

MANAGING RISKS OF ELECTRONIC BANKING

Tijana Radojevic

Singidunum University, Belgrade, Serbia

Dalibor Radovanovic

Singidunum University, Belgrade, Serbia

Abstract

The development of e-banking services and e-commerce (including electronic money) can provide significant opportunities for banks. Application of information technology in banking brings, with one hand, strong organizational and economic growth potential, and on the other hand, opens space for the emergence of new forms of risk. So, rapid development potential of e-banking carries risks and benefits. Therefore, the provision of adequate security, appear as a separate critical factor in the functioning of electronic banking. The essence of security problems of modern electronic banking system reduced the risks of data security breaches and identity of entities, whereby the relative importance of these elements changes with technological development. Problems that are relevant for this group of critical factors required to determine the scope and nature of new risks, opportunities and price protection, and to determine the key division of the additional costs that it brings.

Keywords: banking risks, risk management, electronic banking, principles of risk management, security problems

INTRODUCTION

Information technologies are contributed to the development of electronic banking services. They open new opportunities for banks in the deposit and credit transactions, the possibility of offering new products and services, improve the competitive position, reduce costs, etc.. Of course, when the bank is providing e-banking services, they are faced with certain specific risks - operational, reputation, legal and risk of international operations. Modern banking is daily exposed to the existing and new risks. Bank management must identify risks, assess, control and finance. Risk management is the process of project management which is done continuously, through monitoring and evaluation.

1. Banking risk

Risks as the possibility of absolute or relative loss in relation to expectations in the banking business were characteristic of each of the banking business, and the winning of new instruments, techniques and strategies, financial engineering, new banking products, especially financial derivatives, exchange risk is continually expanding. Uncertainty grows with changes in interest rates, changes in deposits with the

debtor's inability to repay a loan, but under the influence of such factors as deregulation, moral hazard, and the entry of banks in jobs that previously were not traditional banking.

The globalization of banking and trends of merger and acquisition of large banks, urge bank management to identify important risks. This applies primarily to systemic risks, and in particular the risks arising from lags in monitoring the management of the banking business in unfamiliar, geographically distant markets. Banks, according to Basel II, have the right to develop its internal methodology for measuring risk. The general aim of each bank is optimization of the relationship of risk and return. Based on him bank can choose the most profitable products and branch banking, as well as the best way of pricing products. Finally, banks will have to invest significant financial and human resources in order to set a qualitatively higher level of risk management.

2. Risks in electronic banking

During the provision of electronic banking services and the use of electronic money banks are faced with a certain set of specific risks, such as:



Fig. 1. Risk in electronic banking

2.1. Operational risk

Operational risk arises from potential loss due to deficiencies in the system reliability and integrity. Consideration of safety is most importance, due to the possibility of internal and external attacks on the bank or its systems and products. Operational risk may arise due to the abuse by clients or improper designed or implemented electronic banking or electronic money system. According to noted, there are possible forms of operational risk:

- ✓ security risks (reliability and integrity of the system)
- ✓ the risks of designing, implementing and maintaining the system
- ✓ the risks of misuse of products or services by customers

Security risks appear in relation to control of information with which the bank interacts with the environment, electronic money transfers, as well as prevention of fraud or forgery. Example of a possible security risk is unauthorized access to the system. This means that confidential information may be overjoyed by unauthorized persons, for example, by hackers who enter the internal systems. Banks can apply certain measures to manage risk. It is possible to implement communication security measures, such as "fire wall", passwords, encryption technology and authentication of users. It is necessary to perform testing on the "vulnerability" of the system, and constantly checking the system for viruses.

Risks of design, implementation and maintenance of the system have an important impact on the development of electronic banking and electronic money. Risks that may be manifested in this part are the stop or slow down the system, which can have negative consequences to clients of the bank. It is not uncommon for banks to take foreign providers and

experts for the implementation, operation and support which provide smooth conducting electronic banking and electronic money activities.

