MAGYAR NEMZETI BANK

Payments and Securities Settlements

Payment card fraud in Hungary
2008

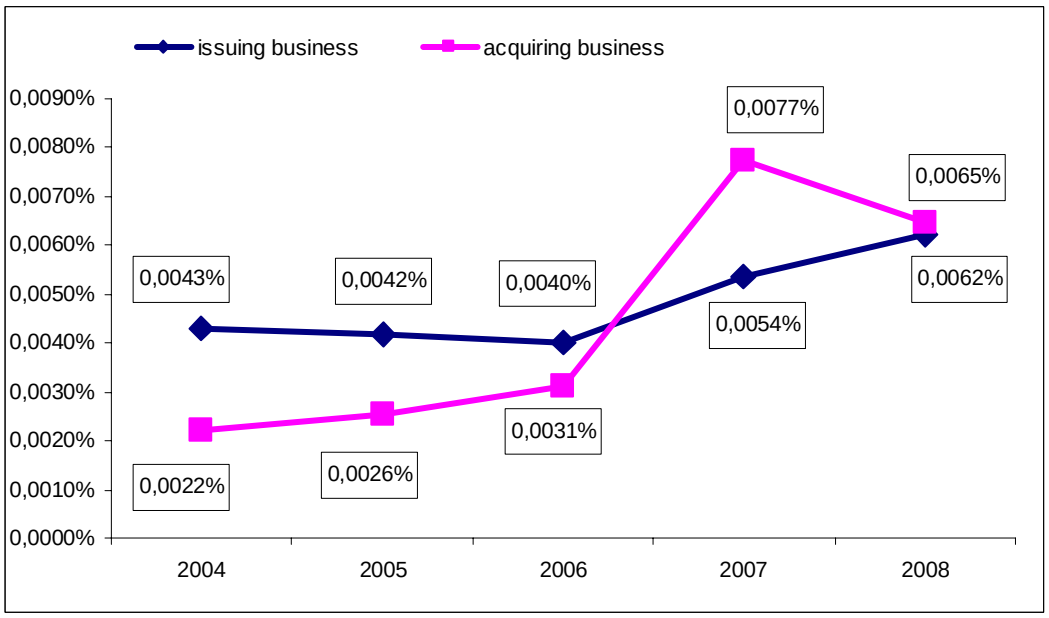
By Éva Keszy-Harmath
Payments and Securities Settlements

Summary

In 2008, fraud arising on Hungarian-issued cards (card issuing business) used in Hungary and abroad continued to rise as a percentage of total plastic card turnover compared with the previous year; however, they remained below losses recorded in, for example, France (0.048%), Spain (0.024%) or the UK (0.094%) in 2007.

After a sharp increase in 2007, the amount and percentage of fraud losses on transactions made on bank cards issued in Hungary and abroad (acquiring business) both fell last year (although this was mainly attributable to a significant decline in fraudulent activity in "Others" category in 2007[1]). Chart 1 shows the amount of total losses as a percentage of total transaction amount.

Chart 1 Value of fraud as a percentage of plastic card turnover in the issuing and acquiring businesses



Note: Frauds in the card-issuing and the acquiring businesses contain some overlaps (see Chart nr.2.), consequently, the figures from the two sectors cannot be combined.

Fraudulent activity in the issuing business amounted to HUF 438 million (an increase of 25% in one year), half of which resulted from counterfeit fraud. Only two of the Hungarian banks has started to equip their cards with EMV chips, currently regarded as the most effective tool to prevent counterfeiting. SEPA mandates that in euro area countries all cards should be equipped with a chip satisfying the EMV standard. Although this requirement does not apply to Hungary for the moment, available information suggests international card brands require their Hungarian member banks to fully migrate to EMV before the end-December 2010 deadline. In Hungary, the share of EMV chip cards was 30% at the end of last year; this compares with an average of 67% for the EU-27.

In an earlier projection, participants of the card issuing business said full migration (including also for ATMs and POS devices) would be necessary as soon as possible because the use of counterfeit cards would expand to countries that have not or not fully migrated to EMV. However, rather unexpectedly, the trend saw a reversal two years ago,

[1] The sharp increase in losses recorded in "Others" category in 2007 was attributable to a surge in fraudulent transactions by cardholders, and in particular to collusion between cardholders and merchants.

and the use of counterfeit bank cards began rising in fully migrated environments. The reason for this was that, in the transitional period, a magnetic stripe has to be attached to all EMV chip cards, in order to ensure that they could be used internationally, and all ATMs and POS terminals compatible with the EMV standard should be capable of accepting cards equipped with a magnetic stripe. In most cases, counterfeit fraud involves skimming magnetic stripe data from the original hibrid card.

Another feature in countries which have made advance with EMV chip migration is that fraudulent activities are beginning to concentrate in fraud types against which chip migration does not offer a protection. These are for example the card-not-present (CNP) transactions where payments are initiated via mail, telephone or the Internet. The share of this type of fraud also rose in Hungary compared with previous years, reaching 16% of total frauds in 2008. In order to prevent the occurrence of further losses, international card brands offer various services to their member banks, including Verified by Visa and MasterCard SecureCode (for more details, see the box in Section 1.1). Domestic banks also use these services to protect their merchant clients; for the time being, however, this service is not available to their cardholders.

Frauds incurred through the use of cards stolen or lost continue to be significant in Hungary (27%). In order to limit such losses, SEPA recommends that PIN should be introduced mandatorily in POS transactions. Currently, PIN is only made compulsory by MasterCard in transactions on POS terminals. For the rest of the brands, issuing banks decide whether customers using a card should provide a signature or a password to authenticate themselves as the legitimate holder of the card.

The amount of **losses written off in the card issuing business** was HUF 393 million in 2008 (an increase of 24% from the previous year). However, the percentage shares accounted for by the participants of the business changed considerably. The consumer protection provisions of Government Decree No. 227/2006, in effect from 1 March 2007, had their greatest effect last year, when losses borne by cardholders fell form 45% to 22%.

Here, the most marked change occurred in the distribution of losses arising from counterfeit fraud: despite a 50% increase in losses in 2008 compared with 2007, losses charged to cardholders fell to one-third of their value in 2007. Within the total, the percentage share of fraud losses charged to cardholders fell nearly to one-fifth (3%) of their level in the previous year.

As regards fraudulent card use via mail, telephone or the Internet, losses charged to cardholders fell to 67% of their level in the previous year and to a half as a percentage of total losses (6% in 2008).

