

OPERATIONAL RISK IN BANKING – CARD FRAUD

Prof. Ioan TRENCA, PhD

„Babeş-Bolyai” University, Cluj-Napoca

Lect. Daniela BOJAN, PhD Student

„Bogdan Vodă” Universitatea, Cluj-Napoca

The card is an instrument of settlements of accounts granting, the authorized card holder, purchase of goods and services without actual presence of the cash money. Thus, the card facilitates the intrinsic financial connection between the trader and consumer, being one simple access key to a bank account. Having the general features of a paying instrument, the card grants also unconditional acquiring of cash money superseding, like this, all functional usage barriers.

The issue and development of the cards was, first of all, because of all advantages given to the card holders and, last but not least, to the traders. In already developed countries this advantage is real.

The advantages of cards to the card holder are referring to the following:

- Easy to use and enhanced security;
- Enables monitoring processes and spending control;
- The range of products and services acquirable by means of cards is extremely wide and the card holder has the possibility to carry out the most profitable acquisitions;
- Is not needed for the customers to withdraw cash and hold large amount of money to pay for the expensive goods ousting in such way the risks of theft and discomfort triggered by the cash on the bearer;
- Having a credit card, the buyer has the opportunity to choose the time to make certain acquisitions because he has the credit at his disposal;
- The transactions are carried out instantly or, if not really so, they are much faster than using cheques ;

- The card holder is able either to pay the debt entirely at the receiving time of the balance situation or to pay it on monthly installments;

In what concerns the advantages for the trader, these are: transactions are done more fluent, the cash is out from the circuit; increased security level; increased sales volume.

Considering banks' advantages, we have to mention:

- Enable increasing automatization's operation level in order to reduce the level of operations performed
- Ascertain decreasing of cash operations;
- Payments performed by means of credit cards are secured;
- High level of control over customers' transactions in comparison with available account funds and overdraft credit;
- Banks' costs to cover card operation are less than using cash or cheque expenses ;
- Interests collected from traders who accept, for their goods or services, payments by card is representing a source of income for the bank;

During all operations made thru cards, appears the risk of financial losses, risk of frauds or disputes over the transactions. Therefore, it is necessary to set some kind of rules and strict mechanisms to reduce the risk for financial losses, to fight against frauds and to treat the disputes because none of them can be eliminated for good. Once the card started to be used as a common paying instrument, the number of frauds has increased due to the opportunity to gain important amounts of money in a relatively simple manner.

The risk of financial losses may be present to all parties involved in a card-based transaction: the card holder; the trader; the card-issuing bank and the accepting bank. Usually, frauds and disputes occur at the level of a transaction.

For sure, copying and fraudulent using of cards represents a negative fact generating multiple damages to world's banking system. The overall trend, new technology and the strictly banking conduct of the nowadays user will ensure a complete cover of negative fraud effects as well as the trust in the functions of this payment instrument.

There are several ways of carrying out frauds by banking cards means but in most of the cases the issuing banks becomes victims.

The widest spread methods of committing frauds are classified by Association of Visa International as follows:

- lost card frauds;
- stolen card frauds;
- mail non-receipt card frauds (NRI);
- counterfeit card frauds;
- non present card fraud;
- card ID theft frauds.

Due to the fact that the above mentioned ones are the most frequent

types of fraud we consider that it is necessary to be detailed:

a) Lost and stolen cards fraud

Lost and stolen card fraud covers entirely all frauds on cards that have been declared by the cardholder as lost or stolen. It may take place in shops that do not have chip and PIN equipment, before the theft or loss is announced by the cardholder. This may be used on phone, internet or mail order transactions.

According to some APACS statistics lost or stolen fraud volume in UK went up from 60 mil £, in 1995, to 114,5 mil £ in 2004. Due to the chip and PIN cards introduction the volumes lost by this type of fraud went down year by year and it is now at the lowest level since 1995. In 1999 lost and stolen card fraud represented 72% of the total losses reaching 11% of total losses in 2007 (See Fig. no. 1,2 and 3)

Further more, the banking industry adopted a number of initiatives in order to fight against this type of fraud. Like this we can mention:

- intelligent card track systems;
- a Hot Card File enables the traders to automatically check if a card is stolen or lost.

