BANKING SECURITY IN THE CONTEXT OF INTERNATIONAL RELATIONS

Adriana BUTCOVAN[1]

ABSTRACT:
IN RECENT YEARS, THE BANKING SECTOR HAS OPERATED IN AN ENVIRONMENT CHARACTERIZED BY A CERTAIN AMOUNT OF INSTABILITY AND UNCERTAINTY, AND THE LOSSES HAVE GENERATED SEVERE DISTURBANCES OF THE BANKING ACTIVITIES. THE REPUTATION AND STABILITY OF BANKING INSTITUTIONS DEPEND ON THEIR ABILITY TO FACE CHALLENGES, WHETHER THEY ARE OF A CRIMINAL NATURE (MONEY LAUNDERING, TERRORISM FINANCING, CORRUPTION OR FRAUD), OR A RESULT OF THE IMPACT OF GLOBALIZATION OR OF ECONOMIC CRISES.
THE TREATMENT OF THIS TOPIC IS NOT AT ALL RANDOM, BEING, IN A WAY, CONSISTENT WITH THE INCREASINGLY APPARENT REALITIES OF THE PAST TWO DECADES, AS WELL AS A CONSEQUENCE OF UNDERSTANDING THE IMPORTANCE OF KNOWLEDGE REGARDING THE FACTORS AND PHENOMENA INFLUENCING BANKING SECURITY, PARTICULARLY EXISTING SOLUTIONS OR SOLUTIONS THAT SHOULD EMERGE IN THIS DIRECTION. ON THE OTHER HAND, EVENTS IN RECENT YEARS IN THE BANKING SECTOR HAVE INCREASINGLY PUT INTO QUESTION A LOT OF MEANINGS OF THE CONCEPT OF "SECURITY", WHICH ARE NOT AT ALL EASY TO MANAGE.

KEY WORDS: BANK SECURITY, MONEY LAUNDERING, TERRORISM, FRAUD, CORRUPTION

INTRODUCTION

The concept of security addresses all levels of organization of a society, from the individual to the state and the international system[2]. Security is based above all on economic stability, but also political stability. Thus, we can say that a viable security system can only be built if these two components are consolidated. Certainty, confidence and peace are rooted not only in the absence of hazards, but also in keeping hazards under control. Banking security is one of the most important sectors of economic security, especially in the context of globalization of international relations.

MAIN TEXT

Why is banking security important for individuals and legal entities? The answer seems to be one of common sense: because they have deposited money and valuables in these

[1] Academic title PhD, Babes Bolayi University, Romania, adriana.butcovan@gmail.com.
[2] See, in this regard, Lucia Zedner, *Security*, London, New York, Edit. Routledge, 2009; *Interpreting Global Security*, edited by Mark Bevir, Oliver Daddow and Ian Hall, London, New York, Edit. Routledge, 2013; Robert J. Fischer, Edward P. Halibozek, David C. Walters, *Introduction to Security*, ninth edition, Waltham, Mass., Butterworth-Heinemann, 2013; New *Challenges for the EU Internal Security Strategy*, ed. by Mary O'Neill, New Castle, 2013, etc.

banking institutions to have them protected and/or multiplied, as well as in order to finance their current activity or needs. Apparently, a discontent customer cannot affect the financial state and stability of a bank, but when complaints multiply exponentially, without the banking institution adopting security measures, the situation may become catastrophic. Bankruptcies of banks in the '90s in Romania have demonstrated the connection between banking security and security and citizens' satisfaction towards the banking system and the economic one, more generally.

The following quotation is a very good illustration of what we are dealing with when working with the human factor: "An impressive steel and concrete bank vault of 3 tons is useless if the back of the vault is made in plasterboard. A prisoner can look back on an electrified barbed wire fence of 15 feet (4.5 m) while exiting through the open gate. And almost any countermeasure that the brilliant engineers designate to protect vital computer systems and valuable information can be accidentally or intentionally circumvented by human interaction"[3].

