"laCaixa"

19th June 2012

ECB Recommendations for the Security of Internet Payments

April 2012

"la Caixa" response

2 RECOMMENDATIONS

GENERAL CONTROL AND SECURITY ENVIRONMENT

Recommendation 1: Governance

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

1.1 KC. *The internet payment services security policy should be properly documented, and regularly reviewed and approved by senior management. It should define security objectives and the PSP's risk appetite.*

1.2 KC. *The internet payment services security policy should define roles and responsibilities, including an independent risk management function, and the reporting lines for internet payment services, including management of sensitive payment data with regard to the risk assessment, control and mitigation.*

Recommendation 1 Comments:

1.1 KC: Security measures should apply to all players, including non licensed institutions

1.2 KC: The concept of "independent" should be clarified because, unlike for the audit function, some degree of integration of the risk management function seems desirable for efficiency and effectiveness reasons.

Recommendation 2: Risk identification and assessment

PSPs should regularly carry out and document thorough risk identification and vulnerability assessments with regard to internet payment services.

2.1 KC. *PSPs, through their risk management function, should carry out and document detailed risk identification and vulnerability assessments, including the assessment and monitoring of security threats relating to the internet payment services the PSP offers or plans to offer, taking into account: i) the technology solutions used by the PSP, ii) its outsourced service providers and, iii) all relevant services offered to customers. PSPs should consider the risks associated with the chosen technology platforms, application architecture, programming techniques and routines both on the side of the PSP 8 and the customer.9*

Recommendation 2 Comments:

2.1 KC: Clients should be responsible for the security and use of their own (internet) payment environment. In order to secure the whole value chain, the security measures proposed by the ECB should also apply to customers and e-merchants through proper legal and contractual arrangements.

Recommendation 3: Monitoring and reporting

PSPs should ensure the central monitoring, handling and follow-up of security incidents, including security-related customer complaints. PSPs should establish a procedure for reporting such incidents to management and, in the event of major incidents, the competent authorities.

3.1 KC. *PSPs should have a process in place to centrally monitor, handle and follow up on security incidents and security-related customer complaints and report such incidents to the management.*

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

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

Recommendation 3 Comments:

These security measures should apply to all service providers, not only PSPs.

Recommendation 4: Risk control and mitigation

PSPs should implement security measures in line with their internet payment services security policy in order to mitigate identified risks. These measures should incorporate multiple layers of security defences, where the failure of one line of defence is caught by the next line of defence ("defence in depth").

4.2 KC. *Public websites and backend servers should be secured in order to limit their vulnerability to attacks. PSPs should use firewalls, proxy servers or other similar security solutions that protect networks, websites, servers and communication links against attackers or abuses such as "man in the middle" and "man in the browser" attacks. PSPs should use security measures that strip the servers of all superfluous functions in order to protect (harden) and eliminate vulnerabilities of applications at risk. Access by the various applications to the data and resources required should be kept to a strict minimum following the "least privileged" principle. In order to restrict the use of " fake" websites imitating legitimate PSP sites, transactional websites offering internet payment services should be identified by extended validation certificates drawn up in the PSP's name or by other similar authentication methods, thereby enabling customers to check the website's authenticity.*

4.4 KC. *Security measures for internet payment services should be tested by the risk management function to ensure their robustness and effectiveness. Tests should also be performed before any changes to the service are put into operation. On the basis of the changes made and the security threats observed, tests should be repeated regularly and include scenarios of relevant and known potential attacks.*

Recommendation 4 Comments:

4.2. KC: These infrastructure security measures are useful to protect the internet payment applications from being abused by external attackers, but their main objective is not protect against "man-in-the-middle" or "man-in-the-browser" attacks. However, they should be deployed because of their usefulness for protecting the infrastructure.

If the goal is the enumeration of security measures that should be required to deploy, there should be a detailed enumeration. In this case, as PCI details the measures that should be deployed, this standard could be used as basis for the technical security recommendations.

The recommendation only takes into account infrastructure security measures, but we think that they should take into account web/mobile/... application security measures.

4.4 KC: Whilst testing is a necessary step, the way it is organised should be left to the discretion of each PSP.

SPECIFIC CONTROL AND SECURITY MEASURES FOR INTERNET PAYMENTS

Recommendation 6: Initial customer identification, information

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

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

clear information on any requirements in terms of customer equipment, software or other necessary tools (e.g. antivirus software, firewalls);

guidelines for the proper and secure use of personalised security credentials;

a step-by-step description of the procedure for the customer to submit and authorise a payment, including the consequences of each action;

guidelines for the proper and secure use of all hardware and software provided to the customer;

the procedures to follow in the event of loss or theft of the personalised security credentials or the customer's hardware or software for logging in or carrying out transactions;

the procedures to follow if an abuse is detected or suspected;

a description of the responsibilities and liabilities of the PSP and the customer respectively with regard to the use of the internet payment service.