Figure no.1 Lost and stolen fraud losses on UK-issued cards 1996-2007

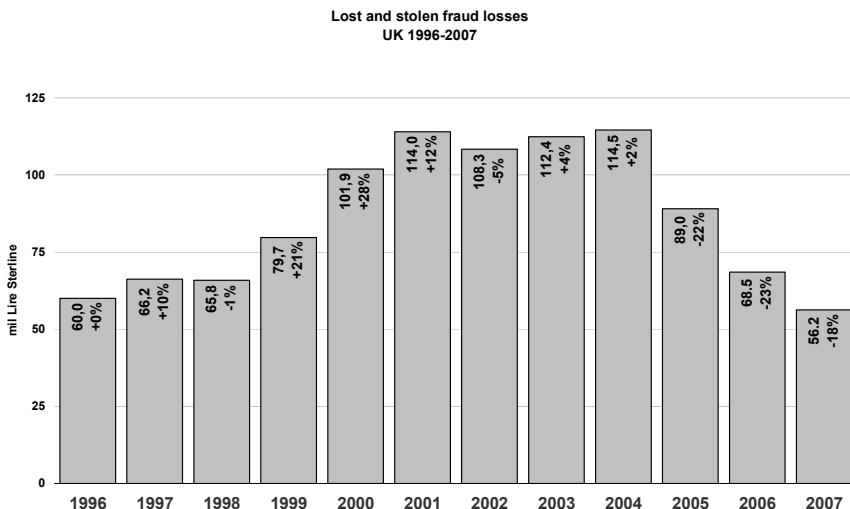


Figure no.2

Card fraud losses split by type
1995

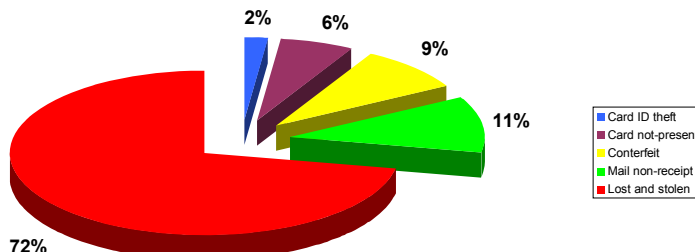
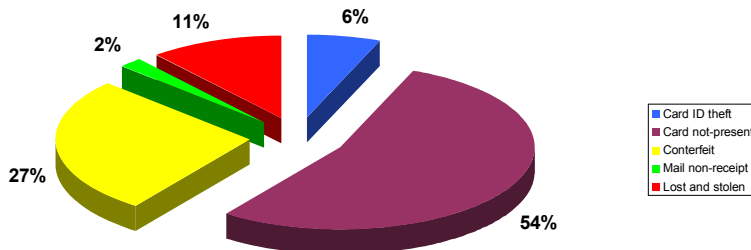


Figure no.3

Card fraud losses split by type
2007



b) mail non-receipt fraud

This type of fraud involves cards stolen or lost during the expedition time, after the card companies have sent them and before the cardholders receive them. In general, those who are exposed to such a risk are living on remote areas, with communal letterboxes. Also, the fraud can be made by the Post Office personnel, the delivery by mistake into letterboxes, can be generated by the case of changing the cardholder address or by stealing from means of