One of the possible risks of designing, implementing and maintaining the system, can be employees and management who accept innovation more difficult. Extremely rapid changes technology can bring to that, so management and employees of the bank were not fully able to understand the nature of new technologies used in banks. The result is weak implementation of new technologies and the inability to provide continuous support to the development. It is necessary to conduct training, as a permanent process, and for the management and employees.

Misuse of products and services by customers, whether intentional or unintentional, is another source of operational risk. The risk increases due to inadequate education of customers, by banks, on security measures during the verification of electronic money transfers. Personal information of bank customers who participate in electronic banking (credit card number, bank account number, etc.) must be specially protected during the electronic money transactions.

2.2. Reputation risk

Reputation risk is the risk of negative public opinion, which results in significant loss or outflow of funds from bank customers. Its negative effect on the image bank, can be permanent. It may arise as a result of taking actions that have resulted in loss of public confidence in the ability of banks to carry out their business. Significantly, disruption of image banks may arise due to poor communication networks, where customers are not able to find out information about the state of their accounts, and so on.

The bank could be protected from reputation risk, it is necessary to provide electronic banking services consistently and constantly, all in accordance with the high expectations of their clients. It is important to establish mechanisms for emergency situations to minimize the reputation risk that may result from unexpected events, including internal and external penetration of the system that may affect the provision of electronic banking.

2.3. Legal risk

Legal risk is caused by the violation or conflict with the laws, rules, regulations or practices

prescribed or in case of legal rights and obligations of participants in the transaction are not legally regulated. Especially must be regulated to prevent money laundering, because the possibility of modern business to a large extent can be very attractive for this kind of abuse. This leads to the conclusion that banks that apply electronic banking and electronic money business, must pay particular attention to identification and authentication client and privacy (as the authentication method banks can use digital certificates).

To minimize the bank's legal risk, which is associated with electronic banking transactions that are done at home and abroad, it is necessary to ensure provision of adequate information on their web pages. This would enable the clients to verify the identity of the regulatory status of the bank before you engage in electronic banking transactions. For example, information that can be put on the web site may be the name and location of bank headquarters and local branches, the way the client can contact the bank in terms of complaints, suspected misuse of accounts, etc., The manner in which clients can appeal to authority that deals with consumer protection, and others.

2.4. Risks of international operations

Electronic banking and electronic money activities are based on technology that knows no geographical barriers. Banks that decide to provide services to clients in various national markets should explore the various national legal requirements, and to understand national differences in expectation and knowledge of products and services by customers. On the other hand, it is necessary to assess the country risk and develop plans for unforeseen liabilities that will predict activity in the case of economic or political issues on the national market. Under the economic problems are include changes in economic trends, economic development, business conditions in a particular country and its external liquidity, while the political issues involve changes in the composition of the government or government policy, political unrest or wars. Of course, that these economic and political changes considered if problems are to the detriment of operations.

2.5. Other risks

Other banking risks include credit risk, liquidity risk, interest rate risk and market risk,

which may arise from electronic banking and electronic money business.

Credit risk is the risk related to the borrower who will not fulfill its obligation of full value, or in estimated time. Banks have the ability to electronically receive applications for credit and to approve, which requires adequate procedures for determining the creditworthiness of customers, because otherwise increases the risk for the bank.

Liquidity risk is the risk that arises in the case that the bank is unable to perform outstanding liabilities that arise in electronic banking. Liquidity risk is the possibility of negative effects on the financial result and capital of banks due to the inability of banks to meet their outstanding obligations. Bank of its assets and liabilities managed in a way that allows her to always meet its outstanding liabilities (liquidity) and to permanently fulfill all its obligations (solvency). In order to effective management of liquidity risk, the bank adopts and implements a policy of liquidity management, which includes the planning of cash inflows and outflows of funds, monitoring the liquidity and the adoption of appropriate measures for the prevention or elimination of the causes of insolvency.

