RISK MANAGEMENT AND PREVENTION OF FRAUD IN CARD TRANSACTIONS

CODRUTA DANIELA PAVEL, CARMEN IMBRESCU, AURA DOMIL, CIPRIAN PAVEL
WEST UNIVERSITY OF TIMIŞOARA, B-dul Vasile Pârvan, Timişoara
codruta.pavel@yahoo.com, carmenimbrescu@yahoo.com, auraemanuela@yahoo.com
„TIBISCUS" UNIVERSITY OF TIMIŞOARA, FACULTY OF ECONOMICS
1/A Daliei Street, Timişoara, 300558
pavel_ciprian9@yahoo.com

Abstract:
Credit institutions issuing and accepting cards have responsibility for identifying, evaluating and mitigation fraud and activities with potentially risk. Risk management is necessary to avoid losses that may occur both directly through fraud and indirectly through loss of customer confidence regarding safety card operations. The risk management in cards activities aims to identifying those events which by their appearance would produce adverse effects on the activity, possible generating financial loss and find solutions to avoid them and reduce their effect.
Credit card fraud refers to any situation where a person deliberately uses: card obtained through illegal methods, a counterfeit card, a valid card code, in order to obtain cash, goods or undue services.

Key words: *Bank, fraud, banking cards, risk*

JEL classification: *G21*

According to the provisions of BNR (National Bank of Romania) Regulations no 4/06.13.2002 and the regulations of Visa and MasterCard card merchant associations, the issuing and accepting banks have to identify, evaluate and limit the effects of frauds and activities which imply a potential risk.

Risk control is necessary to avoid the losses which may occur both directly through the fraud and indirectly through the loss of customers 'confidence towards the safety of card transactions.

Risk control in card activities has the aim to identify the events which might produce inauspicious effects upon the activity, which might generate financial losses, and to find solutions in order to avoid them and to reduce their effect.

So, the Risk Management System aims to: prevent and identify the fraud activities, define and apply some corrective measures, supervise the activity of accepting merchants and card operations issued by the international card associations, control permanently the number of registered frauds.

Frauds defining and classification

Credit card fraud refers to any situation in which a person deliberately uses:

- a credit card obtained through illegal methods
- a spurious credit card
- the code of a valid card

with the aim of obtaining improper cash, products or services.

According to the classification made by the credit card associations, frauds may be: card transactions realized by lost or stolen cards, transactions by cards obtained through skimming, transactions made by issued cards, but which did not succeed to get in the possession of the client for which they were issued, transactions made by cards issued on the basis of some documents for getting into contact with the bank,

documents which were filled in on the basis of false identification data, changing the information written on the receipt by the merchant, account takeover – another person pretends to be the possessor of the card, the merchant issues some receipts without the authorization of the possessor, crediting the account to which the card is attached through the cancelling of a transaction, but without sending the original transaction or sending it with delay, or other kinds.

Out of these, the frauds with counterfeited cards are most common.

The counterfeited card is a false card, made in such a way that it is similar to a real card, using some identification elements of a valid card.

In these cases, the cardholder denies the involvement in a transaction and states that the card is in his possession, and the bank states that the transaction was made in presence of the card, with or without reading the magnetic band of the card.

Depending on the way the counterfeited cards are built, in this category there were identified frauds realized using:

- illegal cards using impersonalized cards;
- real cards transformed through modification of the embossed characters;
- blank cards whose magnetic band is made with data taken from another valid card;
- cards electronically counterfeited, copying the magnetic band of some real cards (skimming) or registering some pieces of information illegally obtained;
- cards with valid codes generated by an illegal software, utilized in transactions which do not need the physical presence of the card (such as MOTO, e-commerce etc).

Risk management in the field of card issuing

Cards can only be issued on the basis of a written application form, signed by the physical person or the official of a juridical person.

Receiving and checking the issuing application form

Preventive measures regarding receiving and checking the application forms for getting into contact with the bank take into account fraud prevention through cards issued on the basis of false identification data, such as:

- the cardholder declares false data in the application form with the aim of:
  - getting a superior risk scoring which may allow a greater overdraft;
  - avoiding some elements which may limit card issuing.
- Filling in some application forms for other persons or for fictive persons with the aim of getting a card used in fraudulent purposes.