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

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

Recommendation 6 Comments:

6.2 KC: Customers should be made aware of any updates to address new security threats in order to prevent fraud.

6.3 KC: Even though anti-money laundering is a sound legitimate objective, it does not seem to belong within a document on security requirements.

6.1 BP: Whilst it is legitimate that internet payments be subject to contractual arrangements, individual institutions should be allowed to decide how they organise their contractual

relationships with their customers.

Recommendation 7: Strong customer authentication

Internet payment services should be initiated by strong customer authentication.

7.1 KC. *[CT/e-mandate] Credit transfers (including bundled credit transfers) or electronic direct debit mandates should be initiated by strong customer authentication. PSPs could consider adopting less stringent customer authentication for outgoing payments to trusted beneficiaries included in previously established "white lists", i.e. a customer-created list of trusted counterparties and beneficiary accounts with strong authentication.*

7.2 KC. *Obtaining access to or amending sensitive payment data requires strong authentication. Where a PSP offers purely consultative services, with no display of sensitive customer or payment information, such as payment card data, that could be easily misused to commit fraud, the PSP may adapt its authentication requirements on the basis of its risk analysis.*

7.3 KC. *[cards] For card transactions, all PSPs offering issuing services should support strong authentication of the cardholder. All cards issued must be technically ready (registered) to be used with strong authentication (e.g. for 3-D Secure, registered in the 3-D Secure Directory) and the customer must have given prior consent to participating in such services. (See Annex 3 for a description of authentication under the cards environment.)*

7.5 KC. *[cards] PSPs offering acquiring services should require their e-merchant to support strong authentication of the cardholder by the issuer for card transactions via the internet. Exemptions to this approach should be justified by a (regularly reviewed) fraud risk analysis. In the case of exemptions, the use of the card verification code, CVx2, should be a minimum requirement.*

7.6 KC. *[cards] All card payment schemes should promote the implementation of strong customer authentication by introducing liability shifts (i.e. from the e-merchant to the issuer) in and across all European markets.*

Recommendation 7 Comments: Customers should only be allowed to enter their credentials and authentication codes by themselves in a secure environment as indicated and approved by the issuing PSP.

With respect to authentication, protection against for example a "Man in the Middle" attack should also be effective. Here it is impossible for the issuing PSP to distinguish between the actual fraudulent and (supposedly) non-fraudulent use of authentication codes not initiated by PSP customers and/or in the secure banking environment. PSPs are not able to inform their customers whether or not these services are genuine and trustworthy. Customers themselves are also not able to recognise the difference between genuine and fraudulent services.

The strong authentication measures to deploy should be in balance with the fraud detection systems.

In this point strong authentication recommendations want to be analysed, but authorisation recommendations are also discussed (i.e. CVx2). We think that there should be two different points, because the recommendations could be different.

Besides, in general the aim of the document is formulating recommendations for internet payments ((a) card payments, (b) e-banking transfers, etc.). The recommendations for strong authentication and authorisation may be quite different for each one of the scenarios, so separating both scenarios could be advisable.

7.2 KC: The first sentence should read "...strong customer authentication...."
7.3 KC: It should be clarified what is meant by "such services"
7.5. KC: Clarify "regularly reviewed".
7.6 KC:

- As there is no contractual relationship between the e-merchant and the issuer, it should read "i.e. from the acquirer to the issuer".

Recommendation 8: Enrolment for and provision of strong authentication tools
PSPs should ensure that customer enrolment for and the initial provision of strong authentication tools required to use the internet payment service is carried out in a secure manner.

8.1 KC. *Enrolment for and provision of strong authentication tools should fulfil the following requirements.*

The related procedures should be carried out in a safe and trusted environment (e.g. face-to-face at a PSP's premises, via an internet banking or other secure website offering comparable security features, or via an automated teller machine).

Personalised security credentials and all internet payment-related devices and software enabling the customer to perform internet payments should be delivered securely. Where tools need to be physically distributed, they should be sent by post or delivered with acknowledgement of receipt signed by the customer. Software should also be digitally signed by the PSP to allow the customer to verify its authenticity and that it has not been tampered with. Moreover, personalised security credentials should not be communicated to the customer via e-mail or website.

[cards] For card transactions, the customer should have the option to register for strong authentication independently of a specific internet

purchase. In addition, activation during online shopping could be offered by re-directing the customer to a safe and trusted environment, preferably to an internet banking or other secure website offering comparable security features.