Interest rate risk relates to the reduction of interest rates to the extent where negative trends in interest rates reduces the value of property depending on the unfulfilled obligation. Interest rate risk consists of risks to interest rates on bank loans and obligations, of course, if these changes are unfavorable for the bank. The risk of interest rates can occur in cases when banks approve loans on certain fixed interest rates on long time periods, which are not accompanied by adequate resources structure of banks. This means that the bank advanced the funds for specific interest rates on longer terms than it has provided deposits. In the event of certain market disruption resources can rise in price, which would lead to situations that banks have certain losses on investments - loans that are granted in the long terms and conditions that are currently on the market unsustainable.

Market risk can arise due to changes in prices in the market, including the exchange rate changes, which certainly characterized by fluctuations, so that banks perform payment in

the form of electronic money in foreign currency risk.

3. Risk management

Electronic banking and electronic money business has become a widely applied by banks, as well as by users of banking services and traders. This has contributed to this modern form of business following a number of risks. Banks aim to achieve control and risk management. The process of risk management involves the following stages: risk assessment, management and risk control and monitoring of risk. These processes must be under the supervision of top management of banks.

3.1. Risk assessment

Risk assessment is necessary to organize as a permanent process which takes place in three phases. In the first phase it is necessary that the bank identifies and quantifies the opportunities and risks. Identification of risk is a key starting assumption of the risk assessment, given that they are the most dangerous risks which banks are not aware, because they can lead to large and unplanned expenses. Identification of risk is possible in several ways, the most common methods are related to empirical experience of banks, as well as the exchange of experiences between the commercial banks. If it is not possible to quantify the risk, it is necessary to determine the potential risk occurs and what are the possibilities to limit these risks. In addition, it is important to determine the frequency of risk occurrence.

The second phase determines the potential for banks in the level of risk tolerance, based on the assessment of loss that the bank will be able to submit. The key for all banks is that they become aware of the risks with which they operate, the way of its manifestation and frequency of occurrence, determine the manifestation of a risk assessment. This assessment is extremely important considering the fact that based on the assessed value - ie the loss due to the manifestation of certain risk, the bank should define preventive and corrective measures. Priority should definitely be the definition of preventive measures and elimination of the preliminary factors that can lead to the emergence of a risk.

The bank should be established for each of the risks that are to define, the indicators, ie indicators whose appearance could indicate the

occurrence of certain negative phenomena, ie. risk and based on these indicators define a list of actions to remedy them. Correction factors have only the effect of mitigating consequences caused by the activity of certain risks and negative cases of operations. In the third stage it is necessary to assess whether the risk exposure within the range limit. The third phase is the phase in which should be defined by monitoring the risks and if it happens. This is particularly relevant to the implementation of corrective measures that would risk or its impact should be to minimize.

3.2. Manage and control risk

After the evaluation of risks and determine their levels of tolerance, the bank's management should start with risk management and their control. Risk management activities include: implementation of security mechanisms and measures, coordination of internal communication, evaluation and improvement of products and services, implementation of measures to control risks related to external service providers and planning unforeseen circumstances.

Security mechanisms and measures which are applied in management and risk control, involve a combination of protective measures, applications and internal controls used to ensure integrity, authenticity and reliability of data, operational processes and reports. Protection is based on the development and implementation of adequate security mechanisms and measures for internal processes. In addition, develop and implement mechanisms and measures for communication between banks and external systems, in order to reduce the risk of external and internal attacks on the system of electronic banking and electronic money. Security measures are a combination of hardware and software tools. As security measures are used: data encryption, digital certificate, the installation of firewalls, antivirus controls, using a PIN, and the like.

The management is essential to establish communication with employees in the bank in charge of the operation of electronic banking (Coordination of internal communication). Also, the necessary communication with the management of IT sector in view of the functioning of the system designed and information about the eventual weaknesses, and measures for their elimination. For the implementation and operation of electronic banking requires a high level of

education of employees and users of bank services, resulting in reduction of direct operating and reputation risk.

3.3. Monitoring risk

Monitoring risk is an important aspect of any risk management process. The Bank may in several ways to manage risk, and one of the basic "tools" is ALM (Asset and Liability Management) concept or management of assets and liabilities of commercial banks. ALM process means that is within the bank to identify and analyze all the risks, define appropriate risk limits (which are in accordance with the strategy of allocation of capital), as well as to monitor the controlled risk limits over the modern information systems. Applying the concept of ALM requires the "top" management to continually modify and improve systems of risk management.

