THE PAYMENT CARD FRAUD IN HUNGARY

2001

June 2002

1 Introduction

Problems caused by rises both in the number of fraudulent activity and the resulting losses have been mounting world-wide. There has been a jump particularly in the use of counterfeit cards, which has prompted international card associations to encourage their member banks to switch to chip technology. The three major international card associations have jointly developed the EMV standard which ensures the technical background for mutually acquiring cards which carry a chip satisfying the criteria on ATM and POS devices that in turn are equipped with the card processor meeting the EMV standard. According to the latest news, Visa and Europay have set 1 January 2006 and 1 January 2005, respectively as the final deadline for their member banks – following these dates, any loss arising from fraud in international payments will have to be borne by the country that has not ensured conditions for reading chip cards on ATM and POS terminals or has failed to supply payment cards with EMV chips, irrespective of the fact whether it could pass losses on to another country, due to the circumstances of fraud.

Internationally, the second most common type of fraud is committed using cards reported lost or stolen. The use of PIN codes have been made compulsory at POS terminals for certain brands (for example Cirrus/Maestro), in order to hold down the occurrence of this type of card fraud. However, there are examples, irrespective of the type of card, for the compulsory use of the secret code in both ATM and POS transactions. In France, where bank cards were equipped with safety chips ten years ago, PIN codes must be entered in every transaction. Another country, where work to introduce the joint use of chips and PIN codes is currently underway, is Great Britain.

‘Card not present’ fraud ranks third. This typically occurs on the payment side of e-commerce, where the customer provides the number of his card to the retail trader. In order to protect against this type of fraud, the customer either confirms the purchase via his mobile phone, or identifies himself with an electronic signature. This may be stored by the chip on the bank card or by a SIM card of a mobile phone.

2 Fraudulent activity and value of losses in the Hungarian card business

In this report, fraudulent activity and the value of losses arising in the domestic bank card business are analysed in two categories:

- The first category comprises fraudulent activity and the value of losses arising in the issuing business (point 2.1.), i.e. fraud committed in Hungary and abroad with cards issued by domestic banks. This category also includes fraud and losses arising in on-us turnover, i.e. those suffered in transactions conducted in the issuing bank's own network using the bank's own card.

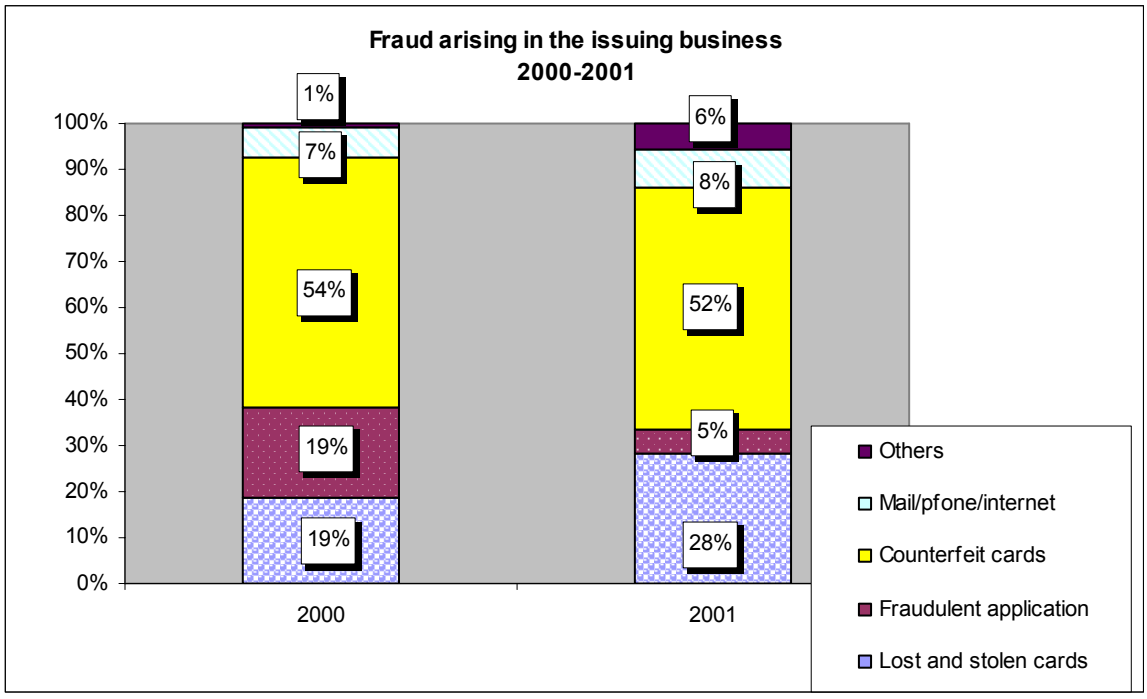
- The second category comprises fraudulent activity and the value of losses arising in the acquiring business (point 2.2), i.e. fraud committed using domestically- and foreign-issued cards in Hungary. Losses incurred in transactions using the acquiring bank's own cards in its own network (in on-us turnover) are not covered by this point of the analysis.

