Co-operative Banking Group response to ECB Recommendations for the Security of Internet Payments

The Co-operative Banking Group is part of The Co-operative Group, the UK's largest consumer co-operative and includes **smile**, Britannia and The Co-operative Insurance. With a combined network of 345 branches serving 8.5 million customers, we offer a range of financial products, including current accounts, savings accounts, credit cards and loans to both retail and corporate customers. In the UK we have, approximately, a 2% share of the Personal Current Account (PCA) market and provide a compelling co-operative alternative to the PLC banks.

Introduction

The Co-operative banking Group welcomes the recommendations to improve the security of internet payments. We feel the integrity of online payments is critical to maintaining consumer confidence and the provision of secure payment services is expected. Any raising of or the introduction of standards will help in this regard.

General comments

- It is not that clear which parties are within scope and why and this area should be enhanced to provide absolute clarity. There needs to be a clear statement that clarifies and aligns to terminology within other legislation such as PSD.

- All institutions / entities involved in online payments should be in scope of the recommendations and this should also include overlay providers who utilise the “host” account to make payments. The recommendations would be much clearer if there were sections depending on the type of payment service you provide (in line with previous bullet point)

- Whilst authentication of the customer is obviously important, there should be recognition of the layered approach to ensuring authenticity and integrity through numerous additional controls and this should feature as part of the recommendations perhaps acknowledging that PSPs could take a risk based approach, rather than a one size fits all recommendation. This is really important given strong customer authentication is currently being subverted through social engineering in the latest online malware attacks and also to ensure we balance security with risk and consumer convenience / usability.

- In respect of timescales, there are many recommendations included, some which are more material than others in terms of securing payments through the channel. It may be beneficial to phase the recommendations, with key timescales aligned to high priority recommendations. Overall mid 2014 seems ambitious given the scope of those included and scale of improvements required.

- It would be beneficial to clarify further what constitutes sensitive payment data. The Glossary states this is data which could be used to carry out fraud. Is this in its entirety or used along with other harvested data to commit fraud? Key point given the focus on PAN data within PCI and the lack of ability to commit fraud with this data alone.

- Consumer education is a key element in any solution to successfully reduce risk and fraud and this is best served from a global or industry perspective, rather than individual institution. Whilst individual responsibility should be a given and is accepted, PSPs need to ensure they do not

provide too much information publicly about what they do to secure payments, which leads to mimicking by criminals and creates a false sense of security to elicit information. Further, latest malware hides security screens and messages and therefore the effectiveness of this at individual institution level is weakened.

Comments on specific recommendations

4.2 KC – Public website 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, services and communications 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 PSPs name or by other similar authentication methods, thereby enabling customers to check the websites authenticity.

This is a broad recommendation stating specific solutions, which are in danger of becoming quickly outdated. Would be preferable to have a higher level recommendation around securing websites and back end servers, rather than a specific list of items which are not comprehensive, i.e. if all were implemented would still have vulnerabilities, given reliance on the customer.

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 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 potential attacks.

Suggest that responsibilities for this should be made generic (e.g. "relevant function(s)" rather than a "risk management function") to ensure that they do not unnecessarily impact on a companies' organisational structure. For instance, responsibilities for performing testing may sit in the first-line whilst the second-line risk management function may provide oversight and challenge.

4.5 KC – The PSPs security measures for internet payment services should be periodically audited to ensure their robustness and effectiveness. The implementation and functioning of the internet services should also be audited. The frequency and focus of such audits should take into consideration, and be in proportion to, the security risk involved. Trusted and independent experts should carry out the audits. They should not be involved in any way in the development, implementation or operational management of the internal payment services provided.

To be meaningful, would suggest rephrasing periodically audited to periodically tested and that testing should be undertaken by external testing companies.

4.6 KC – Whenever PSPs and card payment schemes outsource core functions related to the security of the internet payment services, the contract should include provisions requiring compliance with the principles and recommendations set out in this report.

The recommendations should make it clear what constitutes a core function.

6.1 KC – PSPs should ensure that the customer has undergone the necessary identification procedures and provided adequate identity documents and related information before being granted access to the internet payment services.

This is too ambiguous to be a meaningful control – necessary and adequate could be individually defined. Suggest this is strengthened as feel it is a valid requirement.

6.2KC - 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 etc.

Given consumer PC is the weakest link – may be advantageous to explore any appetite for minimum customer requirements / liability shifts as part of the recommendations. This is very difficult to implement individually, but as a standard industry requirement, could make a big difference to overall security.

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

As above could this form part of a mandated minimum requirement for a customer to maintain a level of security?

7.1KC – 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 counterparts and beneficiary accounts with strong authentication.

Clarity required on the direct debit point being initiated by strong customer authentication. The originator requests the funds and the onus and liability is on them for validation of the identity of the proposer and the account they have provided and signed to debit. The request therefore comes from the merchant and strong customer authentication would not reside with the PSP, unless a DD originator is classed as a PSP. Back to earlier comments around clarity of scope, roles and responsibilities of all players.

7.7 KC – For the card payment schemes accepted by the service, providers of wallet solutions should support technologies allowing the issuer to perform strong authentication when the legitimate holder first registers the card data. Providers of wallet solutions should support strong user authentication when executing 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 CVx2 should be a minimum requirement.

We fully support the recommendation to bring new technologies into scope however more clarity is required on what constitutes 'strong customer authentication'. As previously commented this should not be overly prescriptive and should be based upon a layered approach.

8.1 KC – Enrolment for and provision of strong authentication tools should fulfil the following requirements;

Support requirements here generally but need to distinguish between hardware and software as there is some cross over, i.e. sending software securely via the post?

8.2 KC – 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.

Exceptional cases should also include “opt out” or bypass for DDA purposes which should be appropriately managed and controlled.

Debbie Strickland
Head of Strategy and Fraud Management
Financial Crime Management
The Co-operative Banking Group