THE FRAUD IN ELECTRONIC PAYMENTS AND MEASURES TO FIGHT AGAINST IT

MAGDALENA RĂDULESCU
FACULTY OF ECONOMIC STUDIES, UNIVERSITY OF PITESTI, PITEŞTI, STR. HAMANGIU, NO.22, ARGEŞ, COD 110194, ROMANIA, magdalenaradulescu@yahoo.com

Abstract:
This paper presents the frauds in using credit cards or in electronic commerce in Romania, the main risks of paying by cards and the implementation of 3D Secure System in Romania. The analysis is supported by statistical data and the paper concludes with some measures of fighting against these electronic payment frauds.

Key words*: cards payments, e-commerce, electronic frauds, electronic payment security system.*

JEL classification: *L96, M15*

1. INTRODUCTION

The beginnings of cards' activities in Romania were marked, as it was normal, by fraud attempts by law breakers. As the card began to be commonly used as a payment instruments, the frauds have alarmingly multiplied. In 2000, they had substantially increased (over $ 500,000 in the second quarter), especially the cards issued abroad that were presented for acceptance to the traders within Romania. The activity of the la breakers was facilitated by the fact that, at that time, the Romanian market didn't have effective mechanisms that could protect the cardholders, the merchants and the banks.

The most important measures for limiting the rod of fraud by cards were signing an agreement which established a set of operating principles regarding the payment acceptance on the Romanian territory of the cards issued under Visa and Europay sign and establishing a database containing the fraudulent or suspected traders and which is located at Romcard (which is in charge of its maintenance and permanent update).

According to the RomCard statistics, only 0.2% of the total card transactions conducted via the Internet are frauds or complaints (chargebacks), always generated by the buyer, respectively the card owner. In over 90% of the cases, it does not recognize the transaction.

The anti-fraud system developed by GECAD ePayment checks 24 / 7 the transactions and it has two essential components: *the automatic verification* by applying filters for each transaction and *the manual verification*, in case of suspicious transactions. The automatic filters are designed to uncover fraudulent conduct in the purchasing process and taking account of:

The trading servers are daily checked so they permanently meet the standards asserted by the Visa, MasterCard, Discover & JCB standards.

2. FRAUDS BY CARDS

According to the General Inspectorate of the Romanian Police (IGP) - The Organized Crime Fighting Squad, in the first half of 2008, card frauds have grown exponentially, recording numerous cases of people found at ATM's in Romania using

credit cards fraudulently. Also, the foreign authorities have reported numerous cases in which Romanian citizens are found committing such frauds at the ATM's abroad.

In most of the cases, the criminal activities are initiated in Romania, but it aims for abroad victims or they are completed abroad, where the financial product is taken. The authors use in committing these facts, fast payment systems offered via the Internet (escrow system, paypal accounts, e-gold accounts, internet – banking accounts) or fast money transfer systems (wire transfers - services provided by institutions like Western Union or Money Gramm).

The most active areas of the country, regarding committing such kind of facts are: Bucharest, Alexandria, Ramnicu - Valcea, Craiova, Timisoara, Iasi, Sibiu and Constanta.

According to the IGP reports, it is noticed a continuing specialization trend of the law breakers both on the activities developed and from a technical point of view, for identifying new operating ways: fraudulent auctions, fake escrow sites use, transportation sites, e-commerce sites, phishing sites, hiding the traces via the Internet and the financial product circuit.

Regarding the computer field crime and means of payment frauds, it is noticed a reorientation of the criminal groups, meaning that, they seek, through the criminal activity carried out, to get significant amounts of money.

Out of the cases handled by the IGP, it results that some organized criminal networks, transnational, once operating in other areas (stolen cars traffic, even human trafficking and drugs traffic) had reoriented, committing crimes with credit cards and via the INTERNET, the amounts of money obtained illegally, as a result of these activities, sometimes being much higher than those previously obtained.

The factors which determined the criminal groups' reorientation to with credit cards crimes are:

- large material gains in a relatively short time and with relatively low risks;
- the trans boundary nature of the crimes makes their investigation by the state authorities to be much more difficult, whereas for proving the facts it's necessary, most times, to get information from the competent authorities within several countries, via the international legal assistance requests, procedure which is expensive and slow;
- the easy access to modern equipments that enable complex illicit activities development;
- the possibility of rapid movement from the territory of a state to the territory of another state of the members of a criminal group, tracking their activity being, most of the times, very difficult to achieve by the competent authorities.

Regarding the crimes against the computer and information systems in 2006, there weren't significant evolutions until 2008.

The larger cities, which are also university centers, have a significant rate of such illicit activities. Those dealing with committing these acts (hackers) are usually young, pupils or students. There aren't crimes by which a financial income is pursued, but the use of programs and services via the Internet (Table 1).