Job security is another problem faced by the banking sector and, hence, by its employees. This issue is related to corporate security, but indirectly, to human security, as well. Several studies carried out in connection with the restructuring of banks (in the context of the economic crisis) and the perception of job security that bank employees have, revealed different results, depending on age, gender and training of the employees by the management, but could not invalidate the impact of this problem[4]. A decrease in job security may lead to the kind of problems signaled by the above quotation. Human error, whether accidental or intentional, may lead to multiplied costs, an aspect which should not be neglected by banks, nor by any other companies. But the cost-benefit ratio between policy change and its possible effects should always be taken into account.

An intermediate variable is also the security of personal information. Banks and other credit institutions operate with personal information of their customers, whose interception by third parties may have serious consequences for the security and identity of the individual. So, the computerization of society makes personal safety vulnerable.

Using banking security as a case study of human security, we have found that natural or legal persons make bank deposits in order to have their money protected from physical safety hazards (banks are better equipped to protect valuables than citizens' dwellings), but also because banks invest these values and multiply them (interest). Banking institutions are a favourite target for physical or cyber crime, and in this case the source of threats are individuals or organized crime groups willing to break the law and the economic rights of investing fellow citizens. The success of the attacks on bank assets depends on the vulnerabilities of the banks, and the latter are, most often, caused by intentional or accidental human errors. At the intersection of vulnerabilities and threats lies the banking risk, which exists independently of our will and can be calculated and, therefore, reduced. In recent decades, banking institutions have been in constant competition in order to achieve a higher profit. This "war" for power, a precarious "balance" between demand and supply, between selfish interests of obtaining wealth and welfare, has been a source of insecurity that has affected the individual-bank relationship.

The economic environment, in general, is constantly changing and, as such, subject to uncertainties. Specialists in the economic field, and not only, see the banking system as that system capable to manage risk. Any financial and banking operation is accompanied by a set

[3] Jeff Schmidt, *Humans: The Weakest Link In Information Security* (Forbes, November 3rd, 2011. Source: http://www.forbes.com/sites/ciocentral/2011/11/03/humans-the-weakest-link -in-information-security/).

[4] Ademola B. Owolabi, *Effects of Reengineering in Banks on Employees Perception of Job Security*, (Journal of Management and Strategy, Vol. 2, No. 4, December 2011. Source: Ebscohost).

of risk factors. Financial markets are now much more, which leads to an increase in uncertainty. Economic and banking events in recent times have brought to the surface the fact that the problems that the whole system is facing are precisely the result of heightened risks. Effectively managing banking risks may positively influence a bank's reputation. On the contrary, ineffective management can affect negatively the reputation of other banks, as well. There are risks involved in the banking activity, and the main objective of risk management is to manage them. Only banks that are capable to manage risks and accept them have the ability to forecast future events.

Risk can have a clear impact on the value of a financial institution or banking institution, either as an impact caused by the effects on the staff, partners, customers or the banking authority, or as direct losses incurred. In the banking sector, the risk should be viewed as a conglomeration of dangers, often interdependent, which have common roots, or the occurrence of a type of risk can generate a succession of other risks [5].

Moreover, the banking sector risks are extremely numerous and of various types; they are determined by events occurring at an intra-bank, as well as inter-bank or international level, so that nowadays we can no longer speak of an analysis that does not include an approach from the perspective of international relations. In the specialized literature we find a lot of classifications, based on various criteria. These classifications take into account variables generating risk, their overall approach allowing for a separation of risks: macroeconomic changes, GDP (gross domestic product) dynamics, inflation rate developments, monetary policy, changes as a result of financial, banking and economic regulations, instabilities caused by the employees of a bank with inadequate training, poor organization of the bank, incorrect and unsupervised performance of operations, financial decisions on the bank's equity, interest rate, credit, liquidity, political and economic conditions existing in the country that have an impact on the bank's activity.