The responsibility for the correctness of the information written in the application form is beard by the cardholders through the provisions in the contract.

The Front Office staff shall check the information in the application form on the basis of:

- the identity card provided by the holder;
- the copies of the identity cards brought by the commissioners.

In all these cases there will be kept copies of the identity card, certificates “according to the original” under the signature of the employer who made the operation.

There will be refused the application forms made by the persons who are in the Risk Database because of not repaying the amount of money owed to the bank for previous credits or because of involvement in fraud cases, and also those who are on the list with the persons or organizations suspect of terrorism acts.

Keeping the public records of the entry form will take place in a specially designed space according to the legislation and the normative documents, but not less than five years from the closing of the account to which the card is attached.

Producing personalized cards

Preventive measures for card production take into account fraud prevention through counterfeited card transactions that is avoiding defalcation of blank cards or information about the cardholders or their accounts, which can be used in making false cards.

Card transportation from the producer to the bank has to be done in conditions of maximum safety with the ways of transportation used by the bank to transport the values. During the transportation, the cards shall be packed in sealed boxes and in containers. If the headquarter of the producer is situated in another country, he shall ensure the secure transportation to the Romanian customs, from where the bank shall take it and transport it to the cards storage place.

The reception of the batch of cards shall be done in the presence of the representative of the bank who shall check the conditions of the transportation and the integrity of the boxes in which the cards are transported. The bank shall urgently inform the producer, the transporter, the international associations for card payments, and also the legal authorities in the following circumstances:

- the transportation did not followed the established time table;
- the cards were lost or stolen during the transportation;
- the containers in which the cards were transported were destroyed or opened during the transportation.

The storage of cards not personalized shall be done in the bank treasury. There will be filled in a register for the evidence of cards from the treasury and for every card type will be mentioned all the card entries, on the basis of a reception report, and all the card exits for personalization, in the basis of the issuing-receiving reports, signed by both parties (the representative of cards departament and the representative for treasury administration).

The storage of cards necessary for production shall be done in the safe equipped with a double system of controlling the access. The person charged with the administration of the cards to be personalized shall not take part in the process of personalization. She/he shall give the necessary quantity to the person who makes the personalization, including a minimum supply needed to cover the losses resulted from the process of card personalization, on the basis of a issuing-receiving report.

Personalization cards is done in a specially arranged space with restricted and surveillance systems and alarm. After each card personalization routines, will be made the report of production. The report will highlight for each type of card blank card number used, discarded, stopped from distribution and final stock. Stopped from distributing cards and discarded cards will be destroyed according to a report of destruction of cards signed by two persons. For destruction cards will use special choppers so that the remaining results can not be reconstructed.

Control of cards distribution and PIN envelopes

Preventive measures on distribution of cards and PINs are considering prevent fraud with cards issued and not received by the owner. Generated cards in the card system is active from their issue. In this regard:

- personalized cards and envelopes with PINs are transmitted separately for each unit and product, accompanied by lists in sealed envelopes. In case of any discrepancy between the number of cards / PINs and list entry will perform additional checks and will take action to remedy them before sending to the bank units.
- Envelopes with cards and PINs are delivered based a report to Service Official correspondence signed by a representative of Mail Service.
- PINs units corresponding cards will be sent only after receiving confirmation that the cards are in the bank units.

- Sending cards to bank units will be made by bank couriers or special mail aiming to ensure transport safety, to prevent their loss or unauthorized interception.

Banking units will designate responsible for:

- Cards management
- PINs management

They will acknowledge receipt of envelopes after verifying contents, or shall give notice where there is:

- inconsistencies between the contents of envelopes and lists attached
- damage or breach of sealed envelopes
- non-receipt of cards or PINs in the usual terms of the mailing date, respective 4 days after the distribution list, according to messages sent by e-mail alert.

Handing cards and PINs to owners

Units will notify owners to present to the bank to get cards or PINs.

When handing cards and PINs to the directly nominated card holders, people who are designated for this purpose, have responsibility for carrying out the following operations:

• verify the identity of the owner

• to request the the owner to open the envelope with the card, to verify the data and sign in the official banking space designed specifically for this purpose on the back of the card;

• to indicate the owner the need for memorizing the PIN and after that destroying the PIN number, to ensure confidentiality code.

• advise the owner to keep the card safe and not allow finding CVV2/CVC2 card number or code on the back of the card by other persons.