Table 1. The evolution of the crimes in the computer field

	2006	**2007**	**2008**
Determined crimes	230	256	526
Blamed persons	217	289	340
Held or arrested persons	12	32	65

Source: IGP, 2008.

3. PREVENTION MEASURES AGAINST INTERNET FRAUDS

a. Fraud via the online auctions

- You have to know as well as possible about how the Internet auctions work, what your obligations are as the buyer and what the seller's obligations are. All these, before you start bidding for a product.
- Determine whether the site that you trade on, offers insurance for the listed products and for the transportation. If so, it's preferable for you to pay this insurance.
- Find out more about the seller, especially if you only have his email address. Avoid the sellers that don't provide accurate data.
- Examine the seller's feedback offered by other buyers. If he has a negative trading history, don't make business with him.
- Learn what the seller's preferred payment method is and where he requires the payment. Avoid fast money transfer services regardless of the protective measures that you will be presented.
- If you bid on a site abroad, note on the applicable law in that country in order for you to know how to protect yourself.
- Ask the seller about the way and the delivery time and about any guarantees conditions for the auctioned product.
- Check if the delivery charges are included in the price of the product.
- Do not provide your personal identification number, ID card, passport or driving license serial and number because the seller does not need this information.

b. Fraud via non-delivering the products

- Make sure that you purchase the desired product from a trustworthy person. In the online auctions case, check the seller's reputation whenever this is possible.
- Try to get the physical address where the seller is located. Check if the phone number provided is correct and that the e-mail address is active. Avoid the sellers who use free email services.
- If the seller has a web address, check it in detail and look for other information regarding that website. Do not judge by the quality appearance of the seller's site!
- Be cautious when you trade with individuals or companies abroad.
- The safest trading methods are in the 3D Secure system, provided that your card is enrolled and activated in this system. Also, consider using a neutral system ("a third party") such as the Escrow, but only after you had inquired about the service's using conditions.
- Make sure that the site you trade on, uses a secured connection when you provide confidential information on your card.

c. Credit cards fraud

- Never offer information on the card if the site doesn't use a secured connection and if its reputation is questionable.
- Before using the site, check what security software it uses in order for you to make sure that your data are protected.
- Your card is personal. Your information is confidential. Do not provide this information to anyone until after you had ensured on the security of the transaction.

d. Investments fraud

- Do not invest in any business, basing on appearances. Do not invest in anything until you are absolutely sure and had informed that the business is legitimate.

- Inform yourself about the true identity of the person who offers you an Internet business and make sure that that person is trustworthy. Every detail is extremely important. Do not invest anything if you have the slightest doubt.
- Be very careful with the business proposals received by e-mail (Nigerian letters cases are extremely popular). Be skeptical when persons who recommended themselves as foreign officials ask for your help in moving huge amounts of money from one account to another. Do not believe in the large amounts promised you will be entitled to if you help them. Do not provide any information regarding your account.
- RULE: If something sounds too good to be true, it's very possible not to be!

e. Identity theft (PSHISHING)
- Do not access the link sent in the e-mail messages content received from unknown addresses (even if they seem trustworthy sources). Practice showed many phishing attacks in which e-mails could come from reliable sources such as: the bank where you have an account opened, your card issuing organization, etc.
- Check the site name in the browser, in order to observe the difference from the original site of the institution. Directly access the original site and not via the fraudulent link.
- Contact the bank or the financial institution for checking whether such messages were sent; in the banks' policy there aren't practiced such procedures for requesting the confidential information.
- Never give out confidential information about the card accounts (card number, expiration date, PIN).

4. CARDS FRAUDS COUNTERACTION MEASURES

In order to avoid possible damages caused by the fraudulent use of a card, we ask you to instruct the clients, the BCC card owners, as it follows:
• Immediately after receiving the card from the person responsible with the activity of the cards, the customer must sign it on the back in his presence;
• The card must NOT be given to another person;
• To avoid keeping in the same place the card and the envelope on which is printed the PIN code of the card;
• NOT write down the PIN on the card;
• the PIN is memorized and then the envelope shall be destroyed;
• NOT disclose the PIN under any circumstance and under any excuse to another person, not even the accepting trader's staff or of the bank or not even to the police staff;
• NOT making transactions at ATM's in the presence of other persons who may find out the PIN;
• At shops or other places where POS's payments are made, typing the PIN must be made carefully, using the free hand for hiding the hand in which the PIN is entered, so that the actual typing action not to be visible not even nearby;
• For online payments (Internet sites), which require typing of various card information (card number, validity term, etc.), carefully check out the site and the transactions' security means which must necessarily be specified. In the absence of any such specifications, the transaction must NOT be made!
• If the client forgets the PIN code or it was found out by another person, he is asked to report to the nearest BCC unit in order to reissue a new card;
• Urgently notify the loss / theft of the in order to block it;
• To use the mini - statement offered by the BCC's ATMs (showing the last 10 transactions made) for detecting possible frauds.