Another problem that the banking system is facing is the phenomenon of money laundering and financing of terrorism. In this context, the money laundering phenomenon has gained, since its emergence in the modern version, a clear international dimension. Those who practise this mechanism, of money laundering, try to prevent the discovery of their illegal actions by hiding as deep as possible values resulting from such actions, by various means, which give them a lawful appearance, so that they may be easily introduced into the economic circuit, without being detected.

The international dimension also resides in the manners of concealing values obtained from money laundering, namely through international financial transactions. Thus, the profits achieved illegally are "laundered" much more easily if transferred to a foreign currency, and then brought back to the country of origin as such to be turned and capitalized as clean sums.

Losses resulting from the criminal offence of money laundering affect the entire global economy. Given the rapid movement of values, offenders manage to reinvest the amounts involved in various legal business transactions. Currency exchange rates or even interest rates at worldwide level may be affected this way. So we can say that in the economic market, clean, as well as "dirty" money is circulated.

The modernization of communication technology, as well as the globalization of the economic system helped the development and expansion of this phenomenon. Thus, offenders may transfer in a very short time, large amounts of money from one country to another using the computer, via online transfer services offered by banks.

---

[5] Gheorghe Manolescu, Adriana Sîrbea Diaconescu, *Management bancar (Bank Management), (*Bucharest: Edit. Fundaţiei "România de Mâine" (Publishing House of "România de Mâine" Foundation, 2001), 123; R.P. Nainta, *Banking system, frauds and legal control. Evolution, RBI, bank frauds, legal control, security measures, recent trends*, *fore*word by B.R. (Sharma, New Delhi: Deep & Deep, 2005).

There are areas with different tax regimes, that result in an attraction of capital and tax havens, especially for people who want to launder money resulted from illegal businesses. An example in this respect is Grand Cayman Island, where income is not taxable and it is not mandatory to communicate the name of the beneficiary of a bank account.

The process of money laundering goes through several stages and involves many individuals and entities. The purpose of this process is to make the funds resulting from an illegal activity appear as legitimate as possible. To this end, money launderers acts in several stages.

But money laundering is always based on a criminal offence generating money illegally, such as: illicit drug trafficking, human trafficking, illegal arms trade, theft, fraud, forgery, domestic fraud, bribery, computer system fraud, forced "protection" provided by mafia groups, tax evasion. And the result of such offences is "dirty money" whose source is punishable by law. The stages of the phenomenon of money laundering are: placement (pre-laundering), stratification (the laundering itself) and integration.

With the development of organized crime, the profits achieved have also increased, and the banking circuit has been involved in the transfer of illegally acquired funds; this has become a necessity of financial and technological progress for those involved in money laundering. The policy of authorities and the obligation of banks is to disclose and prevent the traffic of illegally obtained funds.

In terms of preventing and combating the financing of terrorism, the direction and the level of development of the mode, the mechanism of supporting terrorist entities are constantly changing and follow specific developments. Identification difficulties arise from access to legal resources and channels by terrorist entities, as well as their interweaving with illegal ones. Those wishing to plot terrorist attacks seek to identify new ways of doing it, characterized by vulnerabilities of the legal and economic system, but also by limited monitoring capabilities.

Terrorism is a branch of organized crime, just like the phenomenon of money laundering. It is generated by ideological, nationalist interests or even interests related to financial resources. The level and direction of development of this phenomenon are in constant change and go through specific developments, making it very difficult to control. The financial, banking infrastructure is a key element in the discovery and eradication of terrorist networks, and is also an important measure for all the countries of the world.

The dimensions of a financial attack appear as quiet actions and represent only a small part of the whole financial effort. Most financial transactions become alarming only when associated to suspect people. In very few cases, the actual transaction can provide critical indicators that make it possible to identify the involvement in terrorism financing actions. In most cases, the transaction will be part of the broader picture, which adds numerous elements in order to understand and assess what is happening. Only abnormalities or changes in the payment patterns can provide details regarding the planning of such acts of terrorism, so that offensive measures can be taken against the terrorists' funds. It should be noted that, in general, terrorist groups are not interested in profit, only in funds for the subsistence or financing of terrorist acts. Money funds are transferred most often in small amounts, making them extremely difficult to identify and associate with acts of terrorism financing[6].

