Deloitte.

Reff Associates

Financial Services
Industry News

The European Banking Authority ("EBA") issues Guidelines on the security of internet payments

On December 19, 2014, EBA published the Guidelines on the security of internet payments to establish a set of minimum requirements concerning the security of payment services offered through the internet (internet payments). The Guidelines have been issued in response to the high levels of fraud surrounding internet payments and will be implemented on 1 August 2015. More stringent requirements are expected to be applied under the future PSD 2 at a later stage.

The Guidelines are based on the provisions of Directive 2007/64/EC on payment services (the "Payment Services Directive") concerning information requirements for payment services and obligations of payment services providers ("PSPs"). It should be noted that apart from the minimum requirements set out in the Guidelines, it is responsibility of the PSPs to monitor and assess the risks involved in their payment operations, develop their own detailed security policies and implement adequate measures that are commensurate with the risks inherent in the payment services provided. The competent authority may decide to require the PSPs to report that they are complying with the guidelines.

Scope. The Guidelines are addressed to financial institutions as defined by Article 4 paragraph (1) of the Regulation no. 1093/2010 and to competent authorities as defined by Article 4 paragraph (2) of the Regulation no. 1093/2010 and are applicable in the case of internet payment services, irrespective of the access device used, that include: 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"; the execution of credit transfers on the internet; the issuance and amendment of direct debit electronic mandates; transfers of electronic money between two e-money accounts via internet.

Main provisions. There are 14 specific guidelines, each with a number of detailed sub-guidelines and a list of 13 best practices that may be classified in two categories that address the following: 1) specific control and security measures for internet payments and 2) customer awareness, education, and communication

1. Guidelines regarding the specific control and security measures for internet payments

Governance. PSPs should implement and regularly review a formal security policy for internet payment services that should define security objectives and the risk appetite. According to the best practices the security policy could be laid down in a dedicated document.

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

Incident monitoring and reporting. PSPs should ensure the consistent and integrated monitoring, handling and follow-up of security incidents, including security-related customer complaints and also establish a procedure for reporting major payment security incidents to the competent authorities. The PSPs should ensure contractually the collaboration of e-merchants in the case of major payment security incidents, as defined by the Guidelines.

Risk control and mitigation. PSPs should implement security measures incorporating multiple layers of security defences in line with their respective security policies in order to mitigate identified risks and should be subject to periodical independent audit. These type of security measures are some of the most important aspects impacted by the Guidelines, as these will affect networks, sensitive payment data, outsourcing and technology used by the PSPs. The PSPs will ensure that e-merchants and any outsourcing partners comply with the same set of guidelines.

Traceability. PSPs should have processes in place ensuring that all transactions (including the e-mandate process flow) are appropriately traced. The best practices provide that PSPs could contractually require e-merchants who store payment information to have adequate processes in place supporting traceability.

Initial customer identification and information. Customers should be properly identified in line with the European anti-money laundering legislation and confirm their willingness to make internet payments using the services before being granted access to such services. According to the best practices 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).Customers should also be provided with clear and straightforward instructions explaining their responsibilities regarding the secure use of the service.

Strong customer authentication. PSPs will ensure that the initiation of internet payments, including access to sensitive payment data, should be protected by strong customer authentication, as defined by the Guidelines. Examples of strong customer authentication may include elements linking the authentication to a specific amount and payee. The best practices provide that, for customer convenience purposes, PSPs could consider using a single strong customer authentication tool for all internet payment services.

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

Login attempts, session time out, authentication validation. PSPs should set out rules limiting the number of log-in or authentication attempts, define rules for internet payment services session 'time out' and set time limits for the validity of authentication.

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

Protection of sensitive payment data. The Guidelines clearly state that sensitive payment data should be protected when stored, processed or transmitted. In the event e-merchants handle sensitive payment data, such PSPs should contractually require the e-merchants to have the necessary measures in place to protect these data. For this purpose, according to the best practices, 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.

2. Guidelines regarding customer awareness, education, and communication

Customer education and communication. PSPs should provide assistance and guidance to customers, where needed, with regard to the secure use of the internet payment services. At least one secure channel should be available to communicate directly to the customers. Also, according to the best practices, it is desirable that PSPs offering acquiring services arrange educational programmes for their e-merchants on fraud prevention

Notifications and setting of limits. Prior to providing a customer with internet payment services, PSPs should set limits 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 the payment initiation and execution. PSPs should confirm to their customers the payment initiation and provide customers in good time with the information necessary to check that a payment transaction has been correctly initiated and/or executed. Any detailed electronic statements should be made available in a safe and trusted environment. Alternative channels, such as SMS, e- mail or letter, are not considered a trusted environment and, therefore, sensitive payment data should not be included in such communications or, if included, they should be masked.

Implementation. The competent authority must notify the EBA as to whether they comply or intend to comply with these guidelines or otherwise with reasons for non-compliance, no later than May 05, 2015. In the absence of any notification by this deadline, EBA will consider the competent authority to be non-compliant.

For further questions regarding the guide, please do not hesitate to contact us.

Andrei Burz-Pinzaru
Attorney-at-law
+40 21 207 52 05

Irina Albusel
Attorney-at-law
+40 21 207 54 26

For further information please contact us at:
Romania@deloittece.com or visit the web page
www.deloitte.com/ro/tax-alerts