Nets Denmark A/S
Lautrupbjerg 10
PO Box 500
DK-2750 Ballerup

T +45 44 68 44 68
F +45 44 86 09 30
www.nets.eu

CVR-nr. 20016175

Memorandum Nets' answer to EBA Consultation Paper on the Implementation of its Guidelines on the Security of Internet Payments (EBA/CP/2014/31)

14 November 2014

Response to Consultation Paper EBA/2014/31

Consultation Question

Question as stated in the consultation paper:

Do you prefer for the EBA guidelines a. to enter into force, as consulted, on 1 August 2015 with the substance set out in this consultation paper, which means they would apply during a transitional period until stronger requirements enter into force at a later date under PSD 2 (i.e. a two-step approach); or b. to anticipate these stronger PSD 2 requirements and include them in the final guidelines under PSD 1 that enter into force on 1 August 2015, the substance of which would then continue to apply under PSD 2 (i.e. a one-step approach).

Response:

Nets is in favour of a one-step approach (option b) but with an entry into force date following the PSD 2.

Argumentation:

The two step approach has at least the following weaknesses:

- There is a risk of implementing measures defined in the current guidelines that will not be compliant with future guidelines. Such a risk will impose extra (and unnecessary) cost and workload to PSPs, and potentially also confusion and inconvenience to the consumers and e-merchants.

- The guidelines should be enforceable to all PSPs in the value chain, including payment initiation service providers – the latter

being regulated when the PSD 2 comes into force.

In general Nets prefer to operate under firm guidelines, and not in an environment where assumptions are to be made. We understand that quite a number of issues still are under debate in the PSD 2 regulation, making it uncertain what the outcome will be. Our experience is that such regulation will take at least a year for the PSPs to implement.

We strongly recommend to follow a one-step approach, and that the approach is based on the definitive and final text of the PSD 2 and the implementation date of the Guidelines should take into account an appropriate time frame starting from the effective date of adoption of this text.

General comments and questions

In general it is the opinion of Nets that the guidelines express common sense when handling payment data. Nets welcome a regulation of the area throughout Europe. However, the proposals have so far been missing clarity. When planning how to put the text into an operational context it is difficult to determine whether this is a set of requirements ("must") or guidelines ("should").

PSPs operating in the card payment industry are already regulated by a number of European directives as well as national regulation. PSPs are also expected to comply to a number of security requirements from card organisations as an integral part of standard mandatory operational standards, among these PCI DSS. In order to maintain license to operate in the environment, the PSPs must undergo meticulous PCI certification procedures with regular intervals.

It would be very desirable if the coexistence of these independent sets of rules were somewhat coordinated i.e. by expressing that compliance with PCI DSS would satisfy SecuRe Pay recommandations.

It would have been more fruitful to all parties if this set of already existing regulation and requirements were used as a base and used for giving further guidelines.

As a general remark, the use of the abbreviation PSP seems inaccurate. Sometimes it means credit card issuers solely, sometimes the account holding credit institution, sometimes the transaction capturing entity and sometimes the acquirer.

When the PSD 2 becomes national legislation the PSP will include an even broader variety of market participants.

If a requirement is directed at e.g. a credit card issuer, the abbreviation PSP is perceived much too broad.

It would be a lot more precise if specific terms were used when addressing whom a requirement is aimed at.

Specific comments and questions

The reading of the consultation paper has left Nets with the following questions in addition to areas where Nets find a need for clarification:

Title I – Scope and definitions:

- Par. 1 – states that "These draft guidelines establish a set of minimum requirements……". Kindly, clarify whether the draft is a set of guidelines or requirements?

- Par. 4 – Kindly, clarify whether this paragraph means that the ECB report will still be entering into force 1 February 2015?

- Par. 5 – states "The guidelines constitute minimum expectations" which weaken the document even more. Is it mandatory for a PSP to follow the guidelines/requirements?

- Par. 6 – states that "The purpose of the guidelines are to define common minimum requirements for the internet payment services listed below, irrespective of the access device used:". The second bullet includes execution of credit transfers. To our surprise Par. 10 in the fourth bullet exclude "CTs where a third-party accesses the customer's payment account". In our opinion this will not contribute to a level playing field for the market participants.

- Par. 11 sixth bullet – is a Virtual card equal to a token?

Title II – Draft guidelines on the security of internet payments

- Par. 7.9 – Does this clause also cover Token BINs?

- Par. 7.10 – How does this relate to the PCI requirements?

- The heading “Enrolment for, and provision of, authentication tools and/or software delivered to the customer”. It is unclear whether the customer refers to a merchant or a card holder. Kindly, clarify.