75 Westminster Bridge Road

London

SE1 7HS

European Central Bank

Secretariat Division

Kaiserstrasse 29

D-60311 Frankfurt am Main

Germany

By email to: ecb.secretariat@ecb.europa.eu

19th June 2012

Recommendations for the Security of Internet Payments

Following consultation with our members, who include card schemes, acquiring banks, payment processors, payment service providers, hardware/software solutions providers, systems integrators, consultancies, security specialists and indeed representatives from all key stakeholder groups in the European payments industry, Vendorcom, The Cards & Payments Community in Europe, is pleased to make the following submission in response to the Recommendations for the Security of Internet Payments:

1 General Part

Whilst we applaud any initiative aimed at increasing knowledge and understanding of security issues around internet payments, and which puts responsibility for that security onto the relevant parties, given the presence of PCI as a global standard for security for all card/token based payments, including those made over the internet, there is concern that these recommendations, once implemented, may be a source of confusion, unless they harmonise with the PCI standards. We appreciate that these recommendations extend beyond card/token based payments and perhaps it is this area upon which they should be focused.

As a global standard for card/token based payments, supporting PCI should meet the ECB's aim of achieving a 'harmonised EU/EEA-wide minimum level of security'. It would be interesting to understand what level of engagement there has been with the PCI SSC in the process of creating these recommendations.

In addition, there was a level of confusion as to the focus of the recommendations, which we believe to be internet based transactions, where the document specifies that the Forum focused on the whole processing chain..., 'irrespective of the payment channel'.

Scope and Addressees

As a key point of clarification, the recommendations use the Payment Services Directive's definition of PSP:

> 1. This Directive lays down the rules in accordance with which Member States shall distinguish the following six categories of payment service provider:
>
> (a) credit institutions within the meaning of Article 4(1)(a) of Directive 2006/48/EC;
>
> (b) electronic money institutions within the meaning of Article 1(3)(a) of Directive 2000/46/EC;
>
> (c) post office giro institutions which are entitled under national law to provide payment services;
>
> (d) payment institutions within the meaning of this Directive;
>
> (e) the European Central Bank and national central banks when not acting in their capacity as monetary authority or other public authorities;
>
> (f) Member States or their regional or local authorities when not acting in their capacity as public authorities.

The PSD goes on to provide a number of specific exclusions, including:

> (j) services provided by technical service providers, which support the provision of payment services, without them entering at any time into possession of the funds to be transferred, including processing and storage of data, trust and privacy protection services, data and entity authentication, information technology (IT) and communication network provision, provision and maintenance of terminals and devices used for payment services.

Given the broad use of the term PSP in common parlance, where it would typically be used specifically to refer to those organisations covered in (j), rather than issuers and acquirers, it would be useful to have confirmation that these recommendations would not apply to the group defined in (j), as if it did, this would require a very different response to that included in our submission, below. If it were to include (j), many of the recommendations would be unworkable.

In addition to the confusion caused by the use of the term PSP (as highlighted above), the document causes further confusion, by, on occasion referring to 'PSPs offering acquiring services' (11.3KC) or specifically to 'acquirers' (10.2 KC), which implies that in other areas where the term PSP is being used, it may not include these groups? Further in 8.1KC PSP appears to be specifically referring to issuers in this instance (due to the nature of the process being referred to) and yet in 8.2 KC, the term 'issuer' is used specifically.

There is a feeling that we are perhaps seeing the results of the merging of two separate documents, and that the differing terminology used in each has not be harmonised.

As a further point of clarification (not directly related to this section of the document, but vital to raise in relation to clear definitions), the word 'customer' appears to be used inconsistently through the document to mean both 'merchant' and 'consumer'. It is vital to the successful interpretation and implementation of the recommendations that this be resolved. As an example, in Recommendation 6, if PSP means issuer/acquirer, then it is a logical interpretation that 'customer' is the merchant. However, Recommendations 7 and 8 speak to 'strong customer authentication', which, in line with the definition in the document, we interpret to be referring to the 'consumer'. In Recommendation 12, similar confusion arises, from the statement that 'PSPs should communicate with their customers…' as for an issuer, the customer is the consumer and for an acquirer, the customer is the merchant. Is it that, as currently written, the recommendations are trying to address too wide an audience in one document?

