SAFETY MEASURES USED TO PREVENT FRAUD FOR ELECTRONIC PAYMENTS

Lecturer candidate to PhD **Gabriela Bologa**
AGORA University

Abstract:
Information supremacy has become the main element of progress in all domains and it has determined a change of the traditional payment systems as well as a greater attention to banking security and fraud prevention. The global security system of a bank must comprise political, security, control, testing and technical elements.

Key words*:* environment, micro payments, electronic wallet, banking fraud, banking security.

The 20th century has defined itself by information supremacy which has become the main element of progress in all domains. In 1995 new notions appear in the USA such as: **new economy or informational economy or computerized (digital) economy or electronic economy**, terms which all defined a new type of society about to happen.

The technological support of the new society is carried out by the convergence between **information technology, communication technology and digital support output** which opens new perspectives in modernizing services, production of material goods, competition, management and efficiency, with beneficial effects for all social layers.

The model of the society of the future has determined new challenges for governments and their institutions, business and academic communities, society, citizens and consumers in order to understand adopt and comprehend the new dimensions of human relations. In 1999 the European Commission adopts the document **eEurope- a Informational Society for all,** which urges the speeding of the process of digital technology implementation in Europe and the electronic competence acquirement to ensure a wide use of these technologies. The initiative has a central role in the calendar of economic and social renewal which EU intends and it is also the key element to modernizing the European economy.

In the terms of such large scale changes, a change in the traditional payment systems has become a necessity. On one hand the old payment instruments have been modified and adapted and the credit card and the electronic checks are now used for internet operations.

A newer direction is represented by micro payments and the electronic wallet which take us in a completely different direction from the traditional system which involve banks in any payment operation.

The monetary innovations which allow the clients a long distance contact with their bank, company address and home are called **home banking.**

The new support is represented by human voice on the phone which communicated the payment instructions. The advent of computers has determined new progress by the use of prerecorded messages for each product/service, the use of key words for each type of service, the reception of messages from clients and even by affirmative or negative answers to requests.

Later developments have diminished the role of voice phone in favor of communication through the computer which has become more secure, allowed the transmission of precise instructions under electronic signature and access to all electronic banking products and services.

The new distance payment channels have conquered the market. They are represented by internet banking, videotex and mobile banking for the population market and by multicash and cash management for companies.

The development of card activities had emphasized certain imperfections in terms of operation security and usage methods by holders.

- **Security measures used for electronic payments**

Security measures such as holograms, PIN, specific signature have proved insufficient and new measures have been introduced such as the limitation of the authorized sum, of the number of daily transaction from a retailer, the confrontation of identifying elements with those in the data base and other parameters specific to each bank.

At the same time the technological improvement have lead to the replacement of paper base to the electronic base and to the extinction of the phone transmission, which, in some areas, are still prone to fraud.

The newer protection measures involve the codification of the messages sent by phone but this system is complicated, expensive and not completely invulnerable.

In case of more valuable transactions, the retailers have began to interrogate the emitting bank and the card holder about the reality of the transaction, measure which involves an extra answer and a delayed authorization, but the method has proved extremely efficient.

The card banking practice has shown that fraud is mostly produced by in the accepting stage and is determined by the card holders or by other people.

- **Fraud determined by card holders**

a) The holder's use of the card without the existence of necessary amount in the account for several operations which do not require authorization (under the authorization limit), speculating the fact that the operation will not be checked; the emitting bank refuses the operation and the accepting bank will face the retailer. The solution is the authorization for all situations in which risk may be involved.

b) The use of the card for transactions which the user does not admit later either intentionally or form other reasons (the use of the card by another family member without the knowledge or permission of the holder). In this case the

problem of the quality of the selection of bank clients rises as well as that of the preoccupation of implementing a banking culture.

c) The transmission of the card to other people who make transactions (usually abroad) without the holder's knowledge or realization. Another problem which occurs is that of the relation with clients, especially at the beginning of the period of card usage.

