ANALELE ŞTIINŢIFICE ALE UNIVERSITĂŢII „ALEXANDRU IOAN CUZA" DIN IAŞI
Număr special Ştiinţe Economice 2010

NEW TRENDS CONCERNING OPERATIONAL RISC IN E-BANKING

Ioan TRENCA
Babes-Bolyai University, Faculty of Economics and Business Administration
Cluj-Napoca, Romania
itrenca2002@yahoo.com

Hadrian SILIVESTRU
Babes-Bolyai University, Faculty of Economics and Business Administration
Cluj-Napoca, Romania

Dragos PAUN
Babes-Bolyai University, Faculty of Economics and Business Administration
Cluj-Napoca, Romania

Abstract

Through alternative channels which the bank provides to the customers transactions were conducted worthing 18.58 million euros, up 59% over the same period of the last year, according to RomCard, in the first 3 months of 2009. We have tried to summarize below the risks that banks face when they launch an e-banking product type on the market and how they an manage themselves.

Keywords: e-banking, alternative channels, operational risk
JEL classification: G21, G32, O14

Rapid changes that occur in banking and IT, in particular, in recent years, have revolutionized the way in which the banks deliver services and products to the clients so much that each of the banks tries to come up with solutions as fast as possible in order to help customers in conducting their activities. E-banking has some special characteristics that lead to increased and changing risks considered traditional banking activities.

These characteristics are:

- extraordinary speed of change in technology;
- open and global nature of electronic networks;
- integration of electronic banking with the core of banking;
- increasing dependence of banks from third parties, which develops software applications necessary to run the e-banking.

Due to rapid changes occurring in technology, banks are faced with specific risks of electronic banking and electronic money activities. At this level, it appears that operational

risk, reputation risk and legal risk are the most important categories of risk, especially for international banks. Operational risk arises from potential loss due to significant deficiencies in the integrity and viability of the system. Security considerations are supreme, where banks are subject to internal or external attack on their products and systems. Operational risk may arise from non-proper systems of electronic money or electronic bank, and from inappropriate development or implementation of these systems. In this category falls the following risk:

Security Risk. Controlling access to bank systems became increasingly complex because of the developed computer capabilities, geographic dispersion of the access points and use of various communication channels including public networks such as the Internet. Unauthorized access to the network could lead to direct losses, adding some debts to clients etc. It could also be a variety of issues of specific authentification and access. For example, inadequate checks could lead to successful attacks of hackers who operate through the Internet, who could access, save and use confidential information about customers. In the absence of adequate controls, a third person may have access to the computerized system of the bank and could set up a virus in it.

In addition to external attacks on bank electronic systems and electronic money, banks are exposed to operational risk in terms of employee fraud. Employees could purchase clandestine authentication data related to accessing customer accounts or stolen cards with stored value. Errors due to employees could also jeopardize the bank systems. A special importance for surveillance authorities is the risk of infringement of electronic money, which according to the Criminal Code represents a crime. This risk may be increased if banks fail to incorporate adequate measures for discovering and preventing counterfeiting. A bank faces operational risk of counterfeiting and becomes indebted with the amount of the balance of the electronic spoofed money. There can also appear costs due to *repairs of a compromised system risks* related to the design, implementation and maintenance systems. Thus, a bank is exposed to the risk of a breakdown of its systems, if the electronic bank or the electronic money elected by the bank is not compatible with user's requirements. *Risks arising due to improper use* by customers of banking products and services. The risk is increased when a bank fails to properly educate customers on security precautions. In addition, if there is lack of adequate measures of verification of transactions, customers may reject transactions they authorized in the past, thus creating numerous financial losses to the bank. Customers who use personal information (authentication information, numbers of credit cards etc) in an uninsured electronic transmission may allow malicious people to gain access to their accounts. As a result, the bank may suffer financial losses due to unauthorized transactions. Money laundering can be another source of concern. *Reputation risk* is the risk due to a significant and negative public opinion which consists of a critical loss of the funds or bank's customers. Reputation risk can occur when the bank's shares produce a major loss of the public's trust in the ability of the bank to fulfill critical functions to continue the activity. Reputation risk is important not only for a single bank, but it is important for the entire banking system. *Legal risk* appears through the violation or non-conformity with laws, rules, regulations or practices prescribed or where the rights and legal obligations of the parties participating in a transaction are not set correctly.