Example of monitoring risk in banking business, with a focus on electronic product distribution channels, would be the reaction of the banks in case of "fall" of the server that allows a smooth implementation of electronic orders. What happens in this case and how the banks respond, the issue that should occupy not only the internal review but also other parts of the commercial banks. It is necessary that the bank has established measures to be implemented in case of such "fall" of the system. In this case, the construction of a system of preventive measures, there is a faster elimination of the causes that led to errors. However, if it occurs, corrective action performance factors, for example, there is the possibility of including backup server, which allows the continuation of smooth communication with clients.

4. Principles of risk management for electronic banking - Basel Committee

For years banking institutions are provided electronic services to remote clients and the economy. Electronic transfer of funds, including small payments and money management systems for the economy, as well as publicly accessible automated machines for cash management accounts of citizens, is a global supplies. However, the increased acceptance of Internet in the world, as well as delivery channels for banking products and services, provides new business opportunities for banks and service benefits for their clients.

Independent of significant benefits of technological innovation, rapid development of e-banking bears the risks and benefits and it is

important that the banking organization identify and manage these risks on prudential way. The reason stated the Basel Committee on Banking Control conduct preliminary research implications for risk management in e-banking and e-money. These early studies showed a clear need for more work in the field of risk management of e-banking and the mission was entrusted to a working group composed of Bank Supervision and Central Banks, Electronic Banking Group (EBG).

4.1. The challenges of risk management

EBG has noted that the basic features of e-banking (and e-commerce in general) carry a number of challenges for risk management:

- ✓ rate of change in relation to technological innovation in customer service in e-banking is unprecedented. Historically, new banking applications were applied in relatively long periods and only after the fundamental checks. Today, however, banks suffer from competitive pressures to prepare new business applications in a very short time frames - often only a few months from concept to production. This competition is intensifying challenges for management to ensure that adequate strategic assessment, risk analysis and security research carried out before implementation of new applications of e-banking.

- ✓ Transnational e-banking websites and associated applications in work with citizens and the economy are usually integrated as possible into existing computer systems to achieve immediate processing of electronic transactions. Such direct automated processes reduce the scope for human error and fraud that occur with manual processes, but also increase the dependence on a healthy design and architecture of the system.

- ✓ E-banking increases banks' dependence on the information technology, increasing technical complexity of many operational and safety issues and the continuing trend towards greater number of partnership arrangements, outsourcing and alliances with third parties, of which many are subjected to regulation. This development leads to creating new business models involving banks and non-banking entities, such as Internet service providers, telecommunications companies and other technology companies.

- ✓ The Internet is global network. It is also open network which can be accessed anywhere

in the world of the unknown, routing messages through unknown locations and via wireless devices that are developing fast. So, the Internet greatly increases the importance of control of security, data protection, procedures and standards of diary keeping privacy of clients.

4.2. Principles of risk management

Basel Committee for Banking Control ordered the Electronic Banking Group (EBG), to identify the key principles of risk management that would assist banking institutions to expand their existing policy oversight of risks and processes, to cover the activities of e-banking and also to promote safe and healthy electronic supply of bank products and services.

They identified fourteen principles for risk management for electronic banking, which is divided into three broad and frequently overlapping categories of questions, which are to clarity grouped as follows:



Fig. 2. Principles of risk management

Principles of risk management for electronic banking, which have been identified, did not give the absolute demands or even as "best practice", but as a guideline for improving safe and healthy activities of e-banking. The client believes that the appointment of detailed requirements for Risk Management in e-banking can be counterproductive, even because they rapidly become outdated due to speed changes in technological innovations and product innovations. Hence, these principles reflect expectations controller regarding the general aim of banking control to ensure the safety and health of the financial system and not stricter regulation.

