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

EUROJÄRJESTELMÄ
EUROSYSTEMET

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 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 mg-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')

security investments

+ security operational costs

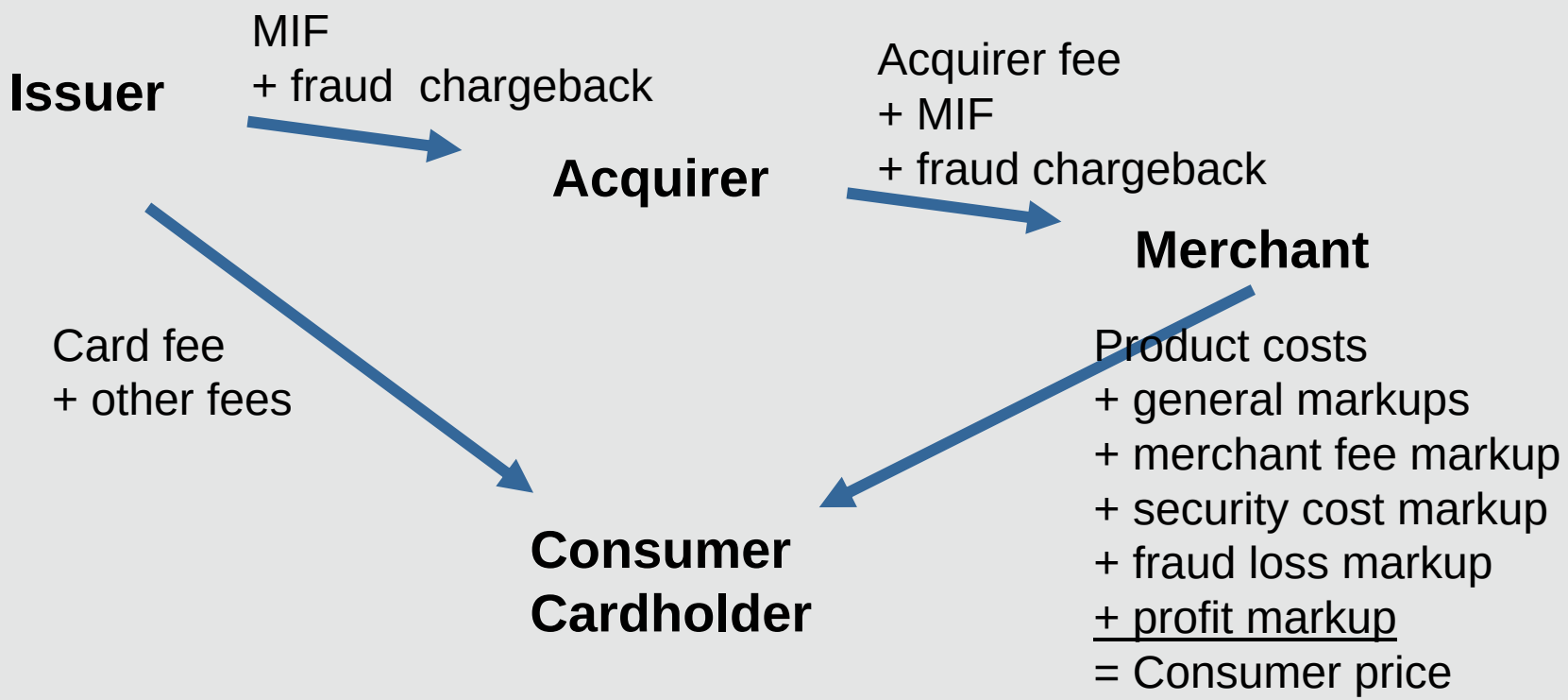
+/- foregone/changed business benefits

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

Generally too costly to abolish fraud losses completely

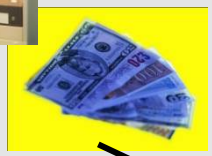
Criminals learn over time to circumvent existing Fraud-controlling measures, so at some point implementing new ones will be required/rewarding (current chip card generation level 3+)

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



Bank account usage

Go to ATM

Take cash to shop

Zero consumer liability = consumers without liability for security breaches in system security, which have hit them at random without fault from their side

Pay in shop Directly with card

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

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.

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

EUROJÄRJESTELMÄ
EUROSYSTEMET

Discussant comments on Do newspaper articles on card fraud affect debit card usage?

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.