Losses charged to cardholders arising from fraudulent transactions with lost or stolen cards also fell (from 78 to 66%). This suggests that customers are increasingly aware of their rights and obligations related to card use in case it is lost or stolen.

Fraudulent activity on cards in the acquiring business amounted to HUF 457 million in 2008, 11% less than in the previous year. The distribution of fraud is similar to that in the issuing business: fraudulent uses of counterfeit cards accounted for 71%, uses of stolen cards for 19% and frauds committed via mail, telephone or the Internet for 6%.

For card acquirers, the objective would be full chip migration, in order to protect against counterfeiting (although the discussion of the card issuing business suggests migration does not have the desired effect in the transitional period). In Hungary, all banks interested in merchant acquiring have started to upgrade their POS terminals. The share of POS devices accepting EMV chip cards was 81% at the and of last year. This is better

compared with a 74% average for the EU-27. However, Hungary lags behind in converting ATMs: 58% of ATMs have already been converted in Hungary, compared with a 91% average for the 27 EU Member States.

Introduction

Structure of the analysis

In the analysis of card fraud, fraudulent activity and losses incurred in the card issuing acquiring businesses will be dealt with separately.

Fraudulent activity means fraudulent acts reported by cardholders or otherwise communicated to banks in the period under review, i.e. in 2008. Such fraudulent acts were investigated by the banks affected during the same year and shown as losses for some participant of the payment card business. In some cases, however, the completion of such investigations is likely to last well into the following year.

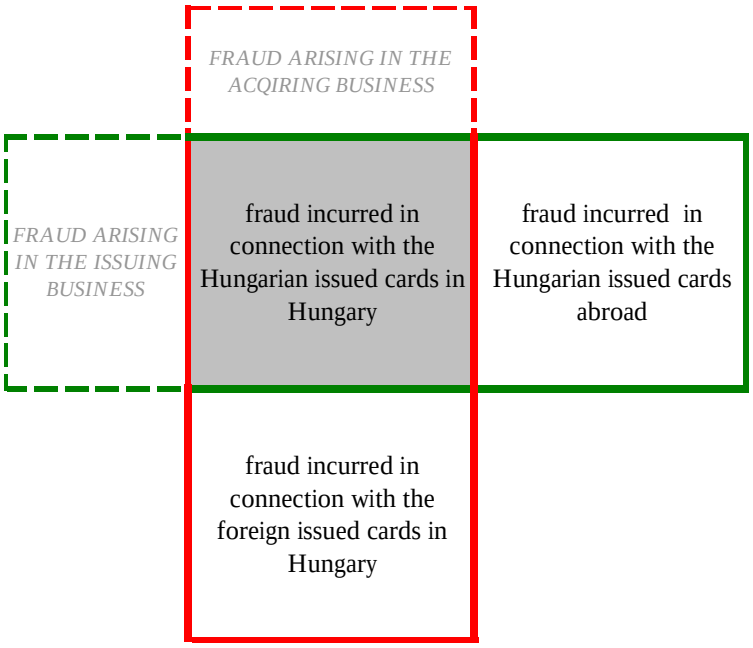
Loss means the recording of financial damage as debt written off by some participant in the card business, i.e. the bank issuing the card, the cardholder or participating retailers or the banks of such (acquiring bank). Financial damage forming the basis of losses occurred either in the period under review or before; however, the investigations were completed in 2008.

Fraudulent activity and losses in the card issuing business mean any fraud committed in Hungary and abroad with cards issued by Hungarian banks. Losses incurred by cardholders are also dealt with in detail in this section of the analysis.

Fraudulent activity and losses arising in the acquiring business mean fraud involving the domestic use of cards issued by Hungarian banks and the domestic use of cards issued abroad.

As shown in Chart 2, data on fraudulent activity (and losses) in the issuing and acquiring businesses are overlapping and, therefore, the corresponding figures for the two lines of business cannot be added together.

Chart 2 Structure of statistics for card fraud used by the MNB for analytical purposes



1 Fraudulent activity and losses in the card issuing business

1.1 Fraudulent activity

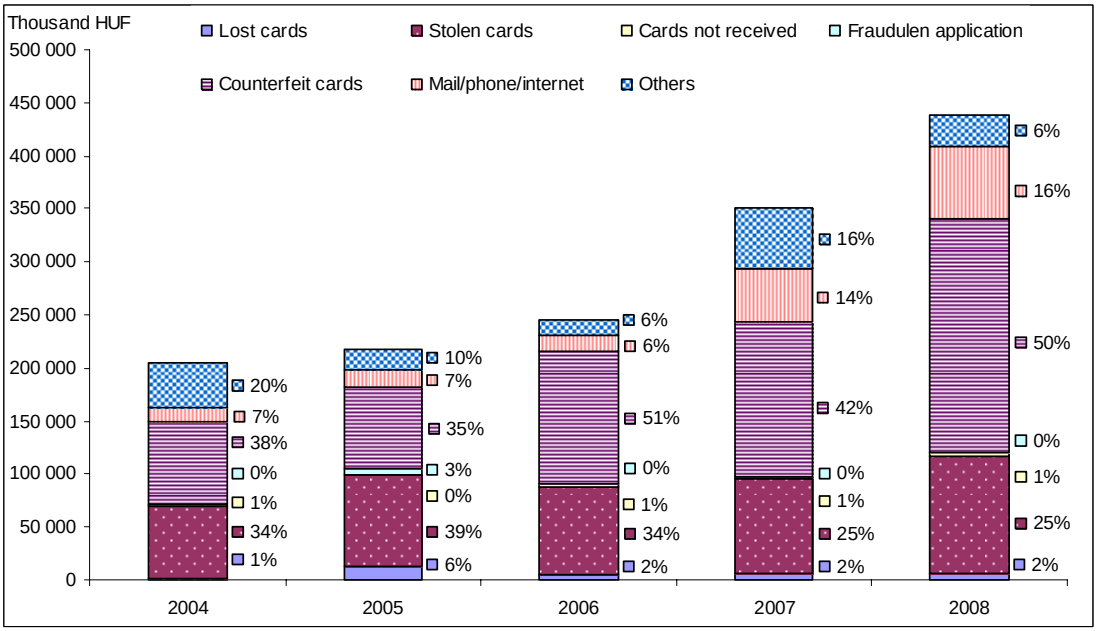
Total fraud committed with domestically issued cards in Hungary and abroad rose sharply in 2007. Last year, however, the rate of growth slowed considerably. Their share of total transaction value, however, was far lower than in, for example, France (0.048%), Spain (0.024%) or the UK (0.094%) in 2007.