- **Fraud determined by other people**

d) When the card number is found out by another person in different ways and when the card is used for fraud. Example: when somebody uses the card in a shop, restaurant or in a hotel for transactions which are recognized and the number of the card is transmitted to people who use this information to commit fraud; or when the card number and its validity are transmitted by internet in order to access to a certain site or to pay for something and when this confidential information is found out by a hacker who misuses it. This is the reason why many emitting banks limit the access of card in internet transactions.

e) When people copy the magnetic band of a valid card whose attached account is fed by another card for commercial purpose, the operation is called skimming and it is very difficult to trace.

f) When stolen/lost or counterfeit card are used by means of retailers' ignorance or their complicity. For example in case of lost/stolen cards the retailer accepts operations below the authorization limit without consulting the list invalid cards. In the situation of counterfeit cards, when more valuable goods are purchased (jewelry, electronic goods, designer clothes etc.) the retailer may not check the card attentively and find out it is not authentic or they may not be careful enough to require the consultancy of the real holder. This type of fraud is recuperated when the real holder requests it first from the emitting bank which goes to the accepting bank which, in turn, requests the sum from the retailer. With a view to prevent this type of situations, the accepting banks either take out an insurance policy or they impose a collateral deposit on the retailer, which would guarantee possible future fraudulent transactions.

Generally the card with processors have proved much safer as fraud is insignificant is their case. Statistics have proved this and more viable security procedures are expected as a consequence to the use of these cards..

The bank must offer firm and quality services to consolidate the trust is their name and brand. As a result, they organize a sophisticated internal check to invigilate their electronic system and to prevent possible fraud and attack attempts, which has become a major preoccupation.

Study shows that electronic systems are more vulnerable to internal attack and less vulnerable to external attacks because internal users have an easier access to information. In the present stage of internet-banking development the highest risk is that of transaction (fraud) due to the fact that the system of telephonic transmission is vulnerable to interceptions.

Here are some recent types of attacks:

- sniffers- monitoring programmes which scan the users' names and passwords when they enter the bank internet site.
- Password finders- programmes which test the great number of possible combinations to get access to a network.
- Raw force- a technique which captures coded messages and then reads them by means of breaking programmes.
- Interception- the interception of transmissions and further use of information.

In order to protect systems, firewalls have been invented. They are a combination of hardware and software which are placed between two networks and through which data recording and wide range of security elements have to pass.

The market risk is more present in the area of stock exchange operations. The fast growth of this domain and the online transactions through the internet may lead to an increase volatilization of stock and consequently to necessity of high amounts of cash. The involvement of the bank in broking operations through the internet or an exposure to high risk must be analyzed with professionalism. As in the situation of cash risk, the effects of on line operations on the volatilization of the market must be monitored, both by banks and further authority.

The strategic risk occurs in the situation of incompatibility between the strategic objectives on one hand and the fulfillment possibilities on the other hand. This risk occurs at the introduction of new products on the market, which in the presence of the internet can lead to substantial changes for the competitors. Most of the times the banks are too willing to appear on the market as soon as possible and they do not test the product /service enough or its implementation is not adequate (especially staff training) and, as a consequence failure may happen which leads to unfortunate situations such as losing clients. That is the reason why we must analyze if we need an expertise to identify, monitor, control the risk and ensure that the objective may be accomplish according to other bank purposes and risks tolerance. Through its nature, the strategic risk is more general and widely spread than other types of risk because management decisions may have implications on all types of risk. An industry such as the internet may bring substantial advantages if the strategy and the manner of conception as well as the implementation of a product/service are adequate.

The reputational risk is determined by the negative impact of the bank's activity on the internet on the public opinion as a result of dubious activities, disrespecting clients' confidentiality, easy promotion of products/services and lack of response to clients' request.

The reputational risk may expose the bank to losing clients, reduction of income and even law sues due to disrespecting obligations for the facilities presented on the site.

The internet operations make the bank more dependant on the partners who supply the technological support and who may not keep the high standard of their

services. That is why the bank must check, manage and monitor this risk and receive information about the suppliers' plans of ensuring the activity.

Another important aspect is the possible faults in the security system of the bank's site, which the client could notice by accessing the site. In order to protect itself from these threats, the bank must develop and maintain high standard performance, revise and periodically test solutions for further activity as well as continually improve the communication strategies.

The management of the internet banking operation risk is a new domain which requires a certain banking technology of identification, assessment, monitor and control of risk exposure. Currently, there is a dilemma about the elaboration of an internal technology or the choice of an external technology which should be implemented by a specialized company. Moreover, we are witnessing the outlining the idea that the entire banking operation on the internet should be left in the hands of a specialized company (out-sourcing), especially for the banks which do not have the necessary infrastructure.