2.1 Fraudulent activity and the value of losses in the issuing business

2.1.1 Value and distribution of fraudulent activity

A total number of 6,000 fraudulent acts using domestically issued bank cards were committed in 2001, in a value of HUF 233 million. This accounted for 0.009% of total value of transactions realised by Hungarian issued bank cards. Deducting the amount of overdrawing on accounts from 2000 data (as it is not included in 2001 data, given that it is a type of abuse which is not related typically to a bank card), the value of losses relative to total turnover fell last year, though only slightly, by 0.001%. This meant a mere HUF 46,000 fall in absolute terms.

The following Chart shows developments in 2001 relative to 2000:



Note: In 2000, the category of 'fraudulent application' was complemented with other fraudulent activities committed by the rightful holder of the card. In 2001, these latter were transposed to the category 'other acts of fraud'.

The Chart clearly shows that, although their proportion fell slightly, more than a half of fraudulent acts was committed using counterfeit cards in 2001. Domestic banks, with help from international card associations, are making preparations for the switch from the magnetic stripe to chip technology, in

order to combat counterfeiting of cards. However, banks are not united in estimating the costs and benefits of such a transition. Many domestic participants believe that the costs of investment would be far higher than the value of write-offs caused by fraud. This division of views is also observable internationally. The costs of replacing cards and adjusting ATM and POS terminals are high indeed (in Great Britain, the total cost of supplying the more than 100 million cards with chips and making the 750,000 POS and 35,000 ATM terminals suitable for reading the chips is estimated to be £1.1 billion[1]); however, the investment could be made more profitable, if the chip was used for other purposes as well. In addition to enhancing safety, it could be used to store the electronic signature used in e-banking and e-commerce, or to store the electronic purse function used for small-value, bulk payments, to collect customer loyalty points in shopping, and, for example, to register the code belonging to the security system of dwellings. Such a diversity of use may share the costs which otherwise seem too high.

The second most frequent type of fraud is using cards stolen or lost. As fraudulent activity with lost and stolen cards was not separated in the analysis for 2000, the data for last year have also been aggregated in the Chart, in order to ensure comparability. As can be seen, there was a significant increase in occurrence of this type of fraud in 2001 relative to the previous year, which underscores the importance of introducing the use of PIN code in POS devices. This, however, carries the danger that, in addition to the copied magnetic stripe, the chance to steal the code as well could be greater, and the counterfeit card could be suitable for use in electronic environment too. Among other reasons, this is why it may be useful for the issuer bank to ascertain in each case, via a mobile call or an SMS message, whether the rightful holder of the card is making the transaction. A number of banks have already been using this practice.

The Chart is evidence of a significant drop in fraudulent applications. As the note below the Chart explains, however, this stems from a revision to the classification last year, with a resulting change in the contents as well. In 2000, fraudulent applications and other acts of fraud committed by the rightful holder were recorded collectively under one category. In the year of 2001 fraudulent applications have been treated as a separate category, and all other acts of fraud committed by the rightful holder have been taken into the category of other acts of fraud. This explains the rise in the proportion of the category ‘Other’ in the upper range of the column chart.

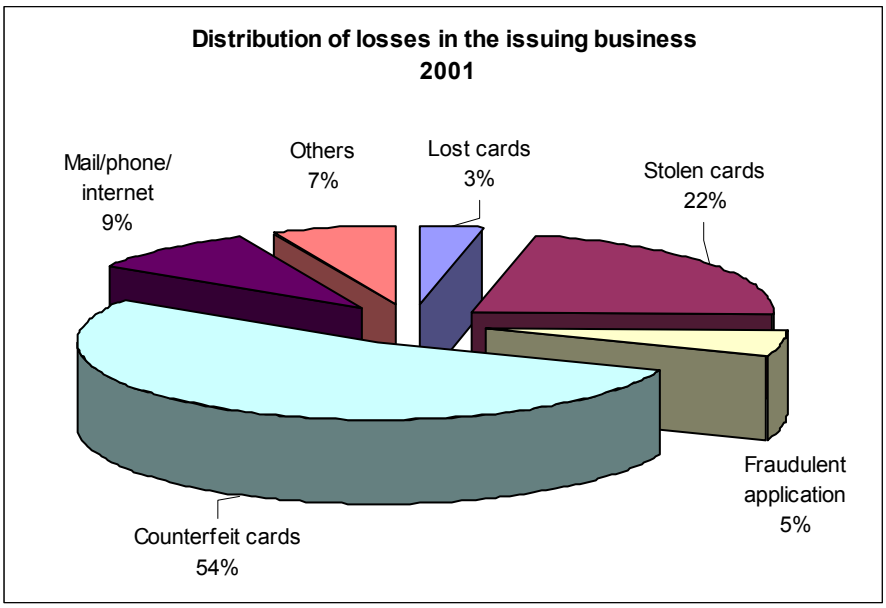
The proportion of fraud caused via mail, telephone or the Internet, i.e. in card-not-present transactions in which the holder only provides the number of his card when payment is made, remained unchanged in 2000–2001. The electronic signature, already noted, and the virtual card (or invoice) currently used by only two banks in Hungary which may be used solely for paying the countervalue of goods or services ordered via the Internet, are used as tools to protect against this type of fraud.