Table 1 Card fraud in the card issuing business

	2004	2005	2006	2007	2008
value of fraud (thousand HUF)	204 028	218 241	245 615	351 177	437 670
rate of growth (%)	2%	7%	13%	43%	25%
share to the issuing turnover	0,0043%	0,0042%	0,0040%	0,0054%	0,0062%

As shown in Chart 3, the sharp increase in 2007 was attributable mainly to the significant rise in fraud via mail/telephone/Internet as well as in Other types of fraud. However, the increase in Other categories was only characteristic of 2007, and was mainly attributable to collusions between cardholders and merchants, in contrast with fraud via mail/telephone/Internet which has been growing globally.

Chart 3 Percentage distribution of losses in the card issuing business according to types of fraud



In mail/telephone/Internet transactions, i.e. when the card is not present, the value of fraud surged by 350% in 2007, before rising by 37% in 2008 from its 2007 base. The underlying reason for this was that, with progress in migration to EMV chip in order to combat card counterfeiting, crime has been channelled towards other types of fraud, mainly towards card-not-present fraud. International card brands combat white-collar crime with constant developments, and offer the following services to their member banks to protect against fraud, in order to enhance the security of card transactions made over the Internet:

The **Verified by Visa** and **MasterCard SecureCode** systems allow the authentication of the cardholder and the merchant. Where any of these two signs – either Verified by VISA or MasterCard SecureCode – are implemented, cards can be used safely. Participating in the programme protects both the merchant and the cardholder, as the latter is only verified by his bank if he confirms his interest in the transaction by giving his pre-selected password. If confirmation is unsuccessful (i.e. if the party initiating the transaction has given a wrong password), the transaction fails.

Both card brands have upgraded their services recently:

The basic feature of the **MasterCard CAP** (chip authentication programme) reader is that the cardholder inserts his EMV chip card into a device the size of a pocket calculator, enters his PIN code associated with his card and receives a one-time password for his actual online payment.

The chip of a **Visa PIN Card** generates the one-time password itself, which appears on the alphanumeric display of the card, after the cardholder has entered his PIN on the keypad built into the card.

In Hungary, all of the banks interested in the acquiring business for Internet transactions (OTP, K&H, CIB, Budapest Bank and Erstebank) make available Verified by Visa and MasterCard SecureCode services for their merchant clients. This solution protects both the acquiring bank and its merchant partner against a liability shift in the case of fraud.[2] At the time of writing the analysis, issuing banks do not yet offer this service to their cardholders.

Half of the value of fraud arose from the use of **counterfeit cards**, and increased by 50% compared with the previous year. Migration to EMV chip, urged by SEPA, is intended to limit this type of fraud. However, in the transitional period, when both the chip and the magnetic stripe are integrated on cards to ensure full usability, counterfeit cards can be produced by copying the details stored on the latter, which then can be used in a magnetic stripe environment. The projection at the beginning of the chip migration was for counterfeiting to be channelled to

- countries where migration have not or not fully implemented; and to
- other types of fraud, for example, mail/telephone/Internet.

However, in the transitional period fraud has also been rising in countries where full migration has been implemented, due to the fact that the hybrid cards noted above are easy to counterfeit. Nevertheless, the EMV chip remains both an effective protection against counterfeit fraud and a way to mitigate losses arising form fraud. This is confirmed by the example of the UK below, and particularly by the distribution of losses in a domestic and international environment.

In Hungary, only two banks, K&H and OTP, have started to equip their cards with EMV chips. At the end of 2008, 30% of the total nearly 9 million cards in use had a chip in addition to a magnetic stripe. By way of comparison, the same ratio was 67% in the EU-27. According to available information, several other banks have started to migrate their cards to the EMV chip technology at the time of writing the analysis.

[2] In international transactions, this services plays a role in payments via the Internet similar to that played by the EMV chip in physical transactions made with counterfeit cards: if the payer has not registered for the service, any loss resulting form the fraud will be charged to the card issuer.

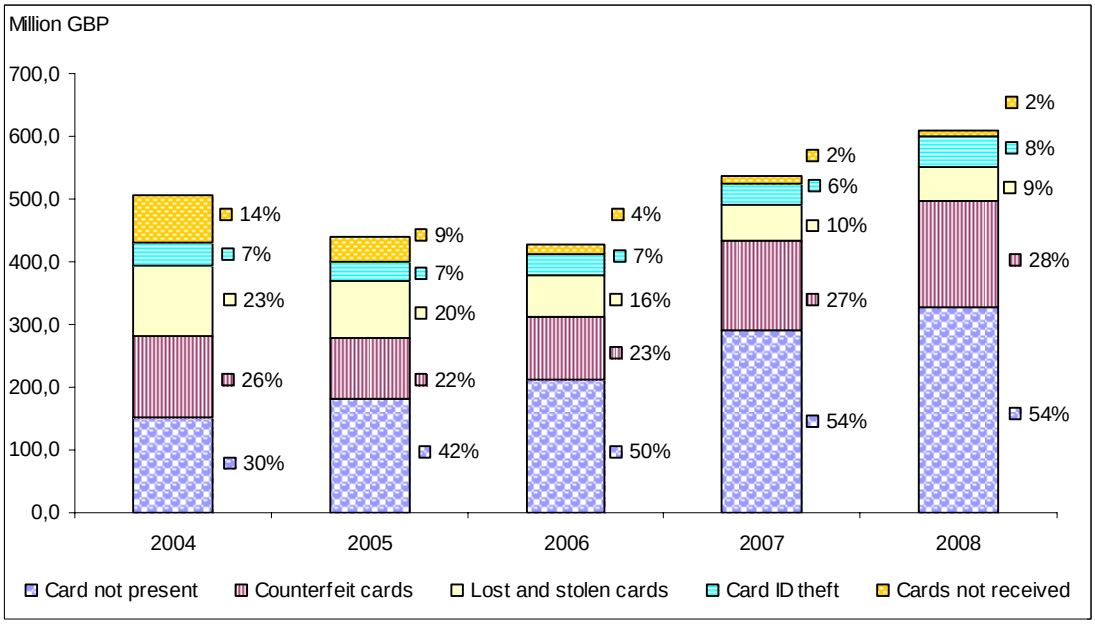
Placing these developments into international context, the UK serves as a good example, where the total value of loss fell with progress made in chip migration: counterfeit fraud losses declined and mail/telephone/Internet fraud losses rose. In 2007, however, this trend saw a reversal, and both the total value of loss and counterfeit fraud losses resumed rising. In addition, mail/telephone/Internet fraud losses continued to rise as well.