Banks engaged in the activities of „e-banking" or „e-money" may face legal risks relating to disclosure of information on customers and the protection of banking secrecy. *Operational risk*, the risk of loss resulted from non conformity or inadequate internal processes, personnel, systems or due to external events. Operational risk specific to e-

banking includes the following factors: security risk; the system design, implementation and its maintenance; the lack of information on bank products and services by banks' customers.

Security Risk

The access control to the bank's system has become increasingly complex since increasing computer capacity, geographic dispersion of the access points, using various routes of communication. It is important to know that the unauthorized access to a bank may have significant losses, which will impact on both customers and bank's image. A great variety of attacks can happen such as attacks via the internet on the bank's system due to the lack of security, implantation of computer viruses, and unauthorized access to customers' accounts and their data. Besides external attacks, the banks may be vulnerable to attacks from their own internal employees who have access to confidential data of customers and they can use for personal interest. Also from the operating mistakes of the employees, the banks are exposed to high risks.

The system design, implementation and its maintenance

The banks are also faced with a situation where the chosen system for the Electronic banking application is not well defined or implemented. For example, a bank is exposed to the risk of interruption or slowing down of the main system if the electronic banking system is not compatible with the application of core banking. Many banks use the services of third parties to implement and support the application of e-banking. This externalization of services enables banks to reduce maintenance costs, monitoring and modifying the application, but represents a source of operational risk because the suppliers chosen for this operation might not rise to the bank's demands, or fail to fulfill the terms of products' delivery.

Lack of banking services and products by bank's customers

The operational risk, in this case, may arise where the bank does not succeed to „educate" its customers concerning the use of application and PC's security. Also, problems can occur when customers, after previously authorized a transaction, after a while they send its cancellation which leads to financial losses from the bank.

As shown, the e-banking operations increased very much. We can talk about a growth resulted from the flexibility of the programmes offered by the banks and from the benefits that the customers have by using these services: reduced costs of administration; fast transactions; lower fees than at the bank's desks.

The development of e-banking services brings, besides the benefits, also higher risks which are mainly due to the security of informatics systems. When we talk of security in e-banking, the first things that we think are usually computers, the connection between them and the bank, and how we can secure. Often, however, security in e-banking is not only the computers and connections, though they remain extremely important and sensitive. If we talk about computer security in the context of e-banking, both sides must be considered in the transaction: on the one hand, the bank itself and its connectivity with other banks and, on the other hand, customers. In terms of safety and security measures to be taken in the banks to ensure optimum security for electronic transactions, Romania has taken measures in accordance with the provisions and international practices. In this sense, the rule of

participation in the interbank discount system is very strict; the NBR responds of its surveillance. Restrictions are imposed on both the infrastructure - computers that are connected to electronic payment system to be in a network separated from the bank's network, the equipments provided by Transfond to be positioned in a special room, lines of communication to meet the technical criteria, and have redundancy - but also on the staff who are allowed to work with such equipments who must be certified and accredited. All these, according to the provisions in force, are audited annually by independent auditors who must be certified by CISA (Certificated Information System Administrator). They analyze the compliance and conformity with all restrictions imposed by the NBR / Transfond upon the infrastructure, processes and personnel. In Romania there is currently about 50 certified auditors by CISA, of which 3 work for Ensight Management Consulting.

