CHALLENGES OF MODERN ELECTRONIC BANKING

Zoran Jović[1],
Goran Ćorić[2],
Igor Pejović[3]

[2]Singidunum University
32 Danijelova Street, Belgrade, Serbia
[2]Raiffeisenbank
Belgrade, Serbia
[3]College of Economics and Administration,
Imotska 1, Belgrade, Serbia

Abstract:
Electronic banking as a set of different ways of performing financial transactions using information and telecommunication technology provides the benefits of temporal and spatial limitlessness, speed of transactions, low prices and a wide range of banking products and services. On the other hand, apart from obvious advantages, e-banking incorporates certain risks that need to be precisely identified and managed. This is the reason why the Basel Committee on Banking Supervision established a task group called EBG (Electronic Banking Group) that consists of banking supervisors and central banks. The group has come to a conclusion that electronic banking impacts some of the traditional risks, modifying and augmenting them, this primarily referring to strategic, operational and reputational risks. Specific challenges of e-banking services relate to rapid changes, increased dependence on the design and system, the trend toward unregulated outsourcing and heightened importance of security controls. The principles of risk management in traditional banking are applicable to e-banking activities, but the complexities of the Internet dictate that the application of these principles be adjusted to on-line banking activities and related challenges. Because of rapid changes in technology, risk management principles of electronic banking are not given as mandatory requirements or strict regulations but as guidelines that express supervisory expectations, the aim being to ensure safety and stability of the financial system. Any rigidity in the regulation of e-banking may be counterproductive because such solutions would quickly become outdated due to a fast pace of technological change.

Key words:
e-banking, Internet, technology innovation, risk.

1. INTRODUCTION

One of the most important technological developments that has influenced the development of banking is electronic money, hence electronic banking. In today's world, money has become a piece of information which defines the right of an entity in relation to goods and services that are offered in society. Hence, the importance of an analysis of electronic banking channels, the mode of their operation, implementation and impact on the development of marketing and trade. The development of information technology has created conditions for the development of electronic banking which, by means of its wide distribution network, allows banks to offer their clients market-segmented banking processes and integrated packages of financial services targeted at certain segments of financial markets. Although banks initially had an aversion towards novelties brought about by the Internet, they have come to realise that

Correspondence:
Zoran Jović

e-mail:
zjovic@singidunum.ac.rs

DOI: 10.15308/Sinteza-2016-442-447

this is not a passing phenomenon, but rather a part of a very promising business reality. In accordance with the bankers' inherent way of thinking, while developing new Internet-based products and services known as e-banking products, banks have also been developing adequate systems of protection and security of their business operations within this segment. By conducting electronic banking operations on a daily basis, banks are exposed to the risk of unauthorised entry into the banking information system, thus allowing third parties to illegally access financial assets or confidential data at the expense of the bank and its clients. By employing adopted methods and principles of risk management, banks eliminate or reduce to an acceptable level the risks that bank clients are exposed to, such as deliberate identity theft or accidental omissions by bank employees.

2. CONTEMPORARY ELECTRONIC PAYMENT SYSTEMS

Electronic money is generated when a certain amount of real money is withdrawn from circulation and electronic money in the same amount is introduced. In this way electronic money systems become separate entities interacting with the environment through an intermediary that performs conversion and payment to this environment.

The general model of an electronic money system includes three distinct domains:

1. Accounting-clearing domain,
2. Emission-operational domain,
3. Retail domain.

In the accounting-clearing domain, financial institutions, clearing banks and central banks perform interbank financial obligations. In the emission-operational domain, a structure for emission and acquisition of electronic value is established. In the retail domain, actual transfers of values between users, such as transfer, payment and deposit, are performed.

The electronic money system consists of several important elements that define its nature - security, anonymity, portability, two-way operation, possibility of off-line operations, and unlimited duration.

An expansion in the use of electronic money is closely linked with the development of electronic banking channels. The main channels of electronic banking are payment cards, ATM machines, POS terminals, mobile commerce, electronic data exchange system and micropayment systems.