Putting together a response to this document has been especially difficult due to the confusion caused by some of the above mentioned terminology issues and so, once definitions have been tightened and inconsistencies eradicated, it may be necessary to review the document again in order to provide the best level of response.

As a final point on Scope and Addressees, significant interest was raised around the exclusion of both corporate cards and non-rechargeable physical or virtual pre-paid cards. Could further explanation as to the reason for exclusion be provided here?

Guiding Principles

To our reading, the definition of 'strong customer authentication' in this section would exclude 3D Secure, as it is currently implemented in some European countries as 3D secure does not meet the requirement that at 'least one of the elements should be non-reusable and non-replicable …'. Whilst we agree that the definition provided here is one to aspire to, given the timescales for implementation of the recommendations, it is our belief that this is unachievable within the timeframe. This becomes of great concern because, in the absence of strong customer authentication (as defined,), a PSP would be denied the opportunity to claim that the customer has authorised the transaction, which significantly undermines the good work that the consumer payments industry has done to achieve the current levels of protection for both consumer and payment processor.

Confusion is also caused by the fact that later in the document, 3D Secure is specifically referred to as an example of 'strong customer authentication' (7.3 KC).

Where the document refers to PSPs engaging in customer awareness programmes, we commend this in relation to where the PSP is the issuer, but question whether this should - or even could - fall to the acquirer, given that they have no direct relationship with the consumer.

Given the current inconsistent implementation of the PSD across the different European geographies, we are concerned as to what level of harmonisation will actually take place should the recommendations become part of the PSD revision. The implementation of the PSD has demonstrated that successful harmonisation is dependent upon the way in which national government translates the Directive into national law and moreover, is then impacted by the way in which the national overseeing bodies interpret that legislation. The final sentence in this section, specifying a 1st July 2014 deadline, but suggesting that national authorities may wish to define shorter implementation periods also leaves significant room for difficulty for PSPs who operate across multiple geographies.

Similarly concern was raised around the timescales from a Direct Debit point of view, where a 1st July 2014 deadline was felt to be unrealistic.

2. Recommendations

It was generally agreed that a short preamble to each of the recommendations, which outlines what it is setting out to achieve would provide useful context within which to ensure accurate interpretation of the recommendation.

Recommendation 1: Governance

Whilst we wouldn't disagree with the recommendations here, our view is that this is that it talks to the heart of the PCI standard, which already requires such a policy in order to achieve compliance and that, as such, could be regarded as an unnecessary duplication. Whether there is advantage in having this codified within the PSD is debatable, as the combination of the PCI standards and current Data Protection legislation (being harmonised for Europe at present) would seem more than adequate to ensure that PSPs meet the listed requirements.

If the concern is that, as an example, Issuers and Acquirers are not currently being held to account under PCI (and it is accepted that this is the case), would it not be better that we seek to resolve this issue directly through ensuring appropriate scheme mandates and sanctions to support the standards already in place, rather than seek to utilise legislation to resolve the matter. This would seem to suggest that there is a desire to take a more legislative approach in these matters rather than work with the consumer payments sector to ensure that their extensive efforts in this area are encourage and strengthened further.

Further clarification around the term ‘independent risk management function’ is required. The assumption is that this means an internal team within a business, which sits outside of the payment service provision function – is this correct?

Recommendation 2: Risk identification and assessment

Again, whilst we wouldn’t disagree with the need for regular risk identification and assessment, this reflects core PCI requirements and as such could be deemed unnecessary.