Table 2 Value of fraud in the issuing business in the UK

	2004	2005	2006	2007	2008
Value of fraud (GBP millions)	504,7	439,5	427,1	535,3	609,9
Growth rate	25%	-13%	-3%	25%	14%

Source: APACS website.

Chart 4 Distribution of the value of fraud in the issuing business in the UK by types of fraud



Source: APACS website.

Looking at the distribution of fraud data, it is clearly observable that in a fully migrated country fraudulent activity has been channelled from domestic to international transactions (see Table 3). However, the trend stalled last year, a probable reasons for which may have been the following (data are not available to confirm this):

- acceptance of magnetic stripe cards at ATM and POS terminals in the UK must be ensured, in order to allow other cardholders to use their cards without EMV chip;
- UK-issued cards must continue to be equipped with a magnetic stripe, in addition to an EMV chip in order to allow other cardholders to use their cards in countries that have not yet upgraded to the EMV standard. As a result of these two factors
- frauds can still be committed with the magnetic stripe version of UK hybrid cards in the fully upgraded domestic environment.

These problems can only be eliminated by full migration to EMV chip as early as possible. This is why international card brands urge their members to upgrade, irrespective of whether or not a country is a member of SEPA. They encourage earliest possible migration by putting in place liability shift, applied to fraud committed in international transactions, to penalise a country that has not migrated to EMV, as well as

by putting pressure on them to meet the deadline for EMV compliance. According to available information, the international card brand MasterCard mandates its domestic member banks to fully migrate to EMV by 1 January 2011. Visa is taking similar steps.

Table 3 Distribution of fraud in the UK

	2004	2005	2006	2007	2008
Total card fraud (GBP millions)	504.8	439.4	427.0	535.2	609.9
Domestic (%)	82	81	73	61	62
International (%)	18	19	27	39	38

Source: APACS website.

While in Hungary fraud arising from fraudulent uses of **lost/stolen cards** has been rising slowly but steadily, accounting for one-fourth of total fraud, their share as a percentage of total fraud has fallen to 9% in the UK since the introduction of mandatory PIN cards.

Identity theft, a category of fraud, which accounts for nearly 10% of total losses in the UK, has an insignificant share in Hungary.

1.2 Distribution of losses written off in the domestic issuing business among participants

The value of losses written off due to card frauds investigated and closed has risen steadily over the past five years, reaching HUF 393 million in 2008 (0.0056% of transactions conducted with domestically issued cards), an increase of more than one-fifth compared with the previous year.

Losses are distributed among the participants of the card business: issuing banks pass part of it on to their cardholders and another part to acquiring banks (which, in turn, may pass it on to their contracted merchants in part or in full, writing off the rest in their books.

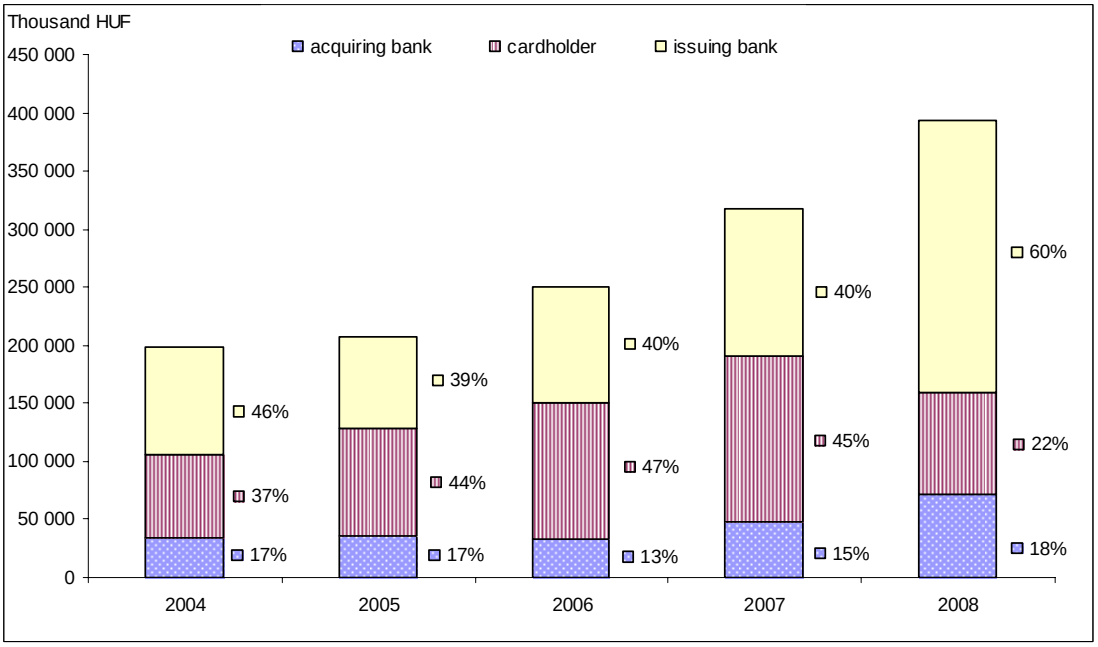
In Hungary, Government Decree 227/2006 on payment services and electronic payment instruments contains liability rules[3] governing situations in which banks can pass losses on to their cardholders. The Government Decree entered into force on 1 March 2007 and tightened further the respective rules of the previous Decree. As a consequence, the share of loss charged to cardholders stopped increasing in the year of entry into force of the Decree, and in 2008 it decreased to a half of its value in the previous year. Table 4 shows the value of losses as well as its distribution among the participants of the business.

Table 4 Losses written off in the issuing business in the past five years

	2004	2005	2006	2007	2008
Fraud losses (HUF thousands)	197,525	207,853	250,380	317,594	393,244
Growth rate (%)	4	5	20	27	24

[3] Liability rules under paragraph 18 in Section V on electronic payment instruments.

Chart 5 Distribution of losses written off in the issuing business among participants



Losses charged to cardholders' accounts accounted for 0.0012% of total annual turnover.

We will analyse the distribution of losses shared according to the major types of fraud over the past five years in the light of the provisions of the Government Decree discussed above. Our analysis focuses on losses incurred through fraud committed with counterfeit cards, as well as the two categories where frauds are likely to be re-channelled with progress in chip migration: losses arising from lost/stolen card fraud and mail/telephone/Internet fraud.