Responsible for managing cards and PINs will registered the handing to the owners, cards and PINs based on signed confirmations.

Undistributed cards to the owners:

• will be delivered daily to keep the treasury unit and registered in the Register of cash in circulation records and other values;

• Within 60 days from confirmation about the receiving of the cards in the unit, will be returned for destruction.

Data access control

Data access control, plans to prevent fraud in transactions with counterfeit cards by using information about owners and accounts from which to make fake cards. In this regard:

- user access rights to systems cards will be allocated by the directors of units limiting the access to carry out specific operations essential;
- each user access to systems will be allowed only after entering correct password, required periodic password change;
- Safety data from the cards will be achieved by informatic specific ways.

Management of reported lost / stolen cards

To prevent fraud with lost / stolen cards, the bank will instruct owners:

- keep the card safely
- not disclose your PIN to anyone
- to notify the bank on the phone(at the number that is written on the back of the card) immediately after becoming aware of the disappearance of the card.

Bank will proceed to block the card immediately after the announcement of the owner about the disappearance of the card is made through the telephone or following receipt of lost or stolen card if the holder has not previously announced telephone bank.

Transaction authorization and approval limits

Authorizing transactions provides a number of transactions by card system to reduce the risk associated with the operations, check that:

- the conditions of validity of the card:
  - the card was issued by the bank
  - the card is valid (refering to the period)
  - the control card CVV code is correct
- blocking the card as a result of its earlier declared as lost / stolen or other situations that require blocking the card;
- availability of required amount in the account card is attached;
- card usage by the owner by checking CVV2/CVC2 code or PIN code for transactions made without the physical presence of the card (operations ordered by mail, telephone or Internet)

The authorization of transactions at ATMs, POS and Internet is done on-line.

The card sistem will block the amounts of the authorized operations in owners accounts for later settlement.

There are also situations in which operations can be performed without authorization, whether the transaction value levels are below certain limits established by international organizations by type of trader and the country takes place. There are also situations in which transactions can be made without a PIN code, only mandatory for all ATM operations or for certain types of cards.

To ensure a higher level of security to the operations carried out, bank may set certain limits on the number or value of transactions authorized to identify and block fraudulent transactions or verify identity of the owner when the transaction it is done.

Management of frauds

The establishment of fraudulent transactions is done by the Department Fraud and Risk- through the analysis in the following situations:

- the owner does not confirm some operations for which they were generated alerts in the monitoring process;
- owner disputes some transactions, noting not participate directly or indirectly to the operation and its refusal, fact confirmed by the inquiry;
- are recorded transactions whose card accounts that were attached are closed or non-existent, or invalid cards, unissued by the bank.

Where appropriate, will require the submission of notices from the owners to refuse to pay, when they have not already been prepared and presented to the bank.

After the analysis, fraudulent operations will be allocated to one of the categories of fraud and will take appropriate measures to stop the emergence of other fraud cases.

In all cases, the cards involved in the operations will be blocked immediately after the finding of fraude. Bank may decide to introduce the card code number on the list of to recover cards published by the international organization.

Identified fraud will be reported to the cards organizations and the central bank, according to regulations.

In the case of lost or stolen cards, the owner is responsible financially for all operations until the bank's phone announcement or the date of notice of loss / theft, will bear losses up to the maximum prescribed by regulations in force.

Owner is the full responsibility if he acted negligently or in bad faith or intentional fraud.

BIBLIOGRAPHY

1. ACFE (2007), The 2007 Fraud Examiners Manual, Association of Certified Fraud Examiners –ACFE, Austin, TX.
2. Coy Barefoot - Revoluția comerțului electronic, Editura Almatea 2004
3. Camelia Hațegan , Codruța Pavel – Contabilitatea instituțiilor de credit confom directivelor europene, Editura Brumar , Timișoara 2011
4. Heteș Gavra Iosif, Buglea Alexandru, Heteș Gavra Roxana - Management bancar, Editura Orizonturi Universitare, Timișoara 2004
5. Vasile Dedu – Gestiune şi audit bancar , ediția a II- a Editura Economica Bucuresti 2008
6. Ordinul BNR nr 27/2011 pentru aprobarea Reglementărilor Contabile conforme cu directivele europene
7. www.bnr.ro