Further clarification of 2.1 KC ‘iii) all relevant services offered to customers’ would be appreciated to understand the parameters for interpretation. Further clarification is required as to what is included in 2.3 KC ‘ii) any other information exchanged in the context of transactions conducted via the internet’.

Recommendation 3: Monitoring and reporting

As with the recommendations above, if PSPs are meeting the requirements of PCI, then they should be doing this already and the PCI standards provide a much more detailed set of requirements than is included here. Care should be taken to avoid watering down the PCI requirements.

A definition of ‘card payment schemes’ as referred to in 3.3 KC would be a useful addition to the glossary, as to whether this applies purely to the current global credit card schemes and national debit schemes, or whether it would seek to encompass new players as they seek to enter the market.

Recommendation 4: Risk control and mitigation

This is pure PCI. Concern has been raised about the requirement in 4.5KC for independent audits. As PCI already requires such audits, would these be sufficient or is there going to be an additional requirement for a further audit?

4.7 KC, in our interpretation, could cause significant difficulty in implementation. As an example, if a PSP (who also offers an Acquiring service) has a small merchant as a customer, for example a t-shirt personalisation business, where the website was written by a family member, but the payment process is outsourced to that PSP, then on a literal reading of the key consideration, that merchant would need to comply with the requirements of recommendation 4 in full. Given that the payment service is outsourced to the PSP, and as such, the merchant is not touching the data, then to put such an unnecessary requirement on the merchant seems inappropriate and negates the true value of them seeking to outsource the payment piece in the first place.

Recommendation 5: Traceability

5.1 KC - in addition to the logging of the transaction data, we would recommend that there also be reference to a separate log monitoring system access to the data included in the transaction log.

Recommendation 6: Initial customer identification, information

In principle, the group agrees with the detail of Recommendation 6, providing that 'customer' is defined as 'merchant'.

Recommendation 7: Strong customer authentication

There is concern that this recommendation, as written 'Internet payment services should be initiated by strong customer authentication', does not allow for the risk based approach now being adopted by many payment service providers, which we see as beneficial to both merchants and consumers. For example, the 3D Secure process has been modified by some, so that where a consumer has a particular pattern (e.g. they regularly buy certain types of goods from a certain merchant), then they are not asked to go through 3D Secure to verify their transaction, where that transaction reflects their usual pattern. To move back from this would be regarded as a negative by all involved including consumers.

7.1 KC appears to speak to the concerns raised above, however, it is felt that a re-wording of the recommendation itself to include reference to a more risk based approach would be preferred and would better reflect the risk based approach that is being advocated across the cards and payments industry.

7.2 KC – could further clarity be provided around what might be included within the 'consultative services' discussed here.

Recommendation 8: Enrolment for and provision of strong authentication tools

8.1KC – could examples of 'other secure website offering comparable security features' be provided.

8.2 KC – this appears to contradict 7.1KC, as it says that strong authentication should only be bypassed in 'exceptional cases'. As per the comments made regarding Recommendation 7 above, the market is seeing a quite deliberate shift to a risk based approach for authentication, which is viewed by all as a positive move, and which we believe is undermined if 'exceptional cases' remains included as a term in this key consideration.

Recommendation 11: Protection of sensitive payment data

'Sensitive payment data should be protected when stored, processed and transmitted'. Specifically in relation card payments, this is the essence of PCI and thus, we refer back to points earlier in this document querying the need recommendations which duplicate standards already in place (see back to comments made in relation to Recommendation 1).

Recommendation 14: Verification of payment execution by the customer

'PSPs should provide customers in good time with…' – 'in good time' is open to significantly different levels of interpretation. Greater clarity of definition would be useful in ensuring consistency in application.

We look forward with interest to the outcome of this much needed consultation and affirm Vendorcom's commitment to working constructively with all stakeholders and influencers in the European payments ecosystem.

Yours sincerely
For Vendorcom

Amanda Faul

Programme Director