[1] See ‘Shopping by numbers’; European Card Review, March–April 2002.

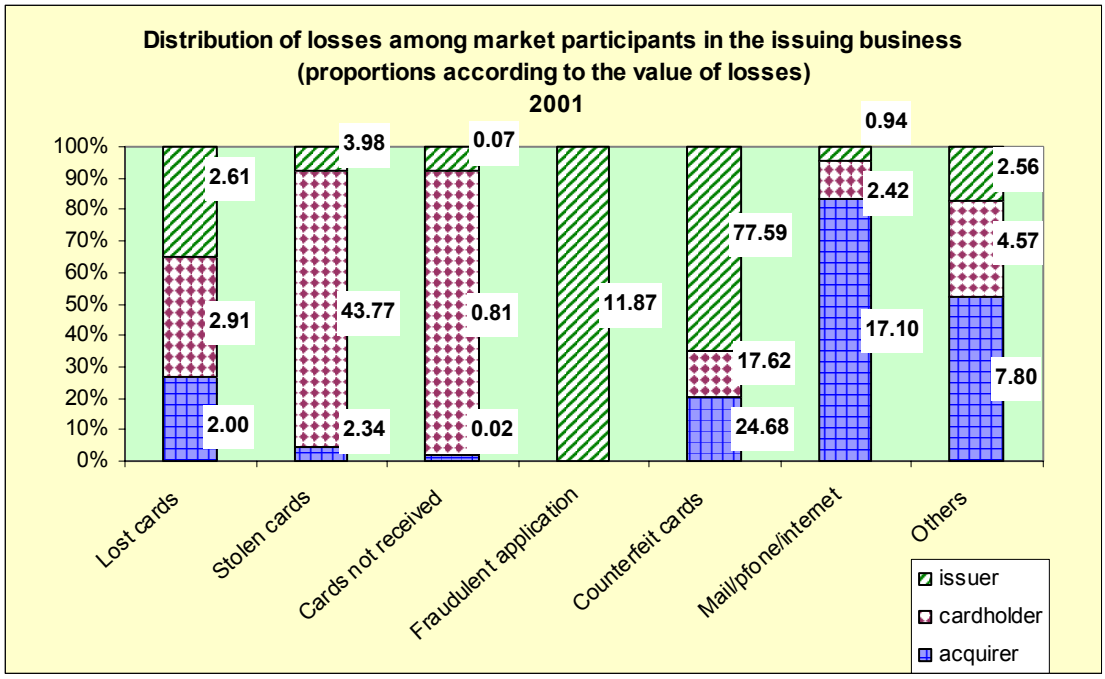
2.1.2 Value and distribution of losses (write offs)

Participants of the domestic payment card business booked a total HUF 226 million loss last year. This was the equivalent of 0.008% of total turnover, compared with 0.01% in 2000. Issuer banks bore 44% of this amount (4% less than in the previous year), 32% was borne by card-holders (3% less than in 2000) and 24% by domestic and foreign acquiring banks (a 7% increase relative to 2000).

As the following Chart shows, the distribution of losses by type was broadly comparable with that of fraudulent acts, with a slight difference.



Analysing the distribution of losses among market participants according to the breakdown presented by the pie chart, we obtain the following picture:



Card-holders accounted for 81% of losses incurred due to fraud committed using lost and stolen cards. This is a particularly noticeable ratio, as from 1 December 1999 losses incurred after the time of reporting (i.e. after the act of notifying the loss or theft to the issuer bank) must be borne by the issuer, unless there is proof of a wilful or grave negligence on the part of the holder, including cases when cards lost or stolen are used together with the PIN code. Issuer banks debited holders with a total HUF 46.68 million last year due to fraud committed using stolen or lost cards. The amount of loss borne by banks was HUF 6.598 million, 11% of the total. The rest of losses was passed on to merchants.