From the other side, of bank's customer, security measures are less regulated, and the vast majority of them are recommended by the banks, or as a result of IT customers' education. The bank is generally responsible for providing access to the e-banking through a secure website on the basis of a certificate signed by an international authority (ex. Verisign), so the identity of the owner to access the page can not be disputed. Additionally, banks can resort to the use of so-called Digipass devices. Digipass is a security device that generates a password - token. It is accessed by entering a PIN (personal identification number), and the password generated by the device offers the user the possibility to access the service "Internet Banking" and to perform operations via the Internet. Thus, through the double authentication (username, password and security code generated by digipass) the possibility of an „identity theft" is greatly restricted. Thus, someone who managed to enter fraudulently in the possession of the username and password (username and password written on the sheet of paper agglutinated on the monitor, or just said by mistake, etc.) needs digipass device and PIN. Also related to the customers' authentication to the e-banking service, Bank of America has introduced a system through which it is verified the computer from which the attempt to authenticate is made, and if it is not stated, the person who is trying to authenticate have to answer additionally to a standard question (ex: parents' names, the name of the pet, etc.) However, the inventiveness of those who want to transfer fraudulently the others'money in their own accounts knows few limits. Thus, was born one of the most common tricks used to gain access to accounts: phishing.

Phishing is described as a criminal activity focused on social engineering, which is trying to obtain confidential information (username / password, etc.) by masking the message that they require as coming from a trustworthy entity. In the definition of this activity it is specified that this type of activity is going on in the communication of e-mail type. The most commonly used method of phishing is the inclusion of a link in e-mail, a link that leads to a site which is similar to the bank's site (it does not belong to the bank), where you are asked to login. Another commonly used method is to send mails with attachments (photos / postcards, etc) but they are in fact tools that memorize and send forth all that is typed on that computer. For example, last the Swedish bank Nordea was the target of such an „attack". It lost over 1.1 million dollars in the last 15 months and approximately 250 customers of the institution have been fooled. Bank's officials have said that criminals sent e-mails to bank customers, inviting them to open up attachments, which are indicated as anti-spam applications. No statistics are gladding; the first effect is the decrease of trust in e-banking. For example, in Britain is estimated that around 600,000 users of e-banking have renounced the use of this service for fear of phishing attacks. The only effective „treatment" in this situation is the education of the customers by the banks. This can be done but only by a specially

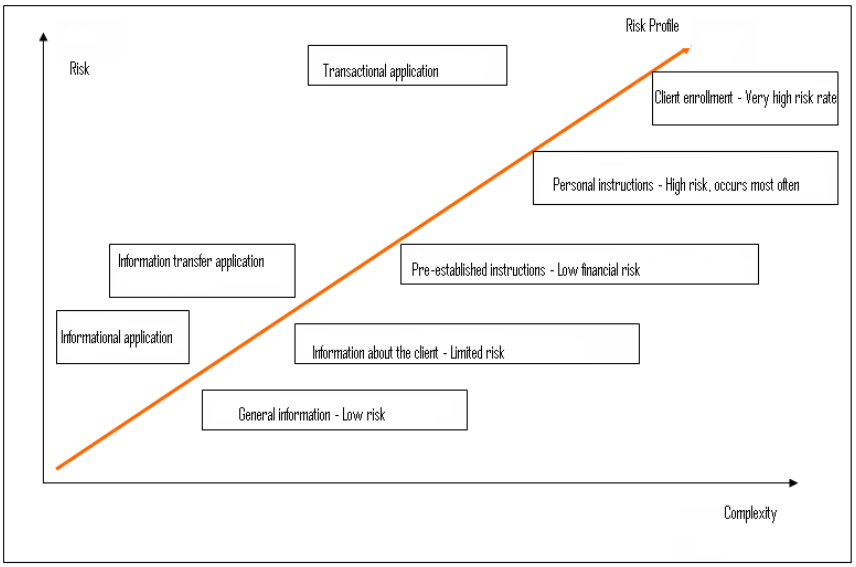
trained staff of people accredited and certified in information security. As mentioned before when talking about security in e-banking we do not only refer to computers, connections and their security. The most important „non-informatics" risk that may generate a need for security is that of violation or non conformity with laws, rules, regulations or prescribed practices or incorrect determination of legal rights and obligations of parties to a transaction.

