Jelena Miljković[1)]

1) Faculty of Economics, Finance and Administration, Belgrade, info@fefa.edu.rs

RISK MANAGEMENT IN E-BANKING: RISK MANAGEMENT PRINCIPLES

Abstract: *The high speed of technological progress, in addition to the great advantage that electronic banking brings, also carries many risks. This prompted the Basel Committee on Banking Supervision to issue a set of Risk Management Principles for Electronic Banking. Risk Management Principles for Electronic Banking can be divided into three categories: monitoring by board and management, safety control and management of legal and reputational risk.*

Keywords: *electronic banking, risk, risk management principles*

1. INTRODUCTION

Modern payment transaction is based on the application of advanced information technology and electronic money transfers. The effects are significant savings in labor and payroll records and payments in a relatively short time.

In the retail area (self-service) of banking three electronic payment systems are developed to perform operations. These are ATM's, point of sale (POS) terminals and home banking. [1]

ATM's are placed in busy places, buildings, banks, shops, etc, and are mostly used on weekends and after working hours. At any time customers can withdraw cash, check account balances, place money into the accounts and transfer money from one account to another.

The POS terminal connects consumer, bank and retail shop. It allows customers to purchase goods and services by using credit or debit cards. On the other hand it allows the retail shop (seller) to give the electronic order of payment via the bank computer center from customers to the sellers account.

Home Banking allows the customer to transfers money, make payments and obtain various financial information such as exchange rates, interest rates, prices of bonds and stocks, all from the comfort of his home.

In developed market economies, small payments are made through automated clearings performed by offsetting assets and liabilities of individual participants in the clearing arrangements. Therefore only the net amount is transferred from one account to the other.

2. DEVELOPMENT OF ELECTRONIC BANKING

The beginnings of electronic banking can be retraced in the 80's in the UK. The first electronic information system called Homelink was made by the Bank of Nottingham Building Society. This online information system enabled the clients to conduct financial transactions like electronic transfer of money, buying securities, etc. [2]

May 1995, Wells Fargo bank developed the first Web banking program for conducting business on the Internet. In the same year the first specialized Internet bank in the world, Security First Network Bank, was founded. In April 1996 the one millionth user was registered for the Internet banking services in the United States and in the following 18 months the number of users increased to record 4.2%

of U.S. households.

Internet development and growth of internet banking services is closely related to the development of information technology. Faster, safer, easier and simpler business on the Internet are the goals set by more demanding financial market for the banks and other financial institutions. To meet these goals, the volume of investments in information technology is constantly increasing.

Banks, for many years, are providing electronic services to clients and the economy. Electronic transfer of funds, cash management systems for corporate and ATMs are the standard offer for the clients. However, the increasing acceptance of the Internet banking in the world, as a delivery channel for products and services, provides new opportunities for bankers and improves services to their clients.

3. FORMS OF ELECTRONIC BANKING

Forms of electronic banking involve the following:

POS terminals: POS system (Point of sale) relates to the development of computer networks and faster realization of financial services using electronic banking. POS system allows more efficient and safer method of non-cash payment between the bank and the customer.

EFT POS system checks the validity of credit card, debits the costumer account, reduces the circulation of cash, stabilizes bank deposit potential and increases circulation of non-cash payments (commissions and fees). Client through this system is provided with faster non-cash charges, cost reduction payments, full control of the financial costs and the likes.

Telephone banking represents direct use of banking services from home as it allow direct transfer of funds and account information via the telephone. In the literature, this type of distribution network is called home banking system. Using this system the client is deprived of the purpose of going to the bank teller and the need for written communication.

SMS Banking, Mobile Banking and Web TV banking SMS banking relies on the use of mobile phones in the function of performing banking transactions. In order to use SMS banking customer needs to fill out the form with his current account and mobile phone details from which the transaction will be executed. After obtaining access, the customer automatically receives a welcome message on his cell phone informing him that he has become an active user of this service.

Mobile banking allows account transactions via laptops, iPads, mobile phones supported with special software for mobile banking.

Web TV banking refers to the television and Internet connected into a single unit. Usually this form of electronic banking is used by the customers who use TV as internet browser.

4. ELECTRONIC PAYMENTS

Electronic payment is done by exchanging electronic messages through the information systems of the participants in the payment transaction. Electronic message is considered to be information that is electronically generated, sent, verified, received and stored (electronic payment order or other financial document). Participants in the electronic payments are banks, customers and agents.

5. RISKS OF ELECTRONIC BANKING

Risk detection consists of activities that enable risk managers to identify, assess and measure risk and their potential impact on the organization. It is one of the most fundamental activities of risk managers, which includes identifying risk, hazard analysis and risk measurement and

outcomes. Although relatively separable in theory these activities are tightly intertwined in practice.