8.2 KC. *[cards] Issuers should actively encourage cardholder enrolment for strong authentication. Cardholders should only be able to bypass strong authentication in exceptional cases where this can be justified by the risk related to the card transaction. In such instances, weak authentication based on the cardholder name, personal account number, expiration date, card verification code (CVx2) and/or static password should be a minimum requirement.*

Recommendation 8 Comments:

8.1 KC: Has a detailed analysis of the various means of communicating security credentials been undertaken to support the recommendation made? For instance, delivery by e-mail is not always considered to be a bad practice. Another example is card-based authentication devices used in some countries for internet payments. Since these devices are not personalised and do neither contain credentials nor secret key material, secure delivery should not be required (in view of the associated costs).
8.2 KC: Unless agreed by the issuer, bypassing of strong authentication by the cardholder should not be allowed and if it were to occur, it should be under the latter's responsibility.

Recommendation 10: Transaction monitoring and authorisation

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

10.1 KC. *PSPs should use real-time fraud detection and prevention systems to identify suspicious transactions, for example based on parameterised rules (such as black lists of compromised or stolen card data), abnormal behaviour patterns of the customer or the customer's access device (change of Internet Protocol (IP) address12 or IP range during the internet payment session, sometimes identified by geolocation IP checks,13 abnormal transaction data or e-merchant categories, etc.) and known fraud scenarios. The extent, complexity and adaptability of the monitoring solutions should be commensurate with the outcome of the fraud risk assessment.*
10.2 KC. *Card payment schemes in cooperation with acquirers should elaborate a harmonised definition of e-merchant categories and require acquirers to implement it accordingly in the authorisation message conveyed to the issuer.14*

Recommendation 10 Comments:

10.1 KC: The level of monitoring should be proportionate to the level of security required and strength of the customer authentication method used.
PSP should put at merchants disposal the appropriate tools to allow them the consolidation of risk qualified transactions and to avoid their automatic settlement.
10.2. KC: the acquirer must guarantee that the client associated real activity information is correctly sent to the issuer with the purpose to help the fraud prevention management tool within the resolutor environment.
10.X. The title of this point is "Transaction monitoring and authorisation", but only fraud detection and stopping processes are discussed. We think that there should be two different points that should be clearly separated: one for authorisation recommendations, and another

one with fraud detection processes recommendations.
For example, in e-banking is a PIN2 recommendable? We think it shouldn't be. Etc.

Recommendation 11: Protection of sensitive payment data

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

> ***11.2 KC.*** *PSPs should ensure that when transmitting sensitive payment data, a secure end-to-end communication channel is maintained throughout the entire duration of the internet payment service provided in order to safeguard the confidentiality of the data, using strong and widely recognised encryption techniques.*
> ***11.3 KC.*** *[cards] PSPs offering acquiring services should encourage their e-merchants not to store any sensitive payment data related to card payments. In the event e-merchants handle, i.e. store, process or transmit sensitive data related to card payments, such PSPs should require the e-merchants to have the necessary measures in place to protect these data and should refrain from providing services to e-merchants who cannot ensure such protection.*

Recommendation 11 Comments:

11.2 KC: End-to-end security is only required when sensitive data has to travel the whole distance from endpoint to endpoint.
11.3 KC: PCI DSS standard already includes sensitive payment data protection. In case that merchant should acces or store sensitive information they must be required to comply with PCI DSS.

CUSTOMER AWARENESS, EDUCATION AND COMMUNICATION

Recommendation 12: Customer education and communication

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

> ***12.4 KC.*** *PSPs and, where relevant, card payment schemes should initiate customer education and awareness programmes designed to ensure customers understand, at a minimum, the need:*
>
> *to protect their passwords, security tokens, personal details and other confidential data;to manage properly the security of the personal device (e.g. computer), through installing and updating security components (antivirus, firewalls, security patches);to consider the significant threats and risks related to downloading software via the internet if the customer cannot be reasonably sure that the software is genuine and has not been tampered with;to use the genuine internet payment website.*

Recommendation 12 Comments:

Education of customers is among others the responsibility of the PSPs. They need to educate their customers on the right level of security including the correct URLs and websites.

12.4 KC: Education is important but it does not exempt customers from their responsibility to keep their own credentials secure.

Recommendation 13: Notifications, setting of limits

PSPs should provide their customers with options for risk limitation when using internet payment services. They may also provide alert services.

> ***13.1 KC.*** *Prior to providing internet payment services, PSPs should agree with each customer on spending limits applying to those services.*
> *(e.g. setting a maximum amount for each individual payment or a cumulative amount over a certain period of time), and on allowing the customer to disable the internet payment functionality.*

Recommendation 13 Comments:

13.1 KC: Managing spending limits should be left to the responsible market players involved with the relation to customers.