The banks engaged in the activities of „e-banking" or „e-money" may be faced with legal risks relating to disclosure of information concerning clients and protection of banking secrecy. Problems in this regard can arise from many causes: poorly conceived system, human errors.

A risk that can arise directly from what we mention above is the image risk, the risk due to a significant adverse public opinion, which will lead to the loss of funds generated to the bank or customers. Therefore, besides the quality assurance of the electronic systems and their audit, as well as of the staff who work with them, is always necessary to have detailed procedures that answer the questions what, when, how and by whom shall execute a certain task. Both procedures and their results must be audited by a lawyer. The most common threats to e-banking are as follows:

- identity theft;
- incorrect definition of rights to use the application (in cases where the client has administrator rights on the bank);
- poor support processes;
- therefore, the risk of fraud is much higher and faster than was and so far the most important factors are:
  - increasing complexity of organizations;
  - inadequacy storing data;
  - faulty management, lack of supervision of operations;
  - errors in the financial and business chosen models

As shown above, the risks coming from using the applications of e-banking offered by banks are countless, but for their limitation it is needed a professional management of banks.



Source: [Basel Consulting Group – Addor Jean Pierre, 2007]
Figure no. 1 Risk vs. Complexity

Banks face a dilemma when they decide to choose a system of e-banking. The more the complexity degree of the used system is, the emerging risks increase in proportion to it. However, should not be neglected the incomes from the use by customers of a complex system in which the client has a multitude of advantages. These things should be well established by the bank's representatives when they decide to purchase certain applications. The banking companies worldwide have provided distance services for their clients well before the apparition of e-banking. Electronic funds transfer for low payments, the administration of cash and machines from where someone can extract money (ATM) by the customers' banks were and are usual presences in countries with banking tradition and in also Romania. However, the provision of financial services at distance using methods likes the Internet, phone, caused massive changes in the financial banking industry. Issues and trends that manifest themselves as carriers of risk in terms of the electronic character of delivery of financial services on the internet or phone are caused by various factors such as the speed with which are introduced new products and services on the market, with the desire to advance competition, speed of processing transactions as a result of spectacular developments in telecommunications, in software and hardware. Unfortunately, this new frenzy in adopting and implementing new technologies is less accompanied by knowledge and experience working with new technologies and with the risks brought by using these technologies. Collecting, storing and sharing data on customers can lead to problems related to confidentiality of client's data and this can lead to the apparition of the legal and reputation risk.

Given the link between technology and e-banking, the operational risk is the most frequent occurrence in providing electronic services. To limit this risk, the banks should consider implementing a technology architecture integrated to a corporate level to facilitate interoperability, to ensure the security, integrity and availability of data and enable the man-

agement of relations with third parties delivery service. How technology is changing dramatically, the business model and operational processes, the banks need to implement and maintain appropriate procedures of control- including change control and implementation of audit processes.

The risk related to security represents for most bankers interviewed by the Electronic Banking Group the main concern related to e-banking. Outside threats such as hacking, sniffing, spoofing or denial of service expose the bank to new risks related to security. Open delivery channels for e-banking create new security problems for banks in terms of respect for confidentiality and integrity of information, gladding of transactions, user authentication and access control. Among the main problems that bankers want to solve as quickly as possible is the development of more robust tools for verification of identity and authenticity of applications demands of large value transactions

In addition, banking industry should continue the work to determine the requirements for developing the best encryption methods, including electronic signature and the legality and electronic documents. Was performed over time, in many organizations, that attacks from the inside, made by employees are more frequent than those from outside. A security with problems could lead to the reputation's damage and even legal problems due to the inability of the bank to protect the personal data of customers.

Data integrity - is an important component of the system's safety. Banking organizations are forced to improve their interoperability inside and outside, to manage effectively the relationships with customers, with other banks or with the service providers. Until standards are created for the management of information stored on electronic support, the banking organizations will continue to be entered in the race to establish the most effective processes to ensure the accuracy and integrity of data transmitted and received. Given the low cost and pervasive nature of the Internet, organizations are using increasingly the protocol TCP / IP as standard protocol for communication. There are many benefits as a result of using this protocol but, banks must ensure that data transferred between electronic existing systems and the third parties systems with whom they interact are properly translated and integrated for use of this standard communication protocol.