Payment cards are one of the most massively used means of electronic banking. In addition to being used as a means of payment for goods and services, cash withdrawals and electronic payments, they offer the convenience of currency conversion. In this way a client can make a payment in any country regardless of the currency of payment, and their account is charged with the transaction in domestic currency. Rapid development of payment cards and the ensuing substantial financial potential led to the creation of large international credit card franchise chains such as Visa, MasterCard, Diners Card, American Express.

ATMs are computerised telecommunication devices that allow clients to perform financial transactions in a public place without the presence of a bank official. They are classified as cash dispenser devices, info ATMs, ATMs for currency exchange operations, cash machines for payment of bills, cash machines for sale of value, and multifunctional ATMs. In terms of location, they can be installed at the bank entrance - the lobby, bank counter halls - indoors, or at entrances to public institutions and at busy public spaces - outdoors. ATMs can be linked to the bank's system in several ways: using a dial - up modem on the telephone line, using a VSAT line - satellite connection or via a leased line - GPRS.

The development of electronic payments and a growing number of clients who wish to make a payment using plastic cards force merchants to install POS terminals. It would be ideal if merchants could accept all cards but numerous complicated administrative procedures created by card organisations through authorised banks, sometimes multiply the number of different POS terminals at a merchant's. All POS terminals in the possession of a merchant are connected to the bank's network or processor and form the so-called banking trade network. Transactions that are carried out on these terminals go to the central system from where they are dispatched to the host bank or processor.

Mobile commerce understands any money transaction which is done via a network of mobile communications. Mobile technology allows purchase and payment of various goods and services, banking transactions, access to paid content and information from any place and at any time. Mobile services have experienced rapid development prompted by the mass character of mobile telephony market, the rapid development of the Internet and e-commerce, development of equipment and devices for mobile phones, the possibilities of authentication and authorization, and new principles of billing services. Mobile operations are carried out on the basis

of close cooperation between mobile operators, financial institutions and companies that issue debit cards. The advantages of using mobile phones when performing banking transactions that clients avail of are personal independence, easy to use, mobility and security. Problems in mobile business relate to profitability, legislation and various technical, health and social issues. Currently, mobile business has got no critical mass of users to become a standard in the market, but new mobile payment services are being further developed and improved.

The electronic data exchange system links business information systems and standardises electronic data exchange in order to overcome shortcomings of operations based on standard documentation. With the aim of reducing or eliminating errors in communication between business partners, EDI - electronic data interchange is used. It increases productivity and efficiency of operations and eliminates delays and mistakes that may occur in the process of exchanging paper documentation.

EDI is used for the exchange of documents such as purchase orders, invoices, receipts, forwarding supporting documents. All documents are in electronic and can be easily sent and received. This dispenses with delays that may occur as a result of forwarding paper documents, copying and multiplication. Since the process is automated, the cost of creating and sending documents is much lower.[1] The field of electronic data interchange (EDI) was standardised by a set of standards commonly known as EDIFACT - Electronic Data Interchange for Administrations, Commerce and Transport, which were introduced in order to facilitate and accelerate the flow of goods and services on the international level.

Micropayments are low-value electronic payments that are specially designed for e-commerce on the Internet, primarily for the purchase of goods and services worth a few dollars to a few cents or less (parking, transport, telephone, drinks, copying Internet content, lottery, gambling, *etc.*). A micropayment is a substitute for coins as it is inexpensive, e-mobile, easier to count, check and verify. A small number of operational micropayment systems have been created so far, the best-known ones being Millicent, Syber Coin and Net Bill.[2] Millicent provides anonymity when making payments. The customer purchases a card that is similar to a telephone card, exchanges the money with the broker and makes a payment, while the seller collects the amount and exchanges it for money. Syber Coin system is based on the accounting transfer of the corresponding amount. Money is transferred from the user's temporary account to the seller's temporary account, which have been opened in the SyberCash bank for that particular purpose. NetBill is a micropayment system which is designed to act as a third party whose responsibility is to verify authenticity, manage accounts, process transactions, bill and inform clients and users in the network.