1.2.1 Counterfeit cards

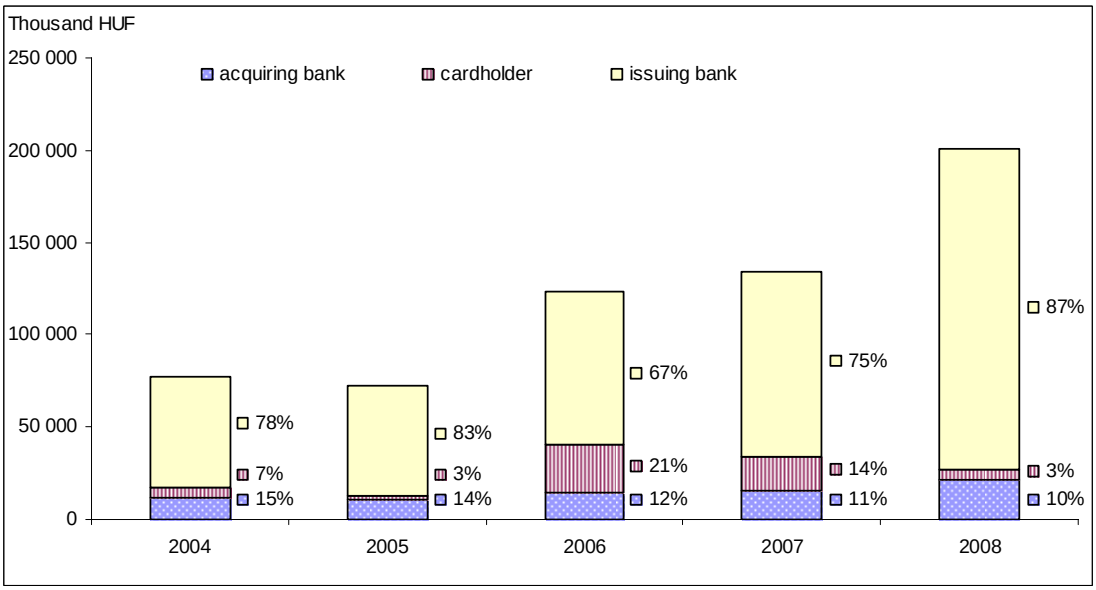
Regulation: The issuer bears responsibility for the execution of transactions which are based on the instruction of a party other than the client. Consequently, any loss will be borne by the issuer, unless he is able to prove the cardholder's wilful or negligent behaviour.

Despite the fact that fraud losses rose by 50% in 2008, the amount of losses charged to cardholders fell to one-third of the previous year's level. Within total losses, the share of losses charged to cardholders fell to nearly one-fifth of its level in 2007. Table 5 shows the amounts and distribution of losses over the past five years. The latter reflects well the effects of the tightening in legal regulations in 2007, namely, the reduction in responsibility of cardholders for a type of fraud which they are unable to influence.

Table 5 Value of losses arising from fraud committed with counterfeit cards in the past five years

	2004	2005	2006	2007	2008
Fraud losses (HUF thousands)	77,343	72,571	123,929	134,501	200,416
Growth rate (%)	0	-6	71	8	49

Chart 6 Distribution of losses arising from fraud committed with counterfeit cards among participants of the business



1.2.2 Lost/stolen cards

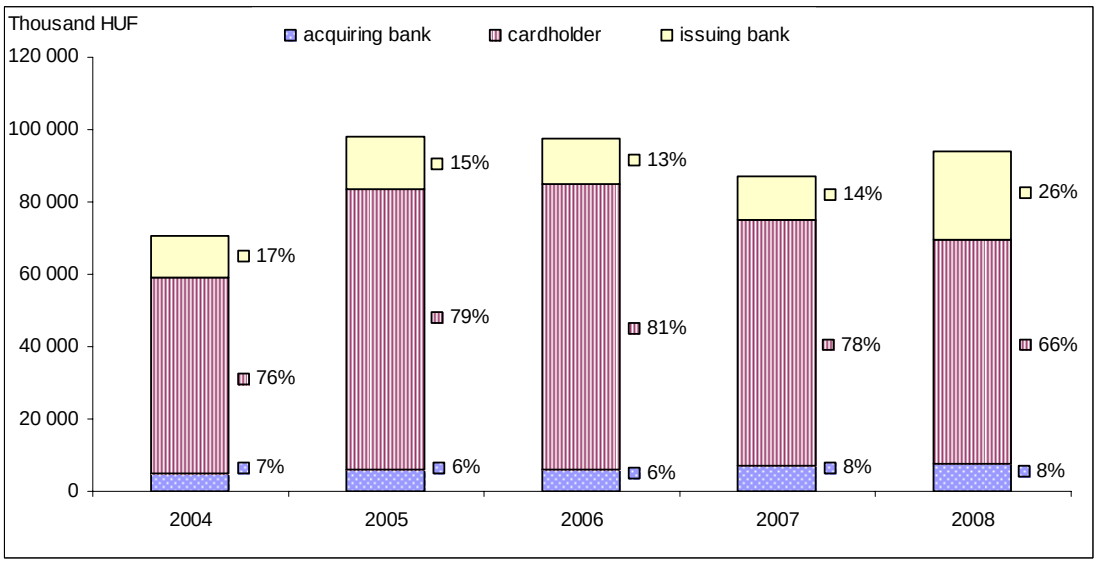
Regulation: The issuing bank is responsible for any losses incurred after reporting lost/stolen cards; however, the cardholder's maximum liability is limited to HUF 45,000 before notification, unless the bank is able to prove the cardholder's wilful or grossly negligent conduct.

Traditionally, cardholders are responsible for the majority of losses arising from this type of fraud, which indicates that gross negligence can be proved. However, there was a marked change in this area last year, when the average loss share charged to cardholders fell back from fourth-fifths to two-thirds. This underlines the importance of providing adequate information to clients about the rule of card use and their responsibilities.

Table 6 Value of losses arising from fraud committed with lost/stolen cards in the past five years

	2004	2005	2006	2007	2008
Fraud losses (HUF thousands)	70,541	98,116	97,676	86,932	94,168
Growth rate (%)	-1	39	0	-11	8

Chart 7 Distribution of losses arising from fraud committed with lost/stolen cards among participants of the business



1.2.3 Mail/telephone/Internet

Regulation: The cardholder bears no responsibility for any loss, if the card has been used without its physical presence or electronic authentication. In such cases, it is a ground for refusal if the bank is able to prove the cardholder's wilful or grossly negligent conduct.