Moreover, while the introduction of middleware and languages such as XML (Extensible Markup Language) facilitate this effort, the development of standards to the banking industry's level to support these new technologies is still in its early stages. System availability - to ensure a secure internal network for their e-banking, the efficient planning of resources is critical in ensuring continuity and availability of e-banking services. The volume of transactions may have a high volatility due to automation and increasing costs per transaction. Also, competition pushes banks to declare that the services offered are available 24 hours from 24, 7 days in 7, and this led to a considerable increase in customer expectations while reducing the tolerance to errors.

To meet competition and to avoid the potential risk significantly related to reputation that can occur under conditions of interruption of delivery services due to the system's overload, banks should provide optimum combination of safety products and services characterized by accuracy and consistency. These factors diminish the importance of continuity of effective service delivery, recovery from error, and plans for responding to incidents. Moreover, the fact that many banks turn to third parties for the provision of e-banking services, require regular checking of their capacity to ensure continued provision of services and the existence of these plans in error recovery and response to incidents - as ef-

fective as those established in the bank. Attacks like denial of services can reduce or eliminate the ability of bank to serve customers during the attack.

These attacks have become increasingly common and have been directed against the biggest players in e-commerce market. An additional challenge is the inability of the bank to control the availability of the Internet as a network. In conclusion, a bank should consider, as part of a plan to solve the adverse situations that may occur, alternatives to deliver services in the case of a major event leading to discontinuation of the operation of part of the Internet

Internal Audit and Control - the ability to detect and correct errors is a critical component of the system of internal control of any banking operation. Moreover, banking organizations should have sufficient operational control procedures to prevent fraud from the outside or inside and protect information and the bank's assets. Much of the efficiency and reduce costs of e-banking is the ability to implement immediate processing, processing which is done automatically, without human intervention. While the benefits of automated processing of transactions are numerous, the reality is that e-banking modifies the way in which the internal control procedures, the sharing of tasks and responsibilities of information and keeping track of transactions for audit are applied on public access channels. Challenge due to these changes is accentuated by the lack of skills and experience in the industry both in scope and operational area of audit. Going forward in this way, banks will be required increasingly more to ensure that the environment provides powerful automated control and that these processes may be audited independently.

Subcontracting –the fact that for the development of e-banking industry, the banks were forced to subcontract significant parts of the operating gear affects to a large extent the risk profile of banks regardless of their size. The large banks subcontract increasingly more activities, as their development, trying to channel their efforts only upon their function and competence, its main activities outside the sphere of banking competences being outsourced to third parties. Small banks often need to subcontract parts of the work carried out because of lack of expertise and lack of technical expertise and resources necessary for the construction of channels for the supply of e-banking services. In addition, low market price of ready-made solutions, decreased financial effort of small banks to provide e-banking.

These developments are beneficial for the market because they allowed entry into the competition of smaller companies but also brought new challenges in the management of operational risk management, relations with third parties having impact on the management of several categories of risks. Studies of EBG have indicated that banks tend to rely on a relatively small number of suppliers, the suppliers being mostly institutions, medium and small-sized. In some cases providers were new companies on the market with a short history. This dependence on a relatively small number of providers presents a safety concern for supervisors that could have implications at the systemic level, of banking industry, if such service provider would face major problems. To properly manage the risks associated with subcontracting, banks should take all precautionary measures and to constantly monitor the relationship and work with service providers.

Terms' accuracy from the supplier contracts of service should also be better evaluated to reduce the risk of violation of law in force. Processing and risk management operations to maintain security, integrity and availability of services are complicated because of subcontracting. Moreover, many service providers and partners, subcontractors, are established and new companies may have gaps in knowledge about the rules of banking. Minor disruption of activity at the service providers can have major effects in terms of image bank, can lead to

significant financial losses and is a significant legal risk. Complexity in risk management is notified of the relationship of interdependence between partners who subcontract operations related to e-banking.