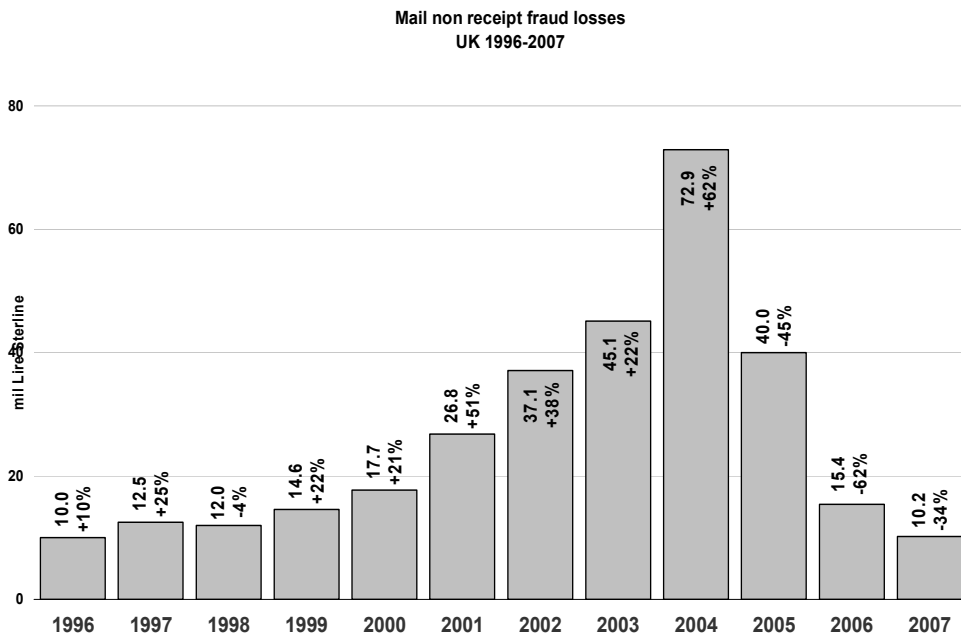
conveyance. World wide, this type of fraud represented around 2% of the overall frauds declared on 2007, compared with 11% recorded on 1995, and it is going down as year by year.

According to some APACS statistics mail non-receipt card fraud volume in UK went down from 72,9 mil £, in 2004, to 10,2 mil £ in 2007 and it represents a 34% decrease from 2006, 15,4 mil £. (See figure no. 4, 2 and 3)

The main reason behind this drastic decrease is the introduction of

chip and PIN cards and also because less cards are being sent via mail.

Figure no. 4 Mail non receipt fraud losses on UK-issued card 1996-2007



c) card not-present fraud (phone, internet and mail order)

One of the most widely spread types of fraud with a consistent increase each year is made during transactions when the card is not present: phone, internet or mail orders. Traders are taking great risks when transactions are made in the absence of both card and cardholder:

- the security elements of the card cannot be checked for authenticity and validity;

- missing signature and non introducing the PIN code increase the

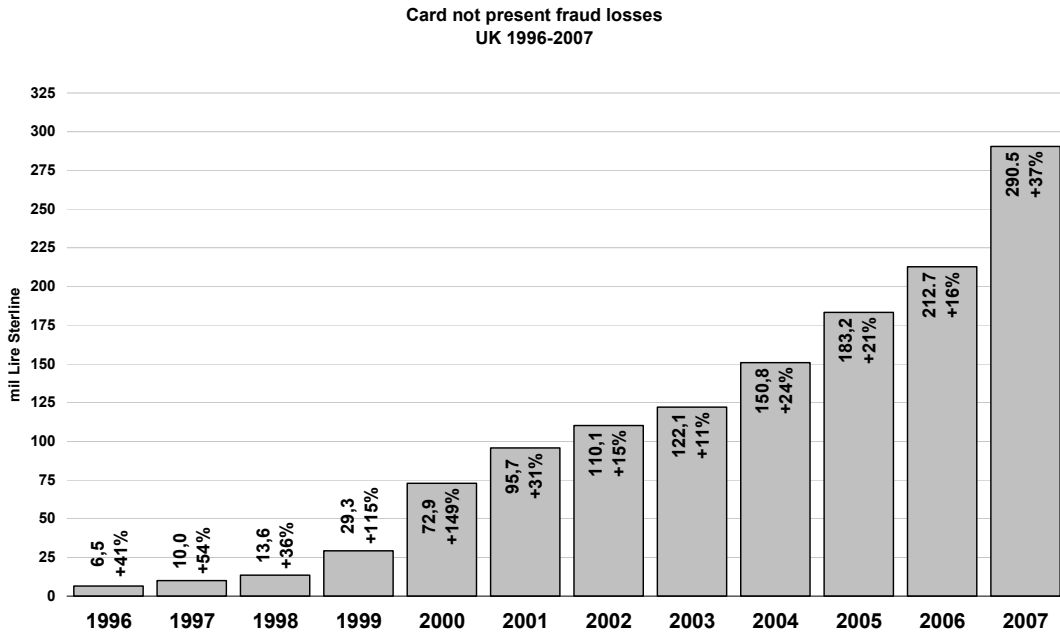
risk that the cardholder be not the legal owner;

- the card-issuing companies cannot guarantee that the information requested during card not present transactions, are not transmitted by the legal owner.