Two concepts of digital money have been introduced so far: the centralized concept (PayPal, Stripe, WebMoney, Payoneer) where operators sell their electronic currency directly to the end user and is used mostly for online transactions; and the non-centralized concept (Bitcoin, Litecoin) which is based on the monetary system within the network.[3]

3. RISK MANAGEMENT IN E-BANKING

An increase in the number of clients using electronic banking services via the Internet, an expanded range of electronic goods and services that banks offer and an increase in the number of transactions renders banks vulnerable to risks in their daily operations and to an increase in the number of fraud cases and perpetrators - cyber-criminals.

Security in business operations via the Network must be the main business principle governing bank's operations and services[4]. Although nowadays there are many highly reliable systems and mechanisms for the protection against Internet banking fraud and robbery, none of them can fully protect the bank and its clients.

Operational, legal and reputational risks are the most important risk categories for the majority of operations in electronic banking involving electronic money. Many practical problems are regarded as borderline cases in the risk categories. Security breaches and unauthorised access to client information can be classified as operational risk but at the same time it can be regarded as legal and reputational risks. Since different types of risk can be generated from one problem, risk management may require different approaches to managing each of these risks separately.

1 Vasković V., Todorović M., E-poslovanje, Beogradska poslovna škola, Beograd, 2013, pp. 87.

2 Jović Z., Primena Interneta u savremenom bankarskom i berzanskom poslovanju, Međunarodna naučna konferencija Sinteza 2014, Zbornik radova, Beograd, 2014, pp. 183.

3 Jović Z., Primena Interneta u savremenom bankarskom i berzanskom poslovanju, Međunarodna naučna konferencija Sinteza 2014, Zbornik radova, Beograd, 2014, pp. 182.

4 Hadžić M., Bankarstvo, Univerzitet Singidunum, Beograd, 2011, pp. 52.

Operational risk is the risk of loss due to significant deficiencies in system reliability or integrity. Security considerations are paramount as banks may be subject to external or internal attacks. Operational risk can also arise from misuse on the part of a client, as well as from an inadequately designed or implemented electronic banking system. Many of these specific potential risks apply to both electronic banking and electronic money.[5]

Operational risk can be related to security risks; design, implementation and maintenance of the system; misuse of products and services by the buyer. Security risk in electronic banking relates to the detection and prevention of counterfeiting. A breach of security via the Internet may incur fake liabilities and losses on the part of the bank and specific problems pertaining to access and authentication may occur. A hacker breaks into a bank's system via the Internet, downloads and uses confidential client information and introduces viruses into the bank's computer system. Besides external attacks, banks are also exposed to internal operational risk which can be a case of deliberate fraud or misuse by employees or their unintentional mistakes. Both cases can compromise the bank's system. Operational risks include the risk of counterfeiting of electronic money.

Operational risks also arise when the bank chooses a system that is not well designed, implemented or maintained, and as such, causes cessation or slowing down of the existing system. Some banks opt for outsourcing and engage service providers and external experts to carry out certain tasks, which potentially renders the bank even more vulnerable to operational risks if the providers do not have the necessary expertise to provide the relevant service or update their technology in a timely manner. Intentional or unintentional misuse of products and services by clients is also a source of operational risk. Clients who use personal information such as authentication information, credit card numbers and bank account numbers in unsafe electronic transactions could allow criminals to access their computer, this possibly incurring financial losses on the part of the bank due to transactions that the client did not approve or for reasons of money laundering.

Reputational risk is the risk of loss due to negative publicity tarnishing the bank's reputation and causing revenue reductions or a decline in the customer base and may arise when systems or products are not as efficient as expected, when security breaches occur as a result of external or internal attacks on the bank's system, or due to errors, fraud and malfeasance by third parties or targeted attacks on the bank. Reputational risk is of significance not only to one particular bank but to the banking system as a whole. The bank which has suffered significant reputational harm in connection with electronic banking compromises the safety of the systems of other banks, this possibly causing systemic disruptions in the whole of the banking system.

