FK | Finanssialan Keskusliitto
FC | Finansbranschens Centralförbund
FFI | Federation of Finnish Financial Services

20 June 2012

Respondent's details	
Name:	*Federation of Finnish Financial Services*
Address:	*Bulevardi 28, FIN-00120 Helsinki, Finland*
Contact persons:	*Mr Mika Linna, e-mail mika.linna@fkl.fi, tel. +358 20 793 4269 or Mr Pekka Laaksonen, e-mail pekka.laaksonen@fkl.fi, tel. +358 20 793 4298*
Business profile:	*Federation of Finnish Financial Services is a trade association representing banks, insurers, finance houses, securities dealers, fund management companies and financial employers operating in Finland. FFI has about 450 member organisations with a total of 43,000employees.*

FEDERATION OF FINNISH FINANCIAL SERVICES' RESPONSE TO CONSULTATION ON THE ECB DRAFT RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS

Federation of Finnish Financial Services ("FFI") welcomes the opportunity to comment on the Consultation on the ECB Draft Recommendations for the Security of Internet Payments ("Recommendations").

FFI shares the ECB's objective to increase the security of internet payments for customers (including both the consumer and the merchant) while not suppressing competition and innovation. However, to achieve this there are several aspects to be taken into account, including:

- Competition, openness and faster product and technical innovation should be supported;
- Internet payments are global, and the relevant security recommendations and standards should be global, as well;
- Regulation, implementation and supervision of any new recommendations or standards should take into account actions already taken on a national level on the basis of global initiatives, recommendations and standards;
- Multiple or overlapping recommendations or standards should be avoided;
- Responsibility on the security of internet payments should not be left on the banks' sole responsibility alone, but it should be distributed across the entire commercial value chain, including the end-users;
- Any new standards or recommendations and any ensuing national activities for regulation or supervision should ensure full transparency, equal treatment and level playing field for all stakeholders in the value chain and between all Payment Service Providers (PSPs);
- Actions by the national supervisory authorities should be aligned at the EU/EEA level.
- The effects and implications of amendments to the Payment Services Directive (PSD) are carefully examined and assessed before a formal legislative process is initiated.

Finanssialan Keskusliitto ry
Bulevardi 28, FI-00120 Helsinki
Puh: 020 793 4200
Faksi: 020 793 4202
etunimi.sukunimi@fkl.fi

Federation of Finnish Financial Services
Bulevardi 28, FI-00120 Helsinki
Tel: +358 20 793 4200
Fax: +358 20 793 4202
firstname.lastname@fkl.fi
www.fkl.fi

1 Scope of the Recommendations

The overall scope of the Recommendations is very comprehensive and main issues concerning security of internet payments are covered. In general, FFI supports the Recommendations and welcomes the notion of fostering the establishment of a harmonised EU/EEA-wide minimum level of security. FFI fully supports the goal of uniform recommendations and standards for all participants linked to the internet payment chain.

However, in FFI's view the scope, the substance and the implications of the Recommendations pose several questions about the consequences and the actual impact to different stakeholders:

- The Recommendations underscore the significance of internet payment services as a distinct risk area. This requirement would appear to be in conflict with the approach adopted by risk management frameworks such as Basel II, COSO ERM and ISO 31000, which all emphasise the importance of creating a uniform view on risk across the organisation. Some of the risks most significant to payment services originate from outside of the payment services infrastructure and can be dealt with effectively only by ensuring that the entire corporate infrastructure is adequately protected.

- Most PSPs at which the Recommendations are have already made invested substantial investments in implementing the prevailing security recommendations, standards and frameworks. Introduction of new binding rules could unfairly penalise these PSPs by forcing them to change their current practices. To avoid this, it should made very clear how the Recommendations would relate to other standards widely adopted by the PSPs (e.g., PCI/DSS, ISO 27001, COBIT, and ITIL).

- The Recommendations fail to take adequate account of the most vulnerable links in the payment value chain, in other words merchants and consumers. In fact, it is right here that the most critical incidents of late have happened, not with major banks or other PSPs.

- In order to ensure a level playing field for all parties involved, the Recommendations and their subsequent implementation should target the entire chain. In addition to consumers and merchants, these parties would include at least service providers, service integrators and other businesses, as well as the public sector.

- Finally, although the challenges are global, application of the Recommendations would be restricted to EU/EEA-area only. This could leave the PSPs within the EU/EEA on an inferior competitive footing as compared to their global peers. Therefore, FFI would very much prefer a global approach over the regional approach suggested by the Recommendations.