Losses arising from card not received fraud were insignificant last year (so small that they can't be seen on the pie chart); however, 90%, i.e. the overwhelming majority of these, was borne by card-holders, the rest being shared between the issuer banks and retailers.

In the case of fraudulent application all losses are borne by issuers.

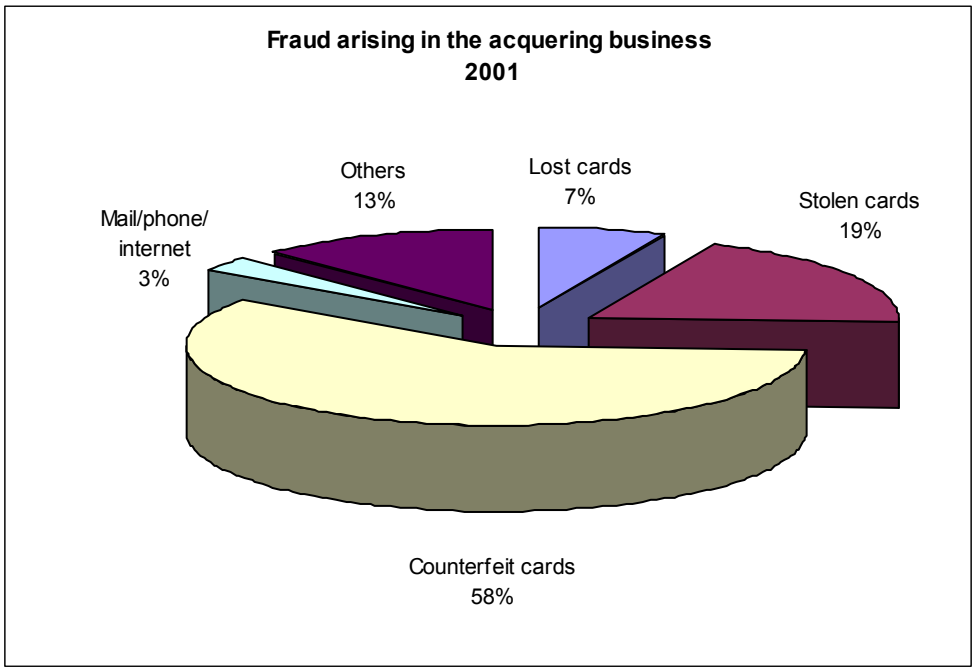
Issuer banks assumed 65% of losses caused by use of counterfeit cards. They passed 21% on to retailers and the rest to card-holders.

Banks passed 84% of losses incurred in payment transactions conducted via mail, telephone or the Internet, i.e. when the card was not present, on to merchants. They registered 4% of the losses in their books and debited card-holders' accounts with the rest. There was a large shift in the proportions relative to 2000, when more than one-third of losses was borne by banks, 60% by retailers and the rest by card-holders.

2.2 Fraudulent activity and losses incurred in the acquiring business

The number of fraudulent acts commited by bank cards was 3,800 last year, in the amount of HUF 157 million. This was the equivalent of 0.006% of total domestic turnover. There was an improvement in terms of both value and proportion relative to the previous year – losses incurred in 2000 amounted to HUF 369 million, 0.016% of total turnover.

The following Chart details the distribution of fraudulent acts incurred according to type:



Comparing the proportions accounted for by the various types of fraud with those in the issuing business, there were only minor shifts in certain types of fraud. Obviously, these originated from the differences between losses incurred in use of foreign-issued cards in Hungary and in that of domestically issued cards abroad.

Participants of the card business wrote off HUF 157 million as a consequence of fraudulent acts incurred in the year under review and in earlier years. This accounted for 0.006% of total turnover. Acquiring banks passed the vast bulk, 85%, of this on to foreign and Hungarian issuer banks, who presumably passed a part further on to their clients.

3 Conclusion

On the whole, the number of fraudulent card uses fell in 2001 relative to the previous year.

This positive development may be attributable to banks using various methods to protect their own customers' interest, recognising that the reinforcement of confidence in the bank card as a payment instrument is a very important condition for recruiting new clients and maintaining existing ones. The majority of banks operate monitoring systems to spot unusual or suspicious transactions. In cases of unusually large-value transactions or those suspicious for other reasons, they check by mobile phone calls or SMS messages whether the card is being used by its rightful holder. Both international card associations have been encouraging their member banks to switch to chip technology, in order to restrict fraud committed using counterfeit cards.