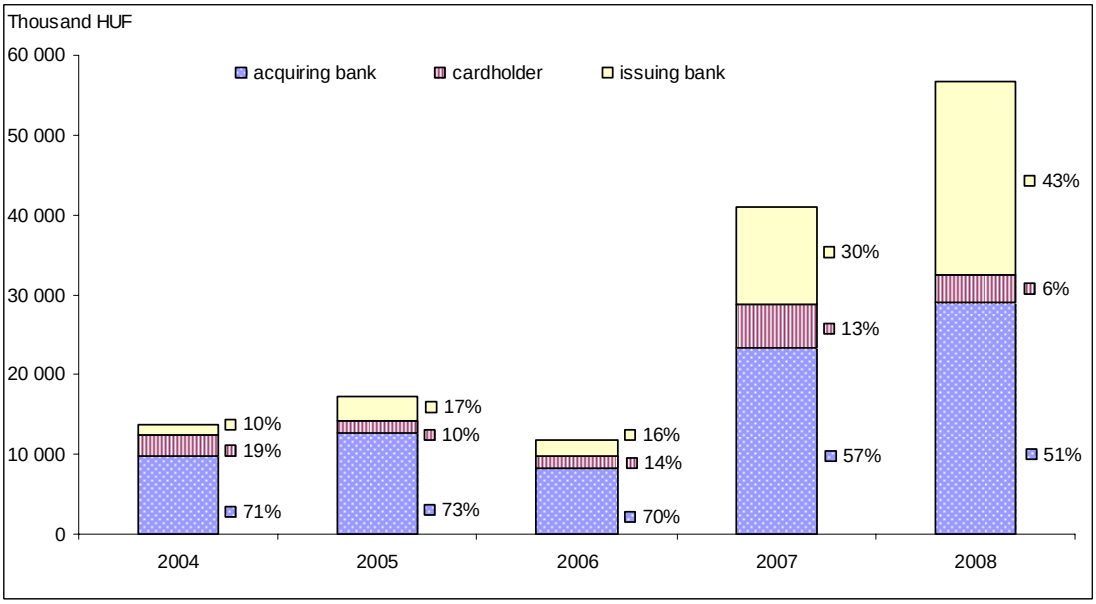
Traditionally, merchants bear all losses arising from this type of fraud (due to the stringent requirements of the card brands and legal regulations). The amount of losses charged to cardholders fell to 67% of its level in the previous year, and to half as a percentage of the total.

Only 0.007% of the total value of purchases via mail/telephone/Internet in 2008 was borne by cardholders, while total losses accounted for 0.12% of the total value of transactions.

Table 7 Value of losses arising from mail/telephone/Internet fraud in the past five years

	2004	2005	2006	2007	2008
Fraud losses (HUF thousands)	13,787	17,128	11,708	40,970	56,817
Growth rate (%)	-15	24	-32	250	39

Chart 8 Distribution of losses arising from mail/telephone/Internet fraud among participants of the business



As can be seen from the above discussion, loss share charged to cardholders fell spectacularly in all three types of fraud, owing to the tightening of regulations. The more conscious and rule-abiding cardholders are, the more secure this payment instrument will be for them. It is especially important, therefore, to provide adequate information and training to clients about the rules of card use, their rights and liabilities.[4]

2 Fraudulent activity and losses in the acquiring business

Fraudulent activity and losses written off arising form the use of domestically and foreign issued cards in the acquiring business include frauds related to transactions conducted at domestic acceptance points (ATMs and POS terminals) of Hungarian banks. Conseuqently, fraudulent activity and losses written off in the acquiring business also include loss events related to the domestic use of domestically issued cards (in the same way as fraudulent activity in the issuing business). Consequently, there are some overlaps in data analysed in sub-sections 1 and 2 and, therefore, cannot be added together.[5]

2.1 Distribution of fraud

Table 8 shows developments in losses resulting from fauds committed in the acceptance network of domestic banks in the past five years.

[4] Bankkártyák (Bank Cards), published by the MNB in early 2008 as the first part of a series of publications on payments and settlements, is intended to contribute to this effort. It is available in Hungarian on the Bank's website at: http://www.mnb.hu/kiadványok/penzforgalomrol_mindenkinek. In addition, the Bank has launched a separate project to improve financial literacy. Within the framework of the project, for example, all final-grade secondary school students receive a short information booklet on the most important issues affecting their age-group, including about the use of bank cards..

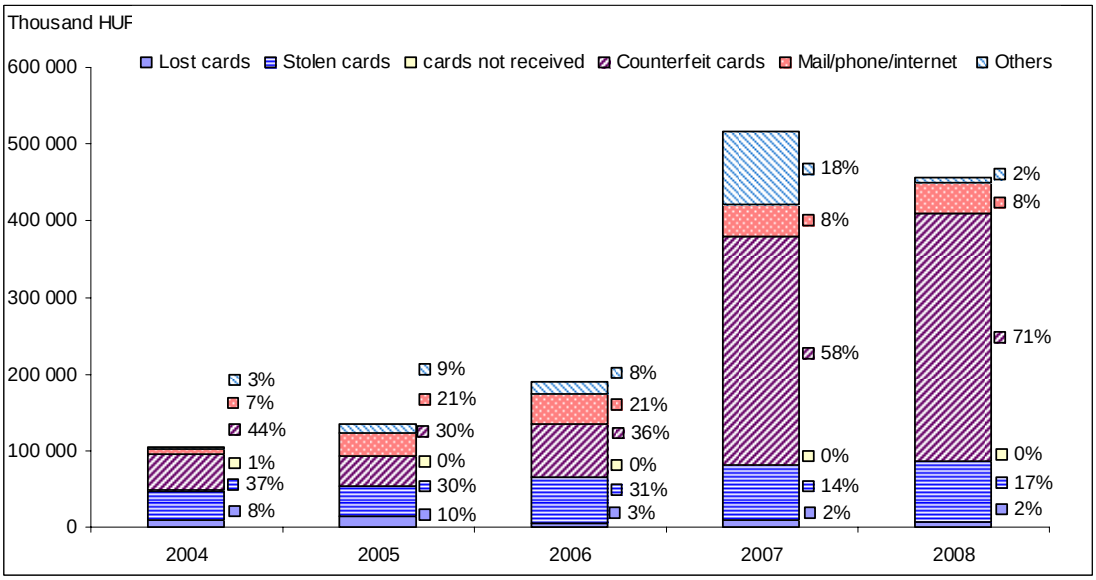
[5] For 2009, the MNB requires data providers to report data on fraud committed at home and abroad in the issuing and acquiring businesses separately. From 2009 therefore data will cease to overlap.