2 Need for Recommendations

FFI raises the question about the actual need for the Recommendations because they seem to be directed at PSPs already strictly regulated and supervised. It also seems to be overlapping with other security standards, recommendations and frameworks already adopted by the PSPs. For instance, in Finland the recommendations of the Basel Committee and the Committee on Payment and Settlement Systems have been implemented as binding regulations by the Finnish Financial Supervisory Authority (FIN-FSA)[1]. In addition,

[1] See for instance, FIN-FSA, Standard 4.4b on Management on Operational Risk, http://www.finanssivalvonta.fi/en/Regulation/Regulations/Financial_sector/4_Capital_adequacy_and_risk_management/Pages/4_4b.aspx. Section 6.7 of the Standard (Information security) is based on the Basel Committee's recommendation Risk Management Principles for Electronic Banking (Basel Committee Publications No. 98 issued in July 2003). Section 6.8 of the Standard (Payment systems and services) is based on Core Principles for Systemically Important Payment Systems issued by the Committee on Payment and Settlement Systems (CPSS Publications No. 43, January 2001).

international information security standards (including PCI/DSS, ISO 27001, COBIT and ITIL) are commonly adopted by the Finnish PSPs.

It should also be noted that a payment encompasses only a limited part of the services provided in the internet. Therefore, to be effective, information security recommendations and standards, including internet security, should cover all participants and stakeholders in the value chain and put specific focus on those parties who have obvious deficiencies their information security practices. These weakest links pose the greatest security threats and risks, and the most lucrative target to fraudsters. As it stands today and likely in the foreseeable future as well, the successful attacks are not launched against the banks' systems but the ones of end-users.

To put the problem in the right perspective, the Recommendations should be targeted at those issues which are most relevant from the fraud prevention perspective. To identify these and to verify the magnitude of the problem, hard data in the form of crime and loss statistics should be used.

3 Actual Problems and Challenges

Security of internet payments falls upon several value chain actors, roles and layers. Majority of the challenges and risks related to the internet payment security originate from outside of the actual payments space. As the recent incidents suggest, the major vulnerabilities are on the end-users, side (i.e., consumers, other customers and merchants).

Bank systems are designed to be secure and robust, and are immensely difficult to hack into. Therefore, card numbers and other sensitive personal information held by, e.g., merchants in their own systems has become an alluring target for fraudsters. Attention should also be paid to customer awareness and behaviour, since this part of the payments chain is out of PSPs' reach and control.

4 Level Playing Field

In FFI's view it vital that the requirements, rules and regulations for safe and reliable internet payments should apply equally to all market participants involved in the internet payment chain (in other words, not only to PSPs but also to merchants, customers, non-regulated service providers and all other parties, as applicable). The role of the national supervisory authorities in adoption, interpretation and enforcement of the Recommendations in a harmonised and uniform way, is critical.

FFI would like to point out that the Recommendations would not applicable outside the EU/EEA. For this reason, FFI would very much prefer a global approach over the regional approach suggested by the Recommendations.

However, should final Recommendations be issued, it should be ensured that the competitiveness of PSPs within the EU/EEA is not weakened vis-à-vis their global peers.

5 Legal Implications

Obligations and legal implications imposed on PSPs deserve in-depth evaluation and impact assessment. Failure to comply with obligations set by applicable law and/or regulations may create a legal presumption that the resulting payment order is not authorised, and hence the PSP is held liable, while the customer's liability is strongly limited.

While FFI fully supports the suggestion that there is a need for greater harmonisation in the implementation of rules on liability, and also shares the view that liabilities of PSPs and the payment service users must be

linked to the proper adoption and implementation of security measures, FFI also stresses the utmost caution in changing the provisions of the PSD and, in particular, in extending the scope of the Directive.

Any extension of the scope of the PSD to cover one leg -transactions would cause great complexity, uncertainty and additional costs to PSPs. It should be remembered that PSPs outside the EU/EEA are not regulated under the PSD. Therefore, there are no enforcement mechanisms in place to ensure that the provisions are being complied with. Some of the requirements may also be in contravention of national legislation and regulations of the non-EU/EEA countries, which in these circumstances would take precedence over the EU/EEA regulations.

The potential inclusion of transactions in non-EU/EEA currencies would add a significant element of extra-territoriality, as the final settlement of non-EU/EEA currencies takes place in the home country of the currency (e.g. US Dollar is settled in the USA). Inclusion may also hamper PSPs' effective liquidity management, as well as management of credit, country and currency risks. Because these risks have to be covered in accordance with the solvency requirements, increased risk level would ultimately have an effect on customer charges and fees, as well.

FFI also wishes to refer to a recent study by the Bank of Finland (BoF Online 7/2011, 23 Dec 2011) which shows that the costs on retail payments are heavily subsidised by the banks' income from interest margin revenues and other loan client fees. The substantial increase of PSPs' costs of providing payment accounts and payment services, while simultaneously preventing cost recovery from the users of those services would inevitably lead to increased pressure towards, e.g., higher interest rate marginal for mortgage and loan customers already under heavy pressure due to the Basel III requirements. This would leave the PSPs within the EU/EEA on an inferior competitive footing as compared to their global peers. At any case, the scope should not be extended to one-leg transactions without appropriate, comprehensive and in-depth impact assessment.

Finally, FFI wishes to point out that limitations of liability may in practice lead to moral hazard and malpractice by the payment service users. For example, in Finland, there have several payment card cases which indicate that the limited responsibility of the user is more likely to encourage more negligent user behaviour than preventing it (regardless of Article 56).

FEDERATION OF FINNISH FINANCIAL SERVICES

Päivi Pelkonen