Compared to the phenomenon of money laundering, we can say that in terms of terrorism financing, there is no clear pattern of sources or of the transactions performed. The

[6] National Office for the Prevention and Control of Money Laundering, *Manual privind abordarea pe bază de risc şi indicatori de tranzacţii suspecte*, (Bucuresti: Editura Prahova, 2010), 17.

stages or sources by which a terrorist group finances its actions are: fundraising, money transfer or movement and spending of the funds[7].

In most cases the phenomena of money laundering and terrorism financing contain similar transactions, most of which are related to the concealment of funds. Owing to the development of the methods of money laundering, and the effects of terrorist attacks, at national and international level, it is necessary to constantly update the strategies and regulations of all organizations involved in preventing and combating money laundering and terrorism financing in order limit the risks and vulnerabilities of the entire economic system, and not only, in dealing with these two criminal phenomena.

Banking institutions are facing another problem, which also has a negative impact on activities and, in particular, on the reputation and credibility of a bank, namely bank fraud. This phenomenon has become, over the years, part of our daily lives. In all spheres of activity, there is a wide variety of fraud types. Substantial funds are needed in order to explore current fraud events, to manage and prevent such crimes. The minimization and prevention of this threat requires more than the introduction of mechanisms for fraud control or of fraud detection technology, no matter how sophisticated and advanced they may be. Those who intend to produce frauds are always one step ahead and always find the methods, as well as the right time to implement their plans. Just one moment of carelessness or misuse of the control mechanisms are sufficient for potential offenders to take action.

All major operational areas of the banking sector provide good opportunities for criminals. Most incidents of fraud are reported in customers with deposits, loans and banking transactions, including cash remittances. The best defence against fraud is vigilance and appropriate training, together with the reporting to the competent bodies of any suspicion or suspicious acts that may occur.

Therefore, banking institutions should adopt an anti-fraud policy whose aims are as follows: training the employees on how to conduct themselves, in order to recognize a case of fraud, as well as promoting an anti-fraud conduct and culture at all levels, knowledge by the employees of the methods to discourage and prevent acts of fraud, development of certain systems, regulations and control mechanisms to prevent and combat fraud, the establishment of actions to be taken by banking financial supervisors where a fraud occurs.

As a result of fraudulent activities, all persons involved in the client-bank relationship have to suffer. The management and staff of each banking institution should place the emphasis on preventing and combating fraud. Such actions are against the principles and values underlying the activities of banking institutions and have or may have a negative impact on the reputation of the institutions concerned and the interests of customers, shareholders and employees. Strict adherence by the staff of a banking institution to the requirements in terms of rules, procedures and roles for each object of activity and area of activity is essential to the safe and continuous operation of the bank, as well as to preventing fraud and other inappropriate or illegal acts that could harm their interests.

With the computerization of banks, new technology-based types of fraud have emerged, which, when successfully committed, are difficult to track down; financial losses of banks are at unimaginable levels. It is very difficult to follow all the permutations and combinations of opportunities that criminals pursue and these are also impossible to prevent before they become apparent. Only continuous monitoring and analysis of fraudulent activities can help us understand the reason behind a fraud, so that we can take preventive and combating measures afterwards.

[7] National Office for the Prevention and Control of Money Laundering, *Manual privind abordarea pe bază de risc şi indicatori de tranzacţii suspecte*, (Bucuresti: Editura Prahova, 2010), 17.

Since many of the banking institutions are not satisfied with the already existing technology, they have decided to adopt new technologies, to introduce new management and employment objectives. Many of them have decided to remove the old software by stages, in order to better satisfy the customers.

