environment. Where PSPs inform customers about the availability of electronic statements (e.g. regularly when a periodic e-statement has been issued, or on an ad hoc basis after execution of a transaction) through an alternative channel, such as SMS, e-mail or letter, sensitive payment data should not be included in such communications or, if included, they should be masked.

Closing remarks

The EBA has set out a set of guiding principles for secure internet payments, which will come into effect on the 1st of August 2015.

These guidelines will put more emphasis, and thus effort, on customer security and privacy, pro-active communication, reporting and notification by PSPs to both their customers as well as to the regulators and the overall responsibility of PSPs for their e-merchants or outsourcing partners. Covering all these guidelines will be a major challenge within a narrow timeframe. Nevertheless it can be seen as a preparation for the next critical phase for payments, security, regulations and workload resulting from the upcoming PSD2.

Contacts

Spike Reply (Brussels)

5, rue de Congrès/Congresstraat
1000 Brussels
Belgium
Tel: +32 (0) 2 880 03 20
E-mail: spike@reply.eu

Spike Reply (Paris)

5, rue des colonnes - 6 ième étage
75002 Paris
France
Tel: +39 06 844341
E-mail: spike@reply.it

Spike Reply (Luxembourg)

46a, avenue J.F. Kennedy
L- 1855 Luxembourg
Luxembourg
Tel: +352 26 00 52 64
E-mail: spike@reply.eu