Legal risk occurs due to violation or non-compliance with laws, rules, regulations, and when legal rights and obligations of the parties performing a transaction have not been clearly established. Due to a large number of innovations in e-banking, rights and obligations of the parties in these transactions can be uncertain. Application of regulations to prevent money laundering may not be appropriate for some forms of electronic payment, while too liberal a system may attract money launderers. E-banking carries the legal risk of disclosure of client's confidential data and the issue of privacy protection, which in some countries may make the bank subject to regulatory sanctions. Digital certificates affect the safety of banking operations and can expose the bank to legal risk as well.

Risk management consists of three basic elements: risk assessment, risk control and risk monitoring.

It is essential that banks have comprehensive risk management that is subject to appropriate supervision by a board of directors and senior management. As soon as new risks in electronic banking are identified and assessed, the board and senior management must be informed about the changes, so as to be able to perform appropriate appraisal and introduce measures of control, as well as monitoring any risks that may arise from the proposed activities.[6]

Challenges in e-banking risk management relate to the pace of technological change and changes in customer service. In the past new banking applications were implemented following a relatively long period of in-depth testing. Today, banks are pressured by fierce competition into launching new business applications in a very short period of time, usually only a few months from concept to realisation. This only intensifies the challenge that the bank faces and that is to do everything in their power to establish security procedures, carry out a strategic assessment, and perform risk and security analyses.

5 Risk Management for Electronic Banking and Electronic Money Activities, Basel Committee on Banking Supervision, Basel, March 1998, pp. 5.

6 Risk Management for Electronic Banking and Electronic Money Activities, Basel Committee on Banking Supervision, Basel, March 1998, pp. 10.

Challenges are also set by transactional e-banking web sites and associated retail and wholesale business applications that are substantially integrated. And, although the system of this kind reduces the chance of human error and fraud, it increases the dependence on the system design and architecture, as well as its operability.

Challenges of modern electronic banking also lie in increased dependence of banks on information technology which enhances technological complexity of numerous operational and safety issues and forces banks to form partnerships, alliances and engage in outsourcing although many of these fields are unregulated. The result is the creation of new business models that, besides banks, engage non-bank entities such as Internet services, telecommunication companies and other technology companies.

The Internet is ubiquitous and global by nature. It is an open, highly accessible network used by unknown parties routing messages by means of unknown locations and via fast evolving wireless devices. This considerably enhances the importance of security controls, customer authentication techniques, data protection, audit trail procedures, and customer privacy standards.[7]

In defining the principles of risk management, the Basel Committee deemed that it is the duty of the Board of Directors and senior management of banks to take steps to ensure that their institutions are reviewed, and that their existing risk management policies and procedures cover all current or planned activities of e-banking. The Basel Committee asked the EBG to identify key risk management principles which would help banks to expand risk monitoring so as to cover all their e-banking activities. This was the basis on which principles of risk management in electronic banking were created. They were not presented as absolute requirements or as 'best practice', but as guidelines for the promotion of safe electronic banking. The Basel Committee maintained that further detailing requirements for risk management in the field of e-banking could be counterproductive because these would probably soon become obsolete due to a fast pace of technological change. That is the reason why these principles do not represent strict regulations but only express supervisory expectations striving to ensure security and stability of the financial system.

The Committee recognizes that banks have to develop risk management procedures appropriate for their individual risk profile, operational structure and corporate culture governance and do so in conformity with specific risk management requirements and policies set forth by bank supervisors in their particular jurisdiction(s).[8]

This means that it is recognised that every bank's risk profile is different and that the presence of electronic banking, material risks, willingness and ability of the bank to manage these risks varies from case to case and that it is expected that the principles of risk management in e-banking are used as tools by national supervisors and that they should reflect specific national requirements where necessary in order to promote safe and secure e-banking activities and operations.