In order to manage the internet banking risk, the Electronic Banking Group in Basel recommends a set of 14 principles, as follows:

1. The Direction Committee and the administrators must organize the effective invigilation of the on line associated risks, including the establishment of specific accountancy, politics and control elements. As a consequence, the strategy of the bank must be revised and a specialized department should be organized to invigilate the risks according to network vulnerability and information sensitivity.
2. The Direction Committee and the administrators must revise and adopt the key aspects information security control. This involves the establishment of the authorizing method, the physical and logical access control and an adequate security infrastructure. At the same time, management is required in the situation of external threat by means of several methods such as anti-virus programmes, programmes of detection of fraudulent network entry and the testing of the penetration degree of the internal and external network.
3. The Direction Committee and the administrators must establish a collaborating policy with their partners to offer internet services. Bank management must assess the partnership risks, must analyze the competence of their partners and must request internal and external audit.
4. The bank will have to take the necessary measures to authorize and identify clients who operate on the internet. The bank must use secure methods to identify (PIN, password, smart card, digital certificate) and authorize clients in order to reduce the risk of identity theft, fraudulent account operations and money laundry.
5. Banks must use transaction authentification methods which should promote non-repudiation. Non-repudiation requires the production of an evidence of the origin of the electronic information delivery to protect

the sender against false negation form emitter. The best known way is the granting of digital certificates, which along with the digital signature allow the unique identification of the emitter.

6. Banks must ensure the necessary measures to separate adequately the tasks of the internet banking, data base and application systems. The separation of the tasks is a usual measure which ensures security that the transactions are authorized, recorded and monitored correctly.
7. Banks must ensure the authorized control and the access conditions. In order to sustain the task separation, banks must strictly control authorization and access conditions.
8. Banks must ensure the integrity of the data. The integrity of the data refers to the fact that both stocked data and transit data cannot be modified without authorization.
9. Banks must ensure the existence of traces for audit. Since information is electronic, only some situations will undergo audit, such as: openings, modifications and closure of accounts, transactions with financial consequences, transactions over the limit, granting, modification or withdrawal of rights to access the system.
10. Banks must take the necessary measures to ensure the confidentiality of information. Banks must make sure that all recordings and information is available to authorized personnel only and that all the confidential data is protected from unauthorized access. The misuse of information or unauthorized exposure of data may pose a legal risk to the bank, as well as affect its reputation.
11. Banks must make sure that the information available on their web pages is adequate and allow potential clients to make an idea about the identity and the status of the bank.
12. Banks must take the necessary measures to ensure the compliance to confidentiality rules applied in the area where they offer internet services. Banks must make all efforts to adjust confidentiality measures to the existing laws and regulations, to present polices to its clients and to avoid the use of private information in unauthorized or forbidden purposes.
13. Long term continuation of activity. Banks must offer long time and foreseeable services for its clients. With this purpose, the current capacity and and predictions must be correlated with dynamics of the ecommerce market and with the future rate of acceptance of internet services by its clients.
14. Banks must develop adequate plans to handle incidents in order to limit and minimize problems which occur unpredictably, including internal or external attacks. These actions refer to mechanisms of identification of an incident or crises right away, communication strategies with mass-media in case of attack and safety links, the simple procedure of alerting

the authorities and the procedure of informing clients and mass-media about possible problems in the system.

Electronic Banking Group mentions that these principles are not finite. They will be added and improved. They are not compulsory either. They take the form of recommendations meant to prevent unwanted events and to ensure confidence in internet banking.

Electronic security is defined by some as "the set of necessary policies, recommendations, processes and actions to minimize the risk resulting from electronic transactions, risk which refers to system intrusion or theft" and by other as " any means, technique or procedure used to protect the volume of information in a system." The value of information in based on its integrity and if the security system does not allow the fulfillment of this request, information loses its significance. In this context, the specialists of the World Bank consider security as a means of adding value, and it has become a major preoccupation of any institution.

The global security system of any bank should comprise policy, security, control, testing and technical components. The World bank recommends a security system to internet operations on 12 levels: the security responsible, autentification, firewalls, active filter of the content, intrusion detection system, anti-virus programmes, cripting, vulnerability testing, adequate administration of the system, management application of the policy of the bank and reaction to incident plan. The key aspects of the functioning of a security system are: access, authentification, trust, non-repudiation, confidentiality, availability.

Bibliography:

1. Dedu V. – *Gestiune şi audit bancar,* Editur Economica, Bucureşti, 2003
2. Gabriela Fiat, Oana Petrişor-Mateuț - *Monedă şi credit. Aspecte teoretice şi aplicative*, Editura Eurobit, Timişoara, 2005,
3. Pavel Ungureanu– *Banking. Produse şi operațiuni bancare*, Editura Dacia, Cluj Napoca 2001
4. www.carduri.ro
5. www.platielectronice.ro
6. www.bnr.ro