Topics of this issue:

1. **Proposed regulation of the Australian ATM scheme**
2. **Dutch retailers' vision of application selection**
3. **A court decision in favour of MasterCard**
4. **The 'payment account': guidance from the EU commission**
5. **Costs of data breaches: Figures from the U.S.**

1. Proposed regulation of the Australian ATM scheme

The Reserve Bank of Australia (RBA) has decided to regulate the Australian ATM system and has published a "Draft Access Regime for the ATM System".[1] The contemplated regulation is meant to support industry-based efforts to improve competition and efficiency in the ATM system. The main elements of the reform package include:

- the abolition of bilateral interchange fees (paid by issuers to ATM owners) and the introduction of a common interchange of zero
- the introduction of the possibility to surcharge cardholders directly
- the introduction of an Access Code regulating entry of new players

There are exceptions to these rules, however. Sub-networks of smaller banks may keep an interchange. In cases where small banks have negotiated access to the network of a larger bank the two banks may agree on an interbank fee and correspondingly no surcharges for the customers of the small bank.

There is only a brief consultation period after which the new regulation shall be put into force (in March 2009). Going beyond the proposed regulation is the requirement that banks change the basic structure of the ATM system. The current system is based on bi-lateral links and the RBA favours a more centralised system.

Our Comment

Australia may be far away from SEPA but the Australian central bank (the RBA) has been something like a front runner in payment card regulation. So, its current move will be closely watched by regulators all over the world.

[1] See http://www.rba.gov.au/PaymentsSystem/Reforms/ATM/ConsultDocDec2008/a_consultation_doc_122008.pdf

The decision of the RBA has been driven by concerns regarding the efficiency and openness of the current system. The Australian ATM system has developed via linking bi-laterally the ATM systems of individual banks (and some groups of small banks).[2]

The move away from interchange to surcharges has been driven by concerns regarding efficiency. The RBA wants price competition between ATM deployers and it wants the right incentives for ATM deployers to put ATMs where card holders need them.

The Australian ATM regime has a lot in common with the regimes in the UK and in Holland

- *common interchange (AU: zero, UK and NL: cost based)*
- *possibility to surcharge*
- *regulatory guidelines for entry*

Moreover, in the UK and Holland, ATM acquirers have to choose between interchange and surcharge. Both countries also restrict double charging of card holders.

Thus, on the whole there are some common elements that might serve as a blue print for future ATM regulation in other countries:

- *common interchange (zero or cost-based)*
- *possibility to surcharge*
- *transparent access regime and*
- *possibly, rules restricting double charging.*

In Europe, recent payment card regulation has been focussing mostly on card payments at the POS. Cash withdrawals at ATMs have been less of an issue. But in some countries, notable Germany, interbank pricing of ATM cash withdrawals has become a hot topic. When looking for a better framework, those in charge of setting the rules might well look at the UK, Holland or the emerging new framework in Australia.

2. Dutch retailers' vision of application selection

The Platform Detailhandel Nederland, a joint venture of Dutch Retail Council and The National Council of Shops of MKB-Nederland, has published a "work plan 2009" that also touches the issue of application selection at the POS.[3]

[2] ATMs of independent deployers are usually linked into the system through one of the banks.
[3] See Platform Detailhandel, Werkplan 2009
http://www.platformdetailhandel.nl/index.cfm/28,551,c,html/Werkplan%202009.pdf

As Dutch retailers point out, it will be a burden for card holders to select between different applications based on one card. Card holders are not aware of price differences. Therefore, Dutch retailers want terminal suppliers to develop a standard terminal application that allows merchants to determine the selection of the card application.

Our comment:

We have repeatedly pointed at that application selection at the point of sale is bound to become a controversial issue. The SEPA Cards Framework includes the provision that card holders should decide. However, both, issuing banks and merchants agree that this does not seem practical. At this point, the agreement ends. When it comes to the question who should decide, if not the cardholder, the opinions go in opposite directions: merchants think they should decide and issuer think that they should have the right to select the application.

For Dutch retailers, a lot is at stake. So far, they have agreed to promote, for instance with tv commercials, the use of PINpas, the Dutch domestic debit card even for small values. This agreement is based on the idea to promote efficiency in POS payments and on the belief of all stakeholders, that PIN is actually more efficient than cash payments. Many cost studies have been performed to confirm this belief. Actually, the success of PIN is impressive with transactions reaching 1.76 bn in 2008 (+10.6%). According to Currence, PIN payments are gaining a share of 32% of total POS payments, 19% of small value payments < 20 EUR and, according to DNB[4], even 5% of payments below 5 EUR.

However, growing use of PIN scheme may increase card dependence of retailers. Obviously an application selection by the cardholder or the issuer bank would provide an incentive for banks to switch to issuing Maestro and V PAY cards. If banks should move into this direction retailers would be 'locked in' and there would be price increases 'through the backdoor'.

Therefore the issue of application selection is of highest strategic importance. It will be interesting to see how the Dutch banks will react. If this issue cannot be solved in a way that is acceptable to both parties, the co-operative way to develop retail payments in the Netherlands might come to an end. This could harm the attempts to steer payment behaviour into a cost-efficient direction.

[4] http://www.dnb.nl/binaries/Working%20paper%20196_tcm46-210266.pdf

3. A court decision in favour of MasterCard

After the settlement with Wal-Mart, a class-action law suit was filed against MasterCard and others over interchange fees. When deciding the potential damages, the judges decided that the period under consideration should start with the date of the MasterCard settlement. An open issue was whether this period should end with the MasterCard IPO in May 2006. Merchants argued that the IPO was only carried out to avoid damages. However, in November 2008, a court decided that with the IPO, banks could no longer control interchange rates.[5] Thus, such rates could no longer be seen as a breach of anti-trust law.