Subcontracting may lead to supplementary risks to preserve the confidentiality of customer data. Banks may be in ignorance of the facts regarding the collection and use of data on customers to third parties subcontractors. To avoid such ambiguous situations, banks should pay great attention at the time of conclusion of contracts with third parties for the subcontracting of e-banking services, provisions relating to confidentiality and sensitive nature of data managed.

The evolution of information technology also reached the banking services both to optimize the existing information system and to expand it. It is important that each risk-bearing operation bank has policies and procedures related to assessment, management and reduction of the risks involved in that operation. E-banking is a new way of providing banking services. It has brought new risks in the system and therefore a need to create tools for managing them. Information technology has evolved a lot, both in terms of channels and communication protocols, hardware components and in terms of innovations in the field of software solutions. In the continuous battle to gain competitive market share represented by users of mobile devices or computers connected to the Internet, banks have made the step and have invested in implementing solutions to transfer the customers who were waiting hours at the banks desks to electronic applications. The speed with which they wanted to appear on the market with these services in order to benefit by the offers' ace of singular services led to the increase of risks factors related to security, application security, confidentiality of information. Detecting these risks, the Banking Supervisory from Basel has developed a set of principles by which expresses its requirements on the supervision activities of e-banking and some guidelines for promoting the solidarity and security activities involved in e-banking, keeping the flexibility required for the implementation that comes from the evolution speed of this area. Due to the fact that a single solution or way of risk management involved in the e-banking would not match all the enterprises which held such activities, the Committee does not provide specific technical or standard solutions in this field. The segment of Internet banking services is growing. Seen only as a channel of distribution, its benefits seem modest. However, by integrating with other channels, Internet banking becomes a powerful tool by which banks can improve customers' satisfaction and create combined favorable sales. Through continuous investment in technology, credit institutions respond to changes in the field. Although apparently virtual services open great possibilities, should not be neglected any traditional branch, because there are many aspects of banking which can not be translated into electronic format. The general trend is that banking services involving high added value to remain in traditional bank. Although distribution channels have diversified due to technology, the real challenge for banks is not to deliver products and services by any means, but their ability to provide the same information, with the same degree of relevance, whatever the means of interaction with client is. The link bank customer is becoming more complex, and the adaptation of services on demand is decisive in the competition. Accordingly, it is necessary to integrate distribution channels and centralize information to obtain a full picture of the customer, both in financial terms, and by the inclusion of socio/cultural aspects. An important aspect related to the virtual bank is that it will not replace the traditional bank, but appears as a complementary component, created in addition to a bank already known, as an alternative to the transactions.

References

[1] Basno Cezar, Dardac Nicolae - "Riscuri bancare. Cerințe prudențiale. Monitorizare" EDP, 1999;
[2] Basno Cezar, Dardac Nicolae - "Management bancar ", , 2002;
[3] Basno Cezar, Dardac Nicolae. "Operațiuni bancare instrumente si tehnici de plata.", EDP, 1996;
[4] Butler C., Mastering Value at Risk, Editura Financial Times Pitman
[5] Trenca Ioan, "Metode si tehnici bancare", 2004
[6] Electronic Banking Group of the Basel Comitee on Banking Supervision,
[7] Electronic Banking Group White Paper, Cross-Border Electronic
[8] Theodor Carp, Securitatea sistemelor informatice, www.enisght.ro
[9] *** Basel Consulting Group – Addor Jean Pierre, 2007
[10] *** Revista Informatica Economică, nr.4(32)/2004
[11] *** Risk Management Principles for Electronic Banking" – mai 2008
[12] *** www.internetworldstats.com
[13] *** www.forrester.com;
[14] *** www.efinance.ro
[15] *** www.datamonitor.com;
[16] *** www.mcti.ro