Currently, banking institutions are in a position to offer banking services through alternative channels by integrating front-office and back-office operations. The customer is the one who decides what fits them best. To satisfy the customer, every banking institution adds attractive parts to the banking product. This requires a lot of technology, expertise and awareness on the part of the bank and of the client, because the bank can become a prey to computer fraud. Banks are the ones to decide on the modernization of their computer networks in order to offer their services through as many channels as possible. That is why they are currently facing risks from inside the bank, as well as from outside. The best defence against fraud cases is vigilance and appropriate training, together with the reporting to the competent bodies of any suspicion or suspicious acts that may occur.

Bank corruption is another phenomenon just as intense in terms of desecuritization of the banking system. The phenomenon of corruption has attracted attention since ancient times. With the advent of social and economic crises and of unfair competition, the degradation of the living standard, the diminishment of the state's authority, the failure to adapt to economic and social legislation, the lack of legislative and institutional reforms which should be consistent with socio-economic conditions, the phenomena of corruption also multiply. There seems to be a desire of the population to get rich as fast as possible and by any means; destitution generates speculation and prohibitions affect consumption, all of which shape the cause of this antisocial phenomenon.

This antisocial phenomenon may jeopardize the orderly conduct of any banking institution, and not only[8]. Over the course of time, many bank employees or managing staff have been investigated for corruption. They were involved in various processes that had an impact on the smooth unfolding of the activity of the banking institutions concerned, but also in terms of customer confidence in these institutions. The desire of some people to get rich by any means and as quickly as possible made the banking system vulnerable.

CONCLUSION

The question is whether crime in the banking system can be stopped? The answer is "**NO**". This issue is an endless one, because, over the years this phenomenon and the fraud methods have evolved, but they have always existed. These attacks occur not only at the level of the banking system, but are present in all areas of social life.

I believe that banking system security can be enhanced by building and improving collaboration between banking institutions, governments and institutions specialized in combating criminal phenomena. It is also important to adapt the national security strategy to these problems, and to extend security, so as to support banking security, as well as national or global security.

[8] Mario A. Aguilar, Jit B.S. Gill, Livio Pino, *Preventing fraud and corruption in World Bank projects. A guide for staff*, (Washington, D.C.: The World Bank, 2000); Heather Marquette, *Corruption, politics and development. The role of the World Bank, Basingstoke*, Palgrave Macmillan, 2003.

REFERENCES

1. **Aguilar, Mario A.; Gill, Jit B.S. and Pino, Livio**; *Preventing fraud and corruption in World Bank projects. A guide for staff*, Washington, D.C.: The World Bank, 2000.
2. **Fischer, Robert J. ; Halibozek, Edward P.; Walters, David C**.; *Introduction to Security*, Waltham, Mass., Butterworth-Heinemann, ninth edition (2013).
3. **Manolescu, Gheorghe and Diaconescu, Adriana Sîrbea**; *Management bancar (Bank Management)*, Bucharest: Fundaţiei "România de Mâine", 2001.
4. **Marc, Bevir; Daddow, Oliver and Hall, Ian**; *Interpreting Global Security*, London, New York: Routledge, 2013.
5. **Marquette, Heather;** *Corruption, politics and development. The role of the World Bank*, Basingstoke, Palgrave Macmillan, 2003.
6. **Nainta, R.P**.; *Banking system, frauds and legal control. Evolution, RBI, bank frauds, legal control, security measures, recent trends*, New Delhi: Deep & Deep, 2005.
7. National Office for the Prevention and Control of Money Laundering; *Manual privind abordarea pe bază de risc şi indicatori de tranzacţii suspecte*, Bucureşti: Prahova, 2010.
8. **O'Neill, Mary**; *New Challenges for the EU Internal Security Strategy*, New Castle (2013).
9. **Owolabi, Ademola B**.; *Effects of Reengineering in Banks on Employees Perception of Job Security*, Journal of Management and Strategy 4 (2011).
10. **Schmidt, Jeff**; *Humans: The Weakest Link In Information Security*, Forbes, November 3rd, 2011. Accessed March 19, 2013; http://www.forbes.com/sites/ciocentral/2011/11/03/humans-the-weakest-link -in-information-security/
11. **Zedner, Lucia**; *Security*, London, New York: Routledge, 2009.