The risks of electronic payment systems can be grouped into several categories:

• Operational risks (security, theft by employees, forgery, system design, implementation, management, service provider risk, obsolete systems, denial of transactions by the user).

• The risks of losing the goodwill and reputation (negative public opinion, deficiency of the system, threat of hacking, errors in similar systems)

• Systemic risks (risks of losing information can cause distrust in the system and expansion of business)

• Legal risks (violations of the laws - ambiguity, legal sanctions, money laundering, inadequate disclosure, invasion of privacy, the violation of the linked sites, risks of a certificate of authority, foreign laws)

• The banking risks (credit, liquidity, interest rates, trade, social, political and economic risks)

• The risks of criminal assault (fraud, forgery, theft, illegal use and incitement to crime).

The high speed of technological progress, in addition to great benefits, also brings risks. In 1998 this prompted the Basel Committee on Banking Supervision to conduct preliminary research on risk management in electronic banking. Noticing great need for quality work in the field of risk management, the task was entrusted to Electronic Banking Group of the Basel Committee on Banking Supervision, which was established in 1999. Electronic Banking Group realized that even if you are not introducing new risks the properties of e-banking significantly increase the existing ones like strategic, operational, legal and reputational risk, and therefore the overall risk of the bank.

In 2003 the Board, in order to facilitate the development of e-banking, founded fourteen Risk Management Principles for Electronic Banking. [3] The Committee did not go into a detailed specification of the principles and requirements considering that due to the speed of technological progress they could be quickly outdated. The Board through these principles wanted to provide a guide on how to mitigate risks, taking into consideration the different characteristics of banks. Risk Management Principles for Electronic Banking may be divided into three categories: board and management supervision, safety control and management of legal and reputational risk. [4]

5.1. Board and management supervision

The Board of Directors and senior management levels are directly responsible for developing business strategies and setting up effective control of the risks. It is expected from the management to make explicit, well-reasoned and documented strategic decisions whether the bank should provide electronic banking services.

Principle 1 The Board of Directors and senior management should establish an effective control of risk management associated with e-banking transactions, including the allocation of specific responsibilities, policies and controls to manage those risks. Also, they should ensure that risk management integrates e-banking into the general risk of the bank. From the management it is expected to draw well-defined division of responsibilities, and reporting procedures in the event of unforeseen circumstances and requiring a third party (the bank with which externalize their systems and applications) to take similar protective measures.

Principle 2 The Board of Directors and senior management should constantly review and approve the key aspects of the security control of the bank. To ensure

this, the management must first review the existing security, and then define policies and procedures for prevention and behavior in case of possible internal and external security threats. Key elements of this process include: a clear definition of responsibilities in order to control and maintain security policies, sufficient physical control to prevent unauthorized access to computer-communication systems, logic control, and adequate monitoring mechanisms to prevent unauthorized access to applications and databases, e-banking, regular checks and testing of security measures and controls, as well as installing the right software to monitor online activities and unauthorized access attempts.

Principle 3 The Board of Directors and senior management should establish a comprehensive and thorough analysis of the continuous control of the business (due diligence) and the monitoring of bank management external relations and other types of reliance on third parties to support e-banking. A large number of partners and service providers, who act as third party e-banking, reduce the direct control and risk management of banks. Accordingly, it is necessary to build a comprehensive system for managing the risks associated with outsourcing and reliance on third parties, and particularly focus on: test of competence and financial strength of providers or partners before making a contract; contractually defined responsibilities of all parties; all externally guided systems and operations shall be in compliance with the policy of risk management, security and privacy within the bank's plans to make outsourcing work for contingency situations.

5.2. Safety control

The basis of successful risk management in e-banking lies in thorough control of security. Adequate control of security includes authentication, authorization, control logical and physical access, secure infrastructure and reliability of data on transactions, documentation and information. The term authentication means procedures and processes for authentication and authorization of clients. Identification techniques are procedures and processes in order to determine the client's identity when opening an account.

Authorization is the procedure for determining legitimacy of access to a particular account by customer or employee, or permission to conduct transactions in that account. Taking into account the fact that privacy regulations vary from state to state, the Board insists on providing a level of safety in terms of publicizing or sharing customer information with third parties.

Principle 4 Banks should take appropriate measures for authentication and authorization of clients with which it operates over the Internet. Determining the client's identity when opening an account reduces the risk of identity theft, fraudulent charges and money laundering. Legitimate user authentication can be forged by spoofing accounts, passwords, personal identification number (PIN) and / or email addresses. Second, using a sniffer ("sniffed") hardware and software can eavesdrop on the communications channel, and so reach the passwords and other sensitive data. For all these reasons, it is important that bank makes a formal policy and procedures to ensure proper authentication and authorization of individuals, agents or systems. Banks can use different authentication techniques, the use of PIN codes, passwords, smart cards to the most advanced biometric technologies. Also, for greater protection, multiple verification mechanisms (such as a fingerprint and password) can be used. Continuous improvement requires to follow best practice of e-banking, which suggests: building a database for authentication with the security simultaneously written audit trails of any attempt to modify the database, the

existence of "safe" system (or persons) to authorize any changes (additions, deletion) of the system or database authentication; applying appropriate control measures within a system for e-banking to avoid replacement of the known to unknown third party client, any interruption of safe and proven sessions in e-banking should require re-authentication.