Therefore, some measures have been taken in order for this kind of transactions to be protected from fraud.

In 2007, this was the most widely spread type of fraud in UK, representing 54% of the overall card fraud losses (in comparison with 6% in 1995). If the total losses due to not present card fraud in 1995 was estimated at 6.5 mil £, in 2007 it reaches 290, 5 mil £. (See Figure no. 5, 2 and 3)

Figure no. 5 Card not present fraud on UK-issued cards 1996 - 2007



d) Counterfeit card fraud

Counterfeit - or forged cards represent cards manufactured illegally and containing information and data in the card legally issued.

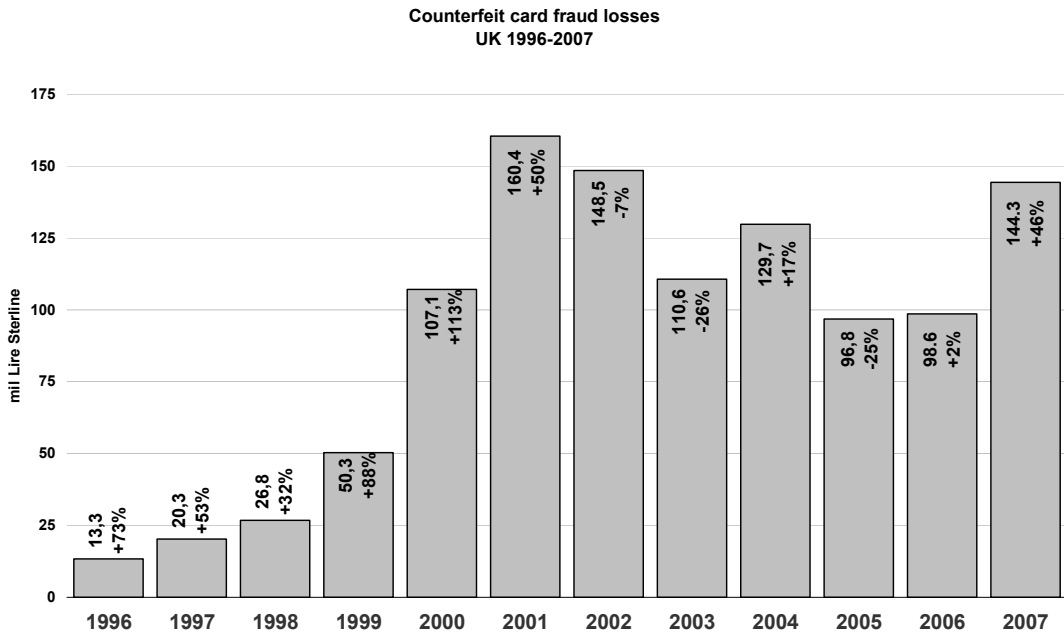
Frauds by counterfeit implies the skimming, a procedure through which the information on the magnetic band of the legal, authentic card, are copied electronically on another card without the legal possessor knowing anything about it. The forged card is identical to a real one and the volume of prejudice is rather high. Generally, the skimmer (the gadget meant to stealing information) was located in a place where corrupt tradesmen copied the cards presented by the customers before the former gave these back to the latter. Later, these were

selling the information to the forgers who, at their turn, followed to use them in counterfeiting. In most of the cases, the legal owners of cards never knew anything about these frauds until they received the bank statement containing the transactions they never contracted.

Beginning in 2003, skimmers were adapted also to the automated teller machines (ATMs).

