Comments on the Recommendations for the Security of Internet Payments

Bank of Finland Payment Forum
Helsinki, 10 May 2012

Mika Linna
Federation of Finnish Financial Services

FFI | Federation of Finnish Financial Services

Principle 1: Specific and regularly updated assessment of risks

1) **Governance**
2) **Risk identification and assessment**
3) **Monitoring and reporting**
4) **Risk control and mitigation**
5) **Traceability**

- To large extent reiterates requirements already in Basel II, etc.
- Siloed vs. integrated approach to risk
- Central vs. coordinated monitoring, reporting and follow-up of incidents
- Value of customer complaints as a risk indicator?
- Multiple layers of security – both technical and administrative controls are needed
- Appropriate tracing of all transactions

Principle 2: Strong customer authentication

6) Initial customer identification

7) Strong customer authentication

8) Provision of strong authentication tools

9) Log-in attempts, session time-out, validity of authentication

- Know-Your-Customer requirements in relation to Anti-Money Laundering
- What is 'adequate', 'prior' and 'regular' information?
- PSP's duty to inform vs. customer's responsibility to know the law?

Principle 3: Transaction monitoring and authorisation

10) Transaction monitoring and authorisation

11) Protection of sensitive payment data

- Multiple monitoring requirements:
  - Fraud detection
  - AML monitoring
  - CTF / Sanctions monitoring
- Conflicting reporting requirements
- Multiple data protection requirements:
  - Sensitive payment data
  - Bank confidential customer data
  - Protection of personal data under privacy laws

Principle 4: Customer awareness and education

12) Customer education and communication

13) Notifications, limits

14) Verification of payment by customer

- Established PSPs have been acting responsibly and will continue to do so
- What are the roles and responsibilities of:
  - Government?
  - Internet service providers?
  - Software providers?
  - Critical infrastructure providers?
  - Customers themselves?
- How about the emerging new players?

In conclusion…

> Robust set of requirements and good practices

> Annex 2 deserves particular attention

> Implementation wise:
- One size won't fit all
- Standalone or integrated approach ?
- What other obligations / requirements / commitments must be taken into account ?
- Make use of "comply or explain" principle