Table 8 Fraud arised in the acquiring business

	2004	2005	2006	2007	2008
Fraud losses (HUF thousands)	104,411	134,192	190,207	515,562	456,853
Growth rate (%)	-49	29	42	171	-11
As a percentage of issuing turnover	0.0022	0.0026	0.0031	0.0077	0.0065

The fall in the value of loss in 2008 following the sharp increase in 2007 was mainly attributable to a decrease in losses arising in the Other category, due to reasons already discussed in the section on issuing business. Chart 9 plots the distribution of fraud by types of fraud.

Chart 9 Distribution of fraud in the acquiring business



The values and percentage shares of fraud continued to increase in two categories: lost and stolen card fraud rose by 7% and coiunterfeit card fraud by 8% compared with the previous year. Fraud via mail/telephone/Internet at acceptance points fell by 9%, being half of fraud registered in the issuing business. This latter suggests that a large part of fraud associated with online uses of domestic cards arises during purchases at foreign merchants.

The continuous rise in frauds committed with counterfeit cards is attributable to the fact that migration to EMV chip has not yet been fully implemented; there are countries outside the European Union where even a decision about migration has not yet been taken; however, progress has been made to various degrees within the EU. As a significant step, in Hungary migration of ATMs to chip technology began in 2007, which continued last year (Chart 11 includes more information). The percentage share of POS devices installed and migrated in merchants' outlets remained unchanged from 2007. the comparison below suggests that Hungary lags quite far behind in migrating ATMs; however, as regards migration of POS devices to chip technology, Hungarys is ahead of the EU average.

At the end of 2008, 58% of the 4,637 ATMs and 81% of the 49,276 POS devices installed at merchant outlets were capable of accepting EMV chip cards.

Eleven banks (their number doubling from the previous year) began migrating their ATMs: Allianz, Budapest Bank, CIB, Erstebank, FHB, Unicredit, KDB, K&H, OTP, Takarékbank and Volksbank.
Seven banks (an increase of one compared wiht the previous year) had POS terminals accepting EMV chip cards: Allianz, Budapest Bank, CIB, Erstebank, Unicredit, K&H and OTP.
By way of comparison, 91% of ATM machines and 74% of POS devices in the EU-27 were capable of accepting EMV chip cards at the end of 2008.

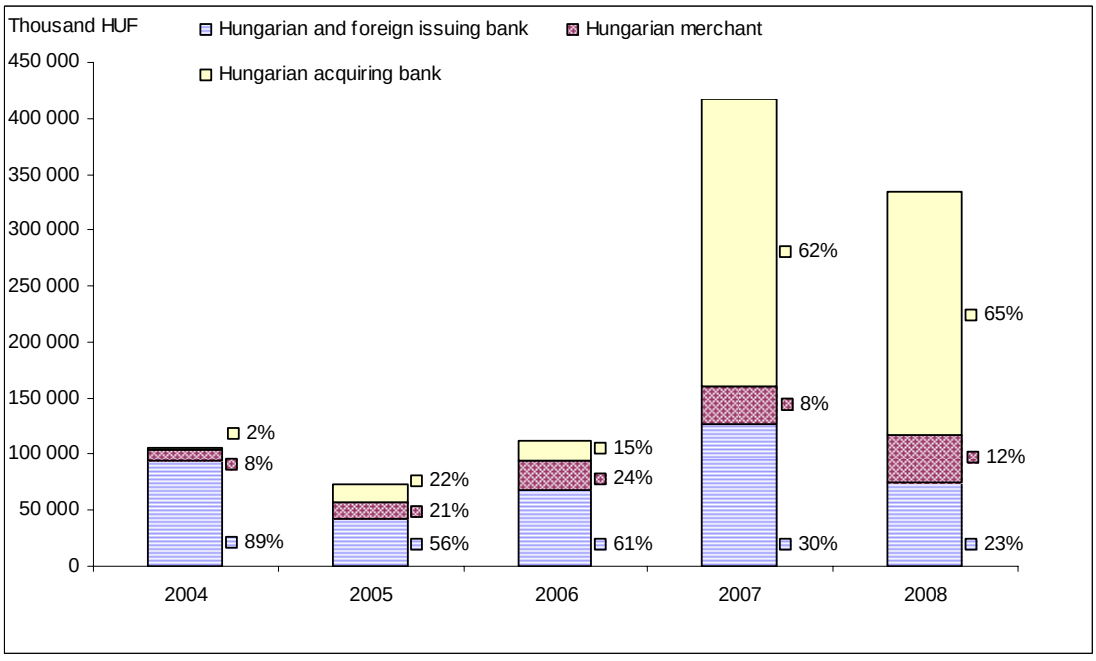
2.2 Distribution of losses written off among participants in the acquiring business

With a fall in the total value of loss, fraud events investigated and closed as well as losses written off as a result fell by one-fifth in 2008 compared with 2007.