The value of counterfeit card fraud losses in UK, in 2006, was as high as 98, 6 mil £ in comparison with 160, 4 mil £ recorded in 2001. This decrease of over 46% in comparison with 2001 is mainly due to the introduction of smart-cards and of PIN codes. (See Figure no. 6, 2 and 3). In 2007 we can see a drastic increase with over 46% of the losses, the recorded value being 144, 3 mil £.

Figure no. 6 Counterfeit card fraud losses on UK-issued cards 1996-2007



e) Card ID thefts fraud

Card ID theft occurs when a delinquent fraudulent acquires information about card or card itself together with personal data which give him the access to a different person account.

We can identify two types of card ID thefts from cardholders:

1. Fraudulent application direct to the bank. In this case, the fraudster is using stolen documents (utility bills, statements of accounts) or fake documents in order to open new account on other person's name;

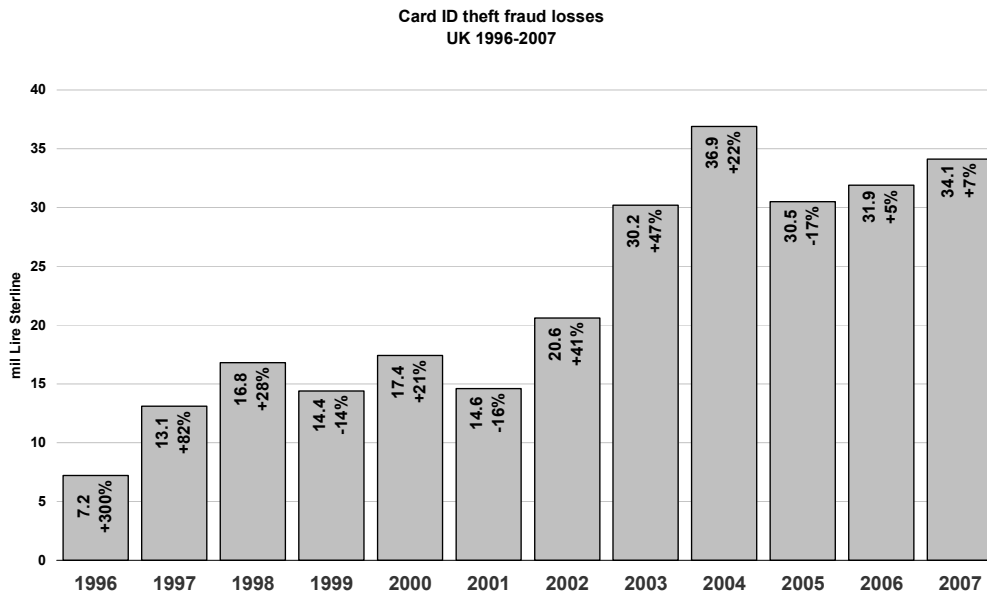
2. Account takeover. In this case, the fraudster is fraudulently obtaining

financial personal data together with legal documents about card itself. The fraudsters are accessing the accounts and in many cases they are changing the cardholder's addresses in order to get new cards or cheques;

Although card ID theft is one of the most rapidly growing theft in the world, in UK, in 2007, the total losses due to this type of fraud is tried to be stabilized after a 2004 36.9 mil £

Evan so, if we consider that in 1995 losses due to card ID thefts were at 2% of the overall losses we can see that in 2007 this percentage increased at 6%. (See Figure no. 7, 2 and 3).

Figure no. 7 Card ID theft fraud losses UK 1996-2007



What industry is doing to fight against card fraud?

In 2007 Visa annual report the company declares that it is already engaged in fighting these types of fraud together with Mastercard by continually anticipating and analyzing the fraud forms, strengthening the industry infrastructure and adopting new risk management disciplines

In order to make transactions safer one of the biggest change was the introduction of Chip and PIN cards. This was very successful across Europe in fighting against counterfeit fraud and also lost and stole cards fraud. Even the counterfeit fraud losses are dramatically decreasing, card not present fraud and cross-border fraud took the biggest ratio over the total losses because of the increasing e-commerce transactions and payments on locations with no POS or ATM's that are deployed with chip technology. That's why for example Visa is running a wide range of programs and services which can help members to

identify and fight against their vulnerability:

- Acquirer Monitoring Program;
- Fraud Reporting Service;
- Global Fraud Information Service;
- Global Zero Floor Limit Program;
- Issuer Monitoring Program;
- Merchant Fraud Performance;
- Risk training courses;
- Visa Account Bulletin
- Visa Intelligent Scoring of Risk
- Visa Europe Merchant Alert Service

What the European Union is doing against card fraud?