Our comment:

Again, the news reported comes from oversees. But, the decision of the US court is also very interesting for the EU. The US judge deciding the case has rejected the retailers' argument that even after the IPO, the credit card schemes are mechanisms to co-ordinate the decisions of member banks on interchange fees. Thus, he rejected the view that there still is a kind of issuer cartel behind MasterCard (and Visa). This decision has to be seen against the current court case in the EU. In its MasterCard decision, the EU Commission has argued (like the American merchants) that even after the IPO, issuing banks still have a major influence on interchange fees and that therefore European anti-trust law against collusive price setting has to be applied. Should the European Court of Justice see things like American judges, MasterCard would stand to win its case against the EU Commission.

Another hopeful event for the card schemes was the decision of Poland's Appeals Court for Competition and Consumer Protection that ruled in favour of Polish banks in an interchange case.[6] Our Polish EPCA partner will report on this case in the next EPSM Newsletter.

4. The 'payment account': guidance from the EU commission

As pointed out already in this newsletter, there are substantial differences in interpreting the meaning of the term 'payment account', run by Payment Institutions after implementation of the PSD in November 2009. In the UK, the payment account is interpreted as a kind of internal account for funds that are en route from payer to payee. German law makers, however, have interpreted the payment account that could be offered by a Payment

[5] See 'MasterCard victory in court', Nilson Report 916, December 2008.
[6] http://www.ksplegal.pl/userfiles/Poland%20loses%20interchange%20appeal.pdf

Institution as a 'giro account light'. We presented the issue to the EU Commission on their Q&A website and the answer has now been published.[7] The EU Commission basically confirms the view of the UK that payment accounts are required to hold funds that are held by a payment service provider due to the fact that execution of payment may take time: The Commission stresses, that these funds should not be held longer than is necessary 'due to operational and technical reasons'.

Our comment:

The German draft for transposing the PSD has reached a fairly advanced state in the law making process. Thus, it is not unlikely that the current interpretation of the term 'payment account' will become effective as of November 2009. If other European law makers follow the interpretation of the EU Commission Germany would have a much more liberal regime for payment institutions than the rest of the EU. Payment institutions with a German license could offer limited purpose payment accounts whereas payment institutions licensed in other countries could not. So, whereas the UK is the country of choice for European e-money institutions, Germany might become the first port of call for European payment institutions.

5. Costs of data breaches: Figures from the U.S.

In the U.S, there have been a number of high profile data breaches (TJX, Hannaford, CardSystems) and many more that received less attention. Little by little, figures on the costs for retailers and processors are being published.

One element of costs are fines that are levied by the schemes. According to a recent publication, such fines have ranged from 64 cents per card breached (TJX) to about 100 US$ (for a small restaurant).[8]

More important than scheme fines are the costs incurred by issuers that ultimately have to be borne by merchants (or acquirers if merchants are unable to pay). According to a study of the 'Bureau of Financial Institutions in the State of Maine', costs of reporting institutes were in the

[7] European Commission, Your questions on PSD, Payment Services Directive 2007/64/EC, Questions and answers, p. 131. http://ec.europa.eu/internal_market/payments/docs/framework/transposition/faq-2009_01_27_en.pdf

[8] See Musante, Ken: Why PCI Fines Need to be Fine-Tuned, Digital Transaction News, July 2008. www.digitaltransactions.net/files/0708acq.doc

range of 7,50 US$ to almost 10 US$.[9] Luckily, for retailers, a surprisingly large part of cards did not have to be re-issued.

Our comment:

For card accepting retailers, data security seems to become an issuer of increasing frustrations. Retailers are forced to undertake large investments. But the benefits are not always clear. Thus, a retailer may be 'PCI compliant' but still face high costs. Apart from managing the crisis after a data breach and searching for the short-comings in the internal IT, there are the costs of the issuers and the fees to be paid to the card schemes. So far, no one seems to be able to show a way that provides an acceptable mix of costs and security. Thus, the question may be permitted whether it is not time to re-design the system in a way that makes it unnecessary to store crucial data in many places. Retailers, in particular, would be relived with fewer obligations regarding data storage.

That much is clear, data breaches are bound to be a fact of life – as witnessed by the first big data breach of 2009 (this time again hitting a processor).[10]

[9] See ‚Issuer costs from data breaches', Nilson Report 917, January 2009.
[10] See 'PCI and the Heartland Payments Breach',
http://www.knowpci.com/index.php?option=com_content&task=view&id=70&Itemid=100

Should you have any questions or comments please contact

Dr. Hugo Godschalk (hgodschalk@paysys.de)

Dr. Malte Krueger (mkrueger@paysys.de)

Christoph Strauch (cstrauch@paysys.de)

PaySys Consultancy GmbH

Im Uhrig 7
60433 Frankfurt / Germany
Tel.: +49 (0) 69 / 95 11 77 0
Fax.: +49 (0) 69 / 52 10 90
e mail: info@paysys.de
www.paysys.de

PaySys Consultancy is German member of

epca
european payments consulting association

Subscription info: The PaySys SEPA-Newsletter is published 10 times a year in English in electronic format (pdf) and contains about 4-6 pages. The price is
- 250 EUR per year (single user license)
- 500 EUR per year (company license)

To order, please send an email to Sepa-newsletter@paysys.de indicating the type of license you wish to purchase and the method of payments (credit transfer or credit card).

Disclaimer: PaySys Consultancy sees to the utmost reliability of its news products. Never-the-less, we do not accept any responsibility for any possible inaccuracies.