The client believes that the expectations of controllers can be cut and adapted according to distribution channel of e-banking, but not to be substantially different from expectations to banking activities, which go to other distribution channels. Hence, the principles that are still exposed are mostly derived and adapted

from principles of control which previously expressed a client or national control during the past year. In some areas, as well as managing relationships outsourcing, control, security and management of legal and reputation risk characteristics and implications of the distribution channels of the Internet creates the need for detailed principles than those that have so far existed.

Customer acknowledges that the Bank need to develop process of risk management that meet their individual risk profile, operational structure and culture corporational governance and are in accordance with the specific requirements of risk management and policy that set the banking control in their particular jurisdiction.

The client does not attempt to dictate the concrete technological solutions for treatment of certain risks or to set technical standards related to e-banking. Technical issues will have to constantly deal with bank institutions and different body standards as the technology developed. This solution will probably refer to the issues related to fact that banks are diferent in size, complexity and culture of risk management and the jurisdiction is diferent in their legal and regulatory frameworks.

For these reasons, a client does not believe access to "one size fits all" responsible management of risks in e-banking and therefore supports the exchange of good practices and standards for addressing additional dimensions of risk that make the channels of delivery e-banking. It is expected that the principle of risk management national controllers using as a tool and to apply, with adaptations that will reflect specific national requirements where necessary, to help promote a safe and secure activities and operations of e-banking.

Customer acknowledges that it is risk profile of each Bank different and require access mitigation of risk corresponding to size of the operations of e-banking, real risks that are present and the willingness and ability of institutions to manage these risks. These differences imply that the principles risk management, aim to be flexible enough to be applied to all relevant institutions in various jurisdictions. National control to estimate the reality risks related to the activities of e-banking present in a given bank and whether to what extent are

the principles of risk management for the e-banking adequately met through the bank's framework for risk management.

CONCLUSION

Risks in banking are an integral part of the job. New communication channel that we call the general name of electronic banking, has provided significant benefits to the bank and its clients. The fact is that electronic banking made to the bank, ways to step out of his office space and allow users to independently carry out their tasks related to the bank. This step brought the one hand significant savings banks and expand user base, but, on the other hand, forced banks to part of their jobs dislocated in other specialized firms.

To protect the bank from the business, legal and reputation risk, e-banking need to provide consistent and timely manner in accordance with high customer expectations in terms of constant and rapid availability, but also with potentially high demand for transactions. Banks must be able to provide e-banking services to all end users and to be able to maintain such availability in all circumstances. Effective mechanisms for responding to incidents are also crucial for reducing the operational, legal and reputation risks that arise as a result of unexpected events, including internal and external attacks that may threaten the provision of e-banking systems and services. To meet the expectations of customers, banks must have effective capacity, business continuity and plans for

every eventuality. Banks should develop appropriate plans for responding to incidents, including communication strategies, which ensure business continuity, control of reputation risk and limiting the obligations under the disturbances in their e-banking.

REFERENCE

- [1] Bjelica, V. 2001. *Banking*, Stylos, Novi Sad, Serbia
- [2] The Bank for International Settlements (BIS), *Risk Management for Electronic Banking and Electronic Money Activities*, Basel Committee on Banking Supervision, march 1998, [online] [accessed 28 Sep 2010]. Available from Internet: <http://www.bis.org/publ/bcbasc215.pdf>
- [3] Kondabagil, J. 2007. *Risk management in electronic banking: concepts and Best Practices*, Wiley
- [4] Rose, P.; Hudgine, S. 2005. *Bank Management and Financial Services*, translation, Data status, Belgrade, Serbia
- [5] Vunjak, N. 2005. *Financial management*, Proleter, Becej, Serbia
- [6] Vukovic, D. 2007. *Principles of risk management for electronic banking*, translation, Yugoslav Survey, Belgrade, Serbia
- [7] Vaskovic, V. 2007. *Payment systems in electronic business*, Faculty of organization science, Belgrade, Serbia
- [8] Vidas-Bubanja, M. 2005. *E-business: management, technology, applications*, Belgrade Business School, Belgrade, Serbia
- [9] Vuksanovic, E. 2006. *Electronic Banking*, Faculty of Banking, Insurance and Finance, Belgrade, Serbia