Regarding the European Union, we can see a continue harmonization of legislation on card payment fraud. The European Commission's Fraud Action Plan was created by Fraud Prevention Expert Group (FPEG)

The FPEG was established by the Commission under its action plans to prevent fraud in non-cash means of payment. It is an experts' group at EU level which includes representatives of

different parties involved in fraud prevention: i.e. national and EU payment schemes, banks, national public authorities, European and international law enforcement agencies (e.g. Europol, Interpol) retailers, consumer groups, network operators etc. The FPEG provides for a platform where stakeholders can effectively exchange information and best practice to prevent fraud. It contributes to intensify cooperation between interested parties, especially at cross-border level. It provides advice to the Commission.

The European Payments Council set up several new frauds prevention policies with the applicability around European Union with the help of law enforcement agencies and each national juridical authority.

The Single Euro Payments Area (SEPA) is an initiative of the European banking industry that will make all electronic payments across the euro area – e.g. by credit card, debit card, bank transfer or direct debit – as easy as domestic payments within one country are now.

How to safely use the card without risks?

- 1.put your signature on the card immediately you have receive it;
- 2.keep the account numbers and PIN number in a safe place;
- 3.periodically check all you cards in order to see if someone is missing;
- 4.destroy any useless paper which indicates you card number
- 5.memorize your PIN number;
- 6.do not give any information regarding accounts numbers or PIN numbers;
- 7.do not give to a third person your card or your PIN number;

How to recognize the fraud?

1.Lost or stolen card - if you discovered the missing card, go immediately to your bank and check the accounts statement. You may find transactions made since the last one you have remembered;

2.Mail non-received - if you know that you have to receive the card thru mail delivery service, you have to check the monthly accounts statement to identify the transactions made by you. You may find other transactions;

3.Counterfeit card – even your bank has issued your card and you have receive it, on monthly accounts statements you may find other transactions in the same time/period as yours;

4.Card not present – on monthly accounts statement you may find payments for mail orders, telephone transactions or online orders not made by you;

5.Cards ID theft – you may find that somebody has changed your home address or has ordered another card on your accounts. This you can check if you will not receive the monthly accounts statement on your address or you may discover expenses on issuing cards from the statement.

What to do when you have identified the fraud?

- 1.contact immediately your bank;
- 2.check if your address is not changed ;
- 3.if you still have the card but there are transactions on your account contact your issue-bank in order to report the abuse and to ask another card;
- 4.you have to announce the credit office that a fraud has been committed. A “fraud alert “ will be mentioned on your file. You have to ask for an account statement and to check it carefully;

REFERENCES

Basno Cezar, Dardac Nicolae	<i>Sisteme de plăți, compensări și decontări.</i> Editura Didactică și Pedagogică, București, 2004;
Cocriș Vasile	<i>Tehnica operațiunilor bancare.</i> Editura Universității "Alexandru Ioan Cuza", Iași, 2006;
Poanta Dorina	<i>Instrumente de plată fără numerar. Operațiuni prin carduri.</i> Cartea Universitară, București, 2005;
Popescu Radu, Tudorcea Cristian	<i>Cardul – instrument modern de plată</i> Editura Tribuna Economică, București, 1998;
*****	www.visainternational.com ;
*****	http://en.wikipedia.org/wiki/Credit_card_fraud ;
*****	http://www.sas.com/industry/fsi/fraud/index.htm ;
*****	http://www.h-online.com/security/Manipulated-ATMs--/features/100187/0 ;
*****	http://www.idtheftcenter.org/ ;
*****	http://www.mastercard.com/ .