Principle 5 Banks should use transaction authentication methods that include disclaiming, and determining liability for e-banking transactions. Possibility of disclaiming transaction provides evidence of the origin of electronic information that protects the sender from denying receipt of data by the recipient or the recipient protects the sender's false denial that the data has been sent. The implementation of this principle requires: secure authentication of all parties to the transaction and control of communication channels, e-banking system should be organized so as to prevent authorized users initiate unintended transactions, data on all financial transactions must be protected from any changes.

Principle 6 Banks should ensure the proper segregation of duties within e-banking systems, databases and applications. Separation of duties is based on internal processes to reduce the risk of fraud within the system of e-banking. Separation of duties is necessary to ensure the proper authorization, accounting and transaction protection. In a system with high-quality separation of duties deception is possible only in mutual collusion of individuals. Construction and maintenance of proper segregation of duties include: development of transaction systems and processes that prevent the same user to initiate, authorize and complete the transaction; the distribution of duties should be maintained between those who generate information and those who verify their integrity; e-banking system must be designed to prevent the possibility of bypassing the distribution of duties; separation must be maintained between those who are developing the system and those who manage the system.

Principle 7 Banks should ensure appropriate control of access rights and authorization for e-banking systems, databases and applications. Quality control of authorization prevents individuals to alter their powers, bypass the distribution of duties and so gain access to systems and databases. No individual or the system can have the authority to change the personal rights of authorization and access to the database. Any changes in the authorization database must be approved by the relevant resources whose adequate measures shall be subject to verification and whose activities are accompanied by a written audit trail. Particular attention should be paid to control the system administrators who typically have the greatest power in the system.

Principle 8 Banks should ensure that appropriate measures are taken to protect the credibility of data on e-banking transactions, records and information. The credibility of the data relates to the prevention of changes of information transmitted or stored without authorization. Banks should introduce appropriate measures to achieve the accuracy, completeness and reliability of e-banking transactions, documentation and information that are stored within the system, the third party or transferred over the Internet. The general practice that is used includes: a transaction should be implemented so that it is very difficult to change throughout the treatment; documents related to e-banking should be resistant to distortion; transactions and record-keeping should be organized so that it is very difficult to bypass the mechanism of detecting unauthorized access, there must be adequate control of all policy changes within the system of e-banking, which can lead to unreliable data.

Principle 9 Banks should ensure that

there are clear written audit trails for all transactions on e-banking. One of the major internal controls is the existence of clear written audit trails of electronic commerce. Audit Trails must follow the following types of e-banking transactions: opening, closing or changing the client's account, each transaction with financial consequences, any authorization which the client gets for exceeding authority; any assignment, modification or termination of access to the system. Good practice for written audit trails suggests that the systems for e-banking must be organized so that the evidence is valid for court record, to prevent distortion or gathering of false information. Also, in cases where the system includes a third party, the bank must provide access to audit trail with the provider and to insist that audit trails meet bank standards.

Principle 10 Banks should take appropriate measures to preserve the confidentiality of key information of e-banking. These measures should correspond to the level of sensitivity of the information transmitted and / or stored in databases. Successful implementation of this principle ensures that: all confidential banking information should be available only to those who have gone through the authorization and authentication, to keep confidential data safely and protected from unauthorized viewing and modification; ensure that the standards and control of the bank protection of data is carried out within a third party as well, that any access to sensitive data is recorded and resistant to distortion.

5.3. Managing legal and reputational risk

In order to protect the bank from the legal and reputational risks, e-banking services must be provide timely, continuous and fast in terms of increased demand for transactions. To fulfill this, the bank would have to effectively use all the capacities and construct contingency plans to ensure business continuity.

Principle 11 Banks should provide adequate information on its web site that will allow potential customers to make unambiguous conclusions about the identity of banks and bank regulatory status before engaging in e-banking transactions. In order to minimize legal and reputational risks, especially when the bank performs abroad, the bank's web page must contain the following set of information: the name of the bank and its location, the identity of the main monitoring body for the head office, the manner in which customers can contact the bank in case of problems with services, the way customers can get to the body for consumer protection and other information that may be of use or application state in which the bank provides.

