

The future of retail payments:
Opportunities and challenges,
ECB and OENB,
Vienna



Discussant comments on Fraud, Investments and Liability Regimes in Payment Platforms

12 May 2011
Harry Leinonen

The views expressed are those of the author and do not necessarily reflect
the views of the Bank of Finland.

**Liability regime differences can be used by
monopolistic payment platforms
to promote merchants security investments and
extract rents from merchants.**

**Modeling the real life issue of EMV card investment
versus magnetic stripe fraud?**

EMV chip card implementation is a good example of the required joint security cooperation

- ◆ Card manufactures must introduce chip cards as a new security technology
- ◆ Issuers must distribute new cards to cardholders
- ◆ Cardholders must learn to use card and PIN
- ◆ ATM and POS terminal equipments need to be developed
- ◆ Banks and merchants must install new or update old ATMs and POS-terminals
- ◆ Acquiring and interbank networks need to be updated to carry new data fields

Often all stakeholders need to participate in security technology updates in a coordinated way, which puts an emphasis on suitable incentives (one uninterested party can hinder the update)

Transaction type and security measure -based merchant liabilities have frequently been used in card payment schemes

- ◆ Authorization call/transaction requirement for given transactions
- ◆ Customer identification requirement for large transactions
- ◆ PIN-requirement for larger transactions (card-only for low value)
- ◆ Larger liability for mag-stripe than EMV-based transactions
- ◆ Larger liability for card-not-present transactions

Merchants know their customers and can affect overall losses by implementing and employing different kinds of security measures

Suitable incentives can support merchants' loss-reduction efforts

Social planner's viewpoint

Total fraud loss reduction > Total (overall stakeholders')

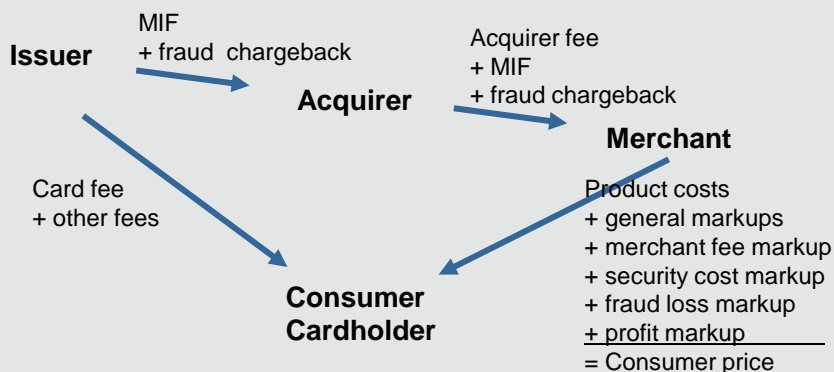
Interesting situation when investment profitability depends on merchant volume, business type etc

security investments
+ security operational costs
+/- foregone/changed business benefits

Generally too costly to abolish fraud losses completely

Criminals learn over time to circumvent existing Fraud-controlling measures, so at some point implementing new ones will be required/rewarding (current chip card generation level 3+)

In the end, ordinary consumers pay all fraud and fraud-prevention costs (just as they pay for shoplifting and shoplifting prevention costs)



Service providers transfer all their costs to consumers as visible or non-visible markups (social planner viewpoint= consumer viewpoint)

Consumer/cardholder will select payment instrument based on visible differences



Embedded markups will hide security-cost differences from consumers/cardholders. Transparent fees and surcharging would promote payment-habit changes.

Merchants will also react to transparent cost differences, ie it will be difficult to make merchants invest, when the result would be increased overall merchant costs, implying higher price markups (merchants view the situation based on long-term volume assessments)

Methodological comments

- ◆ Fraud loss seldom lump sum- mostly transaction size-based
- ◆ Monopolist issuers set prices independent of costs when $p^{opt} > c$
- ◆ Monopolist merchants set prices independent of costs when $p^{opt} > c$
- ◆ Monopolists minimize security investments and fraud costs separately from charges, especially when non-transparent
- ◆ Merchants in competition need to mark up for security costs
- ◆ Payment game is continuous with long-term investments, “profitable fraud possibilities” attract criminals and fraud costs increase over time without investments (Should forgers be included in the model?)
- ◆ Merchants have no interest to disinvest long-term sunk costs
- ◆ Merchant heterogeneity: volume, customer, transaction dependence
- ◆ Individual customer instrument choice and individual merchant terminal investments have marginal impact and are not correlated, especially for security feature updates

Liability schemes can be used to promote security or abused to extract monopoly gains

**All payment instruments
carry risks of fraud,**

**fraud prevention always implies
an extra cost burden,**

**with high probability, current non-transparent
fraud cost distribution convention is non-optimal,
resulting in delayed security investments,**

**implying that customers
use more cash and less cards
compared to optimal situation,**

**and may call for authority (social planner)
intervention to promote security investments.**