The principles of risk management in e-banking can be divided into three broad categories:

- Board and Management Oversight
- Security Control
- Legal and Reputational Risk Management

Board and Management Oversight shall make sure that e-banking plans are clearly integrated into strategic objectives; that a risk analysis of proposed e-banking activities is carried out; that appropriate processes are established to reduce the risk and monitor identified risks; and that electronic banking results are assessed. This category includes the following principles of risk management in e-banking:

- Effective management supervision of e-banking activities,
- Establishment of a comprehensive process of security control,
- Comprehensive analysis and monitoring of outsourcing relations.

Security Control should be given special attention because of security challenges posed by e-banking. In this category, the following principles are of particular importance:

- Authentication of e-banking customers,
- Non-repudiation and accountability for e-banking transactions,
- Data integrity of e-banking transactions, records and information,
- Appropriate measures to ensure segregation of duties,
- Proper authorisation controls within e-banking systems, databases and applications,
- Establishment of clear audit trails for e-banking transactions,
- Confidentiality of key bank information.

7 Risk Management Principles for Electronic Banking, Basel Committee on Banking Supervision, July 2003, pp.5-6.

8 Risk Management Principles for Electronic Banking, Basel Committee on Banking Supervision, July 2003, pp.6.

Management of legal and reputational risks pressurises banks into taking responsibility to provide their clients with a level of comfort regarding information disclosure and client data protection. This category includes the following principles of risk management in e-banking:

- Appropriate disclosure of electronic banking services,
- Privacy of customer information,
- Capacity, business continuity and contingency planning to ensure availability of e-banking systems and services,
- Incident response planning.

4. CONCLUSION

Embracing the Internet across the world as a channel through which banking products and services are delivered provides new business opportunities for banks and secures benefits for their clients. Continual technological innovations have made it possible for electronic banking to be incorporated in traditional banking activities such as accessing financial information, taking out loans and opening deposit accounts, as well as relatively new banking products and services such as electronic bill payment services, personalized „financial portals" and business-to-business market places and exchanges.

As banking operations evolve, so do the risks involved. There is no safe bank that is so infallible that cannot experience a downfall. Banks can only accept, avoid or protect themselves from potential risks.

Although considerable means are being invested to fight cyber-crime, an increase in the number of services provided by banks and other financial institutions causes a considerable rise in the number of users of electronic services who, owing to the poor level of their education, are easy prey for much better organised cyber criminals. At present, the existing systems and mechanisms provide a high level of protection against online banking fraud and robbery, but none of them can fully protect the bank and its clients. However, the safety of operations via the network must be the key principle every bank shall abide by and shape their service palette accordingly.

Such growth prompted the Basel Committee on Banking Supervision to conduct a preliminary study of e-banking and e-money risks. The study showed an apparent need for more work to be done in the field of e-banking risks. This mission was entrusted with the working group EBG (Electronic banking group) consisting of banking supervisors and central banks. The report by the working group contains a list and assessment of major risks associated with e-banking, primarily strategic risk, reputational risk and operational risk, including internal security and legal risks. It states that e-banking activities do not incur risks which have not already been identified as traditional risks, but modifies and affects the overall risk profile. This means that strategic risk, operational risk and reputational risk are heightened by rapid introduction of e-banking activities.

REFERENCES

Hadžić M., Bankarstvo, Univerzitet Singidunum, Beograd, 2011.

Jović Z., Primena Interneta u savremenom bankarskom i berzanskom poslovanju, Međunarodna naučna konferencija Sinteza 2014, Zbornik radova, Beograd, 2014.

Risk Management for Electronic Banking and Electronic Money Activities, Basel Committee on Banking Supervision, Basel, March 1998.

Risk Management Principles for Electronic Banking, Basel Committee on Banking Supervision, July 2003.

Vasković V., Todorović M., E-poslovanje, Beogradska poslovna škola, Beograd, 2013.