Table 9 Losses written off in the card acquiring business

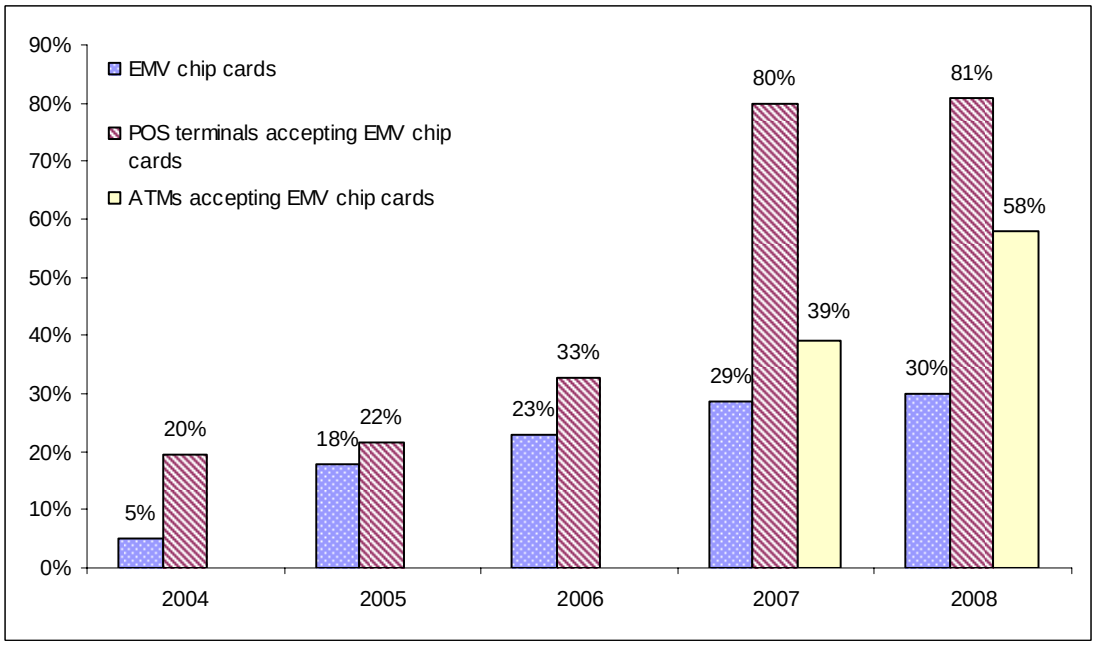
	2004	2005	2006	2007	2008
Losses written off (HUF thousands)	105,736	73,838	112,129	417,394	334,736
Growth rate (%)	-43	-30	52	272	-20

Chart 10 Distribution of losses written off in the acquiring business among particpants



Information about the distribution of these losses across the various types of fraud and between ATMs and POS devices is not available. Nevertheless, the distribution of fraud and international trends suggest that a large part of losses borne by acquiring banks result from the use of counterfeit cards at ATMs. Due to the liability shift applied in international turnover, losses caused by counterfeit cards – if a transactions has been conducted with an EMV chip card – sholuld be borne by the party who has not enabled his devices to accept EMV chip cards. This is why migration of ATMs began in 2007 and an argues for speeding up the process. Chart 11 plots data for the past five years.

Chart 11 Percentage rate of EMV chip migration in Hungary in the past five years



Therefore, it is important even in the transitional period of chip migration to enable ATM and POS terminals to accept chip cards. Otherwise, in the case of European-issued cards all losses resulting form the use of counterfeit cards are borne by the party that has not enabled its ATMs and POS terminal to accept EMV chip cards, in line with the liability rules of international card brands. Another consequence is that countefeit fraud has been channelled to countries where ATMs and POS terminals have not yet been enabled to accept EMV chip cards.

Glossary

I Fraud types discussed in the analysis

Lost/stolen cards: This type of fraud occurs on cards that have been reported as lost or stolen by the cardholder.

Cards not received: Card or mail not received fraud occurs where a genuine card has been sent to the cardholder by the card issuer but has been intercepted before receipt, either in the postal system, or at the delivery address. This type of fraud is uncommon in Hungary.

Card application fraud: Application fraud involves criminals using stolen or false documents to open an account in someone else's name. This type of fraud is uncommon in Hungary.

Counterfeit cards: Includes all types of counterfeiting, for example, criminals make copies of legitimate credit cards by copying or 'skimming' the data contained in a card's magnetic stripe. Using this 'skimmed' information, criminals manufacture counterfeit cards and use them for fraudulent purposes.

Mail/telephone/Internet: This type of fraud occurs when a criminal uses the details of someone else's genuine card or to obtain goods or services, or make payment using details of non-existing cards.

Other fraud: This category includes all other fraud that cannot be categorised under any of the categories above.

Card ID theft: This type of fraud is uncommon in Hungary (rare occurrences are categorised into 'Other'). However, for example, in the UK this type of fraud is recorded under a separate category. Credit card identity theft is when someone else manages to get access to another person's account. This also allows for the criminal to apply for a new card from the issuing bank to his own postal address by notifying the company of a change in address. This way the criminal obtains a card and PIN, which allow him to withdraw cash easily or make purchases to the account of the legitimate cardholder.

II Other terms

ATM (Automated Teller Machine): A bank machine or device which permits authorised users, typically using machine-readable plastic cards, to withdraw cash from, and make payments to, their accounts transferring funds or obtaining information about their bank account.

EMV: A standard for authenticating credit and debit card payments, developed by EMVCo, an international consortium of three companies, which helps facilitate global interoperability and compatibility of chip-based payment cards.

EMV chip migration: An objective of SEPA to convert bank cards with less secure magnetic stripe to chip cards by the end of 2010 as a deadline (for countries outside SEPA the deadline is the date they join SEPA).

Liability shift: A rule applied by Visa and MasterCard in international transactions where an acquirer or issuer that has not implemented the EMV standard or has not

enabled its ATMs and POS terminals to accept EMV chip cards becomes liable for fraudulent transactions.

PIN (Personal Identification Number): A secret numeric, generally four-digit, code to identify a cardholder.

POS (Point of Sale) **terminal**: A device allowing cardholders to make payments (occasionally cash withdrawals) with their cards at acceptance points. Information relating to transactions is collected either electronically or on paper; the former is known as electronic POS (EFTPOS), and the latter as imprinter.

SEPA (Single Euro Payment Area): Single Euro Payment Area. The objective of SEPA in the card framework is to allow for customers to use their cards to make payments or withdraw cash in an easy and convenient way and under the same conditions and security standards throughout the entire SEPA as within their home country. Migration to EMV chip and the requirement to use PIN in retail trade are part of this programme. The international card company MasterCard has mandated the use of PIN for operations on its Cirrus/Maestro cards.

At the time of writing the analysis, the member countries of SEPA are the following: Belgium, Germany, Ireland, Greece, Spain, France, Italy, Cyprus, Luxembourg, Malta, the Netherlands, Austria, Portugal, Slovenia, Slovakia and Finland.

Virtual card: Some banks offer to their customers physically non-existent cards (card numbers) to make transactions in a 'card not present' environment. In addition, a spending limit on the amount stored on the online account may be specified for security reasons. This virtual card number protects cardholders against undesired offline shopping. There are many types of virtual card numbers; however, all of them can be used for Internet shopping. Some card numbers must be applied for every purchase via SMS of the Internet. Other card numbers are generated for multiple purchases. Virtual card numbers may be issued to customers in many forms, for example, on plastic cards similar to traditional bank cards (however, these cards are not equipped with magnetic stripe and no PIN is used with them), or on a paper form (paper card, etc.).