For any situations which you suspect as being possible frauds with a BCC card at the BCC or another bank terminal or another bank card at the BCC terminals, please contact the BCC Cards Processing Department or the Pay Net's Customer Support Department in order to see the STOP LIST of MasterCard and Visa and to make the necessary investigations.

In order to limit cards' frauds, the following measures had been taken:

- The existence of cash withdrawals limits on the BCC cards;
- Equipping the ATM's with video cameras;
- Checking the identity of the card owner in case of cash withdrawal from the POS's installed in the BCC units;
- Instructing by any means the BCC card owners regarding the correct use of the cards;
- The possibility to get a mini statement of account at the BCC ATM's.

5. RECOMMENDATIONS FOR DEVELOPING IN SAFETY AND COMFORT CONDITIONS THE TRANSACTIONS VIA THE INTERNET

a. Meeting the virtual store

Before buying a product or a service from a web site, users should check whether they can trust that dealer (virtual store). Thus, the first step in online trading is to inform the users about the identity of the virtual shop where to buy the desired product or service from:

- Check who the owning firm of the virtual store is and who the site's administrator is. You must find the information regarding the company's legal name and its actual existence by its Trade Registry number and unique identification code (CUI), data which you must find in that site. You can make an idea regarding the seriousness of the company by checking it on the Ministry of Finance website.
- Check the company's contact details (exact mailing address, fixed and mobile telephone number, fax no., e-mail). For your safety, test the telephone numbers displayed on the website in order to be convinced of the existence of the company and use them if something does not work during the transaction. Be suspicious if the virtual shop uses a free email service such as Yahoo and Hotmail.
- Read, carefully, the terms and conditions of using the site. Every online store must have a side entitled "Terms and Conditions" in which are specified the procedures for purchasing the goods and services.
- Check if certain restrictions are applied on the products or services sold, if there are age limits for certain categories of goods, whether or not they can be delivered to your home, if there is a limit of minimum amount to be ordered, etc.
- Try a classic contact with the virtual shop. If it's the first time you are using the site and the shop's services that you had chosen, it is recommended to contact by phone and email with the company's representatives. Write down the name and position of the persons you had talked to, check the store's response time to your written demands, test the courtesy and the information degree of the company's representatives.
- Read or listen to the recommendations (feedbacks) of other users regarding the virtual store and evaluate the satisfaction degree that they had experienced with it. If the virtual store and made a bad name among other users, don't think that you'll be the exception to the rule. Learn the views of others and note the opinion of the majority.
- Look every sign that gives an extra credibility to the virtual store, trust labels and / or trust marks (e.g. the Geo Trust icon, the logos "Verified by Visa" and "MasterCard Secure Code", the RomCard symbol, ISO type quality certificates, partnerships with

credible institutions - the logo of the Romanian Chamber of Commerce and Industry, etc.).

b. The safety of the transactions

If you pay online goods or services, verify if the company provided a secured payment system. Check also if the browser is protected and also the personal information and payment data. E.g., search for the symbol which represents a closed padlock or words like "the information provided is encrypted" or check if the site's address begins with "https:".

If you send the personal information, such as the card number, to an unprotected site or by electronic mail, it is possible for anyone to intercept them and abuse them.

In Romania, there are two types of virtual stores: the ones that operate under the SSL security standard and the ones that are configured under the 3D Secure security standard. What is the difference? The SSL standard is older and risky for the card holder who wishes to purchase a product with online payment. The store working under this standard has access to your credit card information - one can see the serial number and the verification code on the credit card. If, behind the virtual stores, there are mal intended people, the money on your card is in danger. Even in ideal situations, in which the dealer (the virtual store) is of good faith, the database that stores the persons' information on its customers' cards, can easily become the target of informational attacks.

In conclusion, avoid supplying your card details to a SSL virtual store. You can still buy from such a site if you pay, for example, cash on delivery - in this case, the risk that the information / personal data to be mal intentioned accessed, is much smaller, perhaps even 0. It is important to note that, in Romania, the processing banks don't operate under the SSL standard, but only in the 3D Secure. In other words, if you find a SSL site which accepts online card payment, the transactions' processing is made via an external processor such as the 2checkout type, money bookers, etc. or via a foreign bank.

The 3D Secure standard is, at this time, the safest global way to trade on the Internet and pay online, by card. 3D Secure is the abbreviation from 3 Secured Areas, namely the Acceptance Area (Acquirer), the Issuance field (Issuing) and the Interoperability field, which belongs to the international cards issuing organizations (Visa and MasterCard). The novelty of this standard comes from the fact that the responsibilities of the parties are divided on the three areas that I had mentioned. Thus, on part of Acceptance, the responsibility belongs to the accepting bank and those that were set up as virtual operators. Regarding the Issuance field, the responsible is the card's issuing bank together with the card holder and the Interoperability field belongs to Visa and MasterCard.