Based on daily
ATM and EFTPOS volumes and
published newspaper articles on card fraud

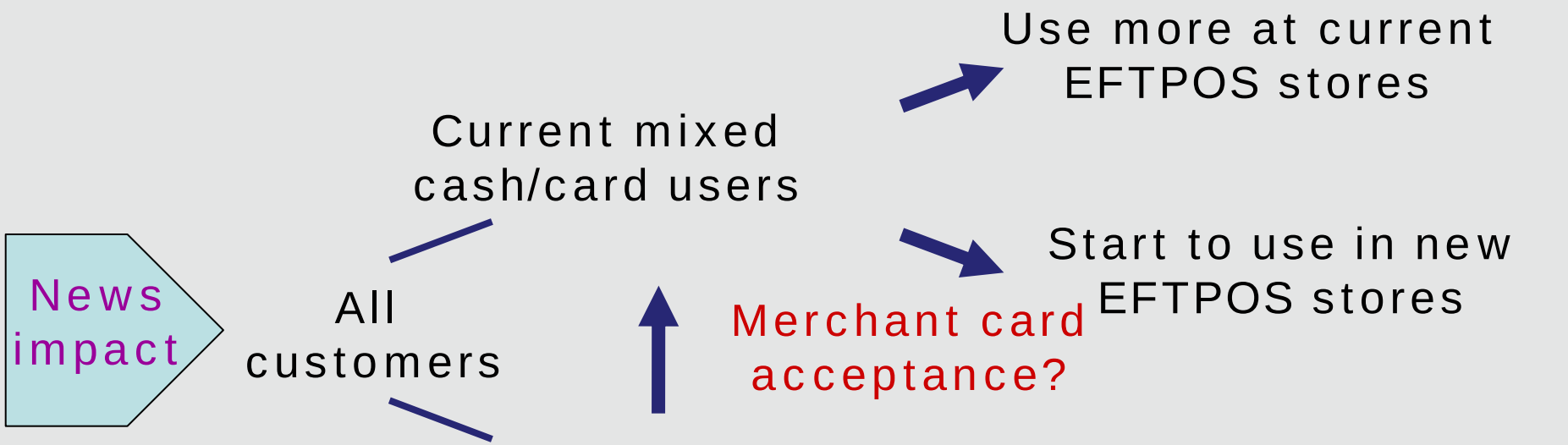
a statistical effect is found
which lasts for one day
and implies that

an ATM fraud/skimming article
increases EFTPOS usage by 1.1% the next day
but reverts the following day

an EFTPOS fraud/skimming article
decreases EFTPOS usage by 0.8% during
publication day but reverts the next day

= about 50 000 transactions less on impact day
= 3 of 1000 inhabitants react

The debit card / EFTPOS growth patterns and possible news impact



Effect on cash-only users?
Postponement of card usage?

Effect on merchant interest?
Postponement of terminal investments?

Longer-lasting effects?

What would long-term growth have been without the impact of risk news?

According to a Finnish study
customers are very security sensitive
when deciding to start to use new instruments
(BoF DP 32/2008 Dahlberg-Öörni)

suggesting that the largest delaying effects
will be found among non-card/cash-only users

Difficulty to control other factors with similar impact in statistical correlation studies

- News on cash robberies and other cash-related crimes?
- Card-promoting news in newspapers?
- Banks' card-promoting marketing campaigns?

- Customers' skimming liabilities = zero, Do they mind?
- Do they see a difference between ATM and EFTPOS skimming?

- Banks push skimming news in order to activate higher customer alertness to skimming devices?
- EMV cards have removed skimming possibilities?

Is the finding a real causal relationship or just coinciding developments due to other factors?

Some methodological comments

- Weighting newspaper articles according population coverage
- Weighting rainfall according to business hours and strength (eg light summer rains bring customers to shops)
- Checking for true randomness of publication days (news papers have publication patterns which may coincide with daily fluctuations of purchase patterns)
- Checking for payday patterns, other than monthly
- NL is a small country with lots of commuters
- Plot diagrams of impact strength

The differences are rather small and small changes in the parameters could affect the results considerably (just 3 out of 1000)

Further research suggestions

- Checking with direct customer questionnaires that the statistical correlation is causal for current card customers
- Checking how the impact varies across merchant types (daily purchases, large-value purchases, web-purchases etc…)
- Checking the delaying impact on cash-only customers and the difference between ATM and OTC cash customers
- Checking the impact of news published on consecutive days
- Building a robust model for main external factors affecting ATM and EFTPOS daily usage fluctuations

Interesting micro-data -based data-mining research

Personally skeptical about causal effect:

card customers read morning paper
covering skimming news and

about 3 of 1000 decides

that today I will by my gasoline
and/or lunch with cash
instead of the usual card,
but tomorrow no card risk?