Principle 12 Banks should take appropriate measures to ensure compliance with requirements respecting customer privacy that apply in countries where the bank provides products and services of e-banking. The bank must ensure that: its policies and standards regarding the policy comply with regulations and laws of the State in which the bank provides services, clients are informed about these standards and policies; clients has the opportunity to refuse banks permission to share his personal or financial information shared with third party; clients data may not be used for purposes not approved by the client.

Principle 13 Banks should have adequate capacity, business continuity and contingency planning for the circumstances to ensure the availability of systems and services of e-banking. Success in implementing this principle depends on the quality of the reserve system for unforeseen circumstances, which must ensure the smooth continuity of service provision. Banks would have to provide: continuous analysis of current capacity of e-banking and evaluate future system overload, capacity assessment as well as

transaction processing and testing the stress of the situation, to develop appropriate emergency plans and that all systems involved in emergency situations are constantly tested.

Principle 14 Banks should develop appropriate plans for incident cases, in order to manage, solve or minimize problems arising from unexpected events including internal and external intrusions into a system which can prevent the provision of e-banking. To ensure the efficient operation in case of emergency, bank must prepare: plans for incident cases, mechanisms for determining the incident, assess its importance and control reputational risk associated with it; communication strategy related to issues with external markets or media that can be occur in a security compromise, infiltration into the system or the failure of e-banking, a clear process of alerting regulatory bodies; teams for incidents; a clear chain of command (which includes internal and external affairs); processes that ensure that third parties, clients and the media are timely informed about the disorder in the e-banking system; processes for collecting and preserving evidence valid at the court and assist in the prosecution of the perpetrator.

6. PAYMENT SYSTEM OVERSIGHT

Oversight of payment systems is a function of central banks in which the goal is promoting safety and efficiency through monitoring existing and planned systems, evaluation of these systems and, if necessary, initiating changes in them. Central banks are particularly interested in the safe and efficient functioning of payment systems for exercising their basic function - to provide confidence in the national currency and safeguard financial stability. Performing the supervisory function of the central bank is focused on a particular system, rather than at individual participants in the system.

The main objectives of monitoring are the safety and efficiency of payment systems and instruments that can initiate payment transactions.

Security means limiting the risks that can occur in the payment system and which may jeopardize or adversely affect the proper and continuous functioning of the systems and financial stability.

Efficiency means quickly and economically performed operations in the payment system, and the level of service that is cost-effective system for participants and their customers, and that suits their needs.

Oversight of payment systems in the Republic of Serbia includes the following activities:

• monitoring and analysis of statistical data, information, reports and other documents relating to the functioning of payment systems and the use of payment instruments at the disposal of National Bank of Serbia;

• assess compliance of payment systems to international standards and principles for the functioning of the systems established by the decision to prescribe the manner of its oversight (hereinafter referred to as conformity assessment of payment systems);

Monitoring is a continuous activity which performance results in creation of various reports that contribute to the understanding of the functioning of payment systems and their linkages and impact on financial stability.

Assessment of compliance of payment systems is a periodic activity that is done with consideration to compatibility of these systems with international standards and principles. The mentioned activity is not directed at individual participants in the system, but the payment system as a whole and is done in accordance with the methodology for assessing compliance of payment systems.

National Bank of Serbia defines

guidelines for the application of principles for the functioning of payment systems in order to transparently show the standards that they are using for the assessment of payment systems, as one of the activities under supervision.

Based on the results of monitoring and conformity assessment of such systems, the National Bank of Serbia may propose and initiate changes in payment systems through:

• making recommendations to the payment system operator on the implementation of necessary changes that are important for its safe and efficient operation;

•mutual cooperation between organizational units of the National Bank of Serbia;

• amending the legislation governing the payment of the country, and by adopting various guidelines and recommendations that will ensure the fulfillment of the main objectives of monitoring;

• for transparency, the National Bank of Serbia presents the results in the annual report on the country's financial situation, as well as through various reports published on its website.

National Bank of Serbia applies internationally recognized standards in monitoring payments system.

7. CONCLUSION

Characteristics of e-banking are: constant technological advancements, improvement of customer services, global usage, integration of e-banking applications with existing computer systems, increased dependence of banking transactions from information-communication technology. E-banking in addition to the many benefits carries with it certain disadvantages. If risks are identified and analyzed on time, it is possible to redistribute them, and therefore they can be managed well. Basel Committee on Banking Supervision guidance is essential for providing good risk management practice in electronic banking.

REFERENCES:

[1] Lukić R, "Banking and Accounting," CID Faculty of Economics in Belgrade, Belgrade, 2009.
[2] Živković A, Stankić R, Krstić B, "Banking and Payment System", Faculty of Economics in Belgrade, Belgrade, 2009.
[3] Radović O, Risk management of electronic banking. Economics. 2004, 42 (1-2) :505-511th
[4] Risk Management Principles for Electronic Banking, Basel Committee on Banking Supervision, July 2003.