**Main Consultation Question: 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).

Nordea response

Electronic banking services and related technology is subject of rapid technical and operational change. Nordea doesn’t support approach to implement unreleased regulation as a guideline. It is assumed the coming PSD 2 regulation will require fundamental changes in service production. Therefore any premature requirement related to services will cause unnecessary costs and operational risks in the light of the service provision and customer communication.

Nordea does not see any justified ground to set the entry into force 1 August 2015. As a one of the biggest net-bank service providers in Europe we already have schemes to migrate the services to meet Securepay recommendations. However, implementation of these schemes will take relatively long time period. **Therefore Nordea favors option B (one step – approach) provided that entry into force will be adjusted in line with the Final provisions and confirmed implementation time of PSD 2 regulation.**

Other comments

At the page 15 sets general requirement of security policy.

“1.1 The security policy should be properly documented, and regularly reviewed (in line with guideline 2.4) and approved by senior management. It should define security objectives and the risk appetite. “

at the page 28 (Best Practice Examples) indicates (1.1.) The Security Policy could be laid down in a **dedicated document**.

We fully support the need of coherent security documentation. However requirement of one dedicated document is not justified. Internet services are often compilations of wider range of services and therefore the documentation subject to changes. It should be acknowledged that coherent compilation of security policies would be acceptable as well.

**Page 17 process for monitoring**

4.3 PSPs should have appropriate processes in place to monitor, track and restrict access to: i) sensitive payment data, and ii) logical and physical critical resources, such as networks, systems, databases, security modules, etc. PSPs should create, store and analyse appropriate logs and audit trails.

As an example we’d like to point out that this above mentioned requirement is typically an obligation which needs to be elaborated closely in the light of the final provisions of PSD 2 regulations.

**Page 19 Strong Customer authentication**

We assume that these guidelines are based on the assumption that only customers themselves are allowed to use their personalized service credentials. Proper safeguarding of personalized credentials is the utmost important security measure to ensure security also with the internet payments. Until otherwise regulated this approach should be included into the guidelines.

Page 25 – Limits – White lists, black lists

13.1 Prior to providing a customer with internet payment services, PSPs should set limits30 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. (Also in the 13.3. at the page 29 examples of best practice)

Nordea is of the opinion that payment services in general should support multi-channel approach. Therefore any channel specific limitations etc. are costly and may not interact with the other channels.

Given that the scope of these guidelines is targeted merely to internet payments an exhaustive review of other channels and actual benefits of such detailed requirements should be executed before adopting these kinds of requirements to the guidelines.