A transaction under the 3D Secure system can only run by covering the three fields. Each entity is responsible for the security degree within its domain. In addition, Visa and MasterCard have also implemented the liability shift rule in order to settle the possible disputes. By this, the responsibility belongs to the one who is not compatible with the standard. E.g., if a merchant is enrolled in 3D Secure and the issuing bank or the cardholder isn't, the virtual shop would gain in a possible dispute.

The 3D Secure security standard also brings other innovations compared to the old SSL. First, it promotes the idea of authentication which is done on two levels: a verification level of the card (if it is enrolled and activated in the 3D Secure system) and one of checking the trader. Last but not least, the card holder is verified by introducing the unique password that only the owner knows, this being encrypted only on the RomCard servers without the virtual shop knowing it. The security measure supports

the anti – carding fight by which there were registered many frauds. Also for this aspect, another security breach had been removed through which the trader (the virtual shop) had access to the serial number and the verification code on the buyer's card in the old SSL standard. In 3D Secure, this is no longer possible; the trader can't "see" under any circumstance the identification data on the card.

On the RomCard 3D Secure configured traders, look for the signs (logos) "Verified by Visa" and "MasterCard Secure Code". For your tranquility, ask a RomCard representative if the site you are about to trade, is, indeed 3D Secure configured. If the answer is positive, in order to protect the liability shift rule (responsibility transfer) in the event of a dispute with the merchant, activate your card in the 3D Secure system. This is done simply, without any additional cost, in a request to your card issuing bank.

Shortly, when you trade online by card, check if: the store is enrolled in 3D Secure, your card is enrolled and activated in the 3D Secure, and your authentication password is no longer known by any other person. If these conditions are met, your card information is safe when you pay online.

- Any payment method you had used (payment by card, cash on delivery, reimbursed payment, payment bill), always check the integrity of the good delivered.
- Make sure that the personal data you provided to the virtual store, are protected. E.g., when completing the order form, check if the transmission of the data is made via a secure connection ("https"). Check how your personal data will be used and provided and if you have the possibility to refuse them to be sold to third parties or exchanged. You should think twice before making the transaction if your personal data are not protected.

6. CONCLUSIONS

Industries, which develop fast, are often vulnerable to fraud schemes invented by those seeking to gain capital using new criminal opportunities, outdated security measures and outdated laws. The credit card sector is not an exception.

Currently, it is noticed a tendency to increase the damage caused by crimes within the banking technologies.

The crimes committed with the use of cards can be assigned to the most dangerous economic crimes, due to the fact that the negative impact is turned back not only on the bank's activity, but also on other subjects.

The executory authorities continue to face new and complex fraud schemes, including credit card crimes against the financial institutions and the companies producing bank cards. The criminals act with the help of people who have easy access to the information about the credit cards - as are officials from the credit card agencies, people responsible for luggage passing through airports and postal couriers up to organized groups involved in large-scale cards' theft, manipulations and counterfeiting activities.

In Romania, fraud is of 4 euro at 100,000 traded with Visa cards, while in Europe, Visa cards' fraud is of 58 euros in the same amount traded. Although there were frauds in Romania, their level is insignificant, the fight against fraud has increased once with the implementation of CIP cards. According to the Visa data, at European level, on the cip cards' markets, there is a decrease of the fraud up to 0.012% in 2008 from 0.026% in 2003.

As for the change of magnetic strip cards in CIP cards, no bank will change them overnight, but they could be automatically replaced at the expiry of the current cards, which would mean that, within two to four years, they could be totally replaced.

REFERENCES

1. **Gămulescu, C.; Manolea, B.; Taloi, L.** (2008) *Studiu privind dezvoltarea comerţului electronic în România*, Editura Economica, Bucuresti.

2. **Rădulescu M**. (2006) *Monedă şi credit*, Editura Sitech, Craiova.

3. **Rădulescu M.** (2007) *Operatiuni interbancare de plati si incasari fara numerar. Transferuri bancare si compensari*, Editura Paralela 45, Pitesti.

4. RomCard, (2009) 3D Secure System, [Online], available at http://www.romcard.ro/nou/tds.php , [accessed at 30 April 2010]

7. Payment Council, (2010), *New Report Reveals Massive Change in the Ways We Pay over the Last Decade* , [Online], available at http://www.nocash.info.ro/category/analize/ , [accessed at 30 April 2010].

8. VISA, (2010), *Serviciu mai rapid*, [Online], avialable at http://www.visa.ro/acceptare/main.html, [accessed at 30 April 2010].