Economics and Management
ISSN: 2367-7600; 1312-594X
Volume: XV, Issue: 2, Year: 2018, pp. 27-43

ВЗАИМОДЕЙСТВИЕ НА СЪОТВЕТСТВИЕТО МЕЖДУ БАНКИТЕ И СИСТЕМИТЕ ЗА ОПОЛЗОТВОРЯВАНЕ НА ИНФОРМАЦИЯ В БАЗИ ДАННИ, СЪЗДАДЕНИ ОТ ТЯХ

Елена Ставрова, Недялко Вълканов

CORRESPONDENCE INTERRELATIONS BETWEEN BANKS AND SYSTEMS FOR INFORMATION DISCOVERY IN DATABASES CREATED FOR THEM

Elena Stavrova[1], Nedialko Valkanov[2]

Received: 30.10.2018, Accepted: 10.11.2018

Abstract

This article studies the possibility of using the correspondence relations between banks as mechanisms for legalisation of funds of an obscure or criminal origin, in times of economic instability, local wars and introduced restrictive sanctioning action in respect of certain economic regions as well as the methods for prevention of such attempts. It is impossible to provide an efficient system for monitoring and registering the financial transactions of suspicious customers or these originating from areas with possibilities of tax planning, without developed systems for automation of selection and processing of bank information.

A particular attention is paid to the methods using information technologies for processing the database containing the transactions carried out through iteration procedures, as well as to the heuristic methods for unsystematic transactions containing suspicious features between correspondent banks for cash flow circulating in various segments of the financial system.

Keywords: *international financial and economic sanctions, steady management, correspondent banks, relational base, associative rules, information technologies, heuristic methods.*

JEL Codes*: G02, G18, G38.*

[1] South-West University "Neofit Rilski"-Blagoevgrad, Faculty of Economics, Assoc. Prof., PhD, helena_stavrova@abv.bg
[2] University of Economics, Varna, Assist. Prof., PhD

1. Introduction

The terrorist attacks in September of 11, 2001, the annexation of Crimea from Russia, and the war in the Middle East and Syria have been recent milestone of all effort, attention and instability who provoke not only a huge loss for the local populations, because they were under threat and instability in the financial systems of other countries. Here appears the need to limit to full access to the resources of criminal regimes, military groups of people and criminals. Efforts to actions the financing of terrorism and criminal group are a central pillar of this approach. Restricting access to finance criminal activities is one way to limit their actions, but also by preventing the expansion of their activities and the damage to society as a whole. Community of interest in law enforcement, including the various components of the national legal systems of the countries concerned undertake joint efforts of national institutions and experts to identify, investigate and combat specific threats, enforcing the applicable laws and regulations and prosecuting supporters to actions deter potential funders forces.

The introduction of restrictions on the free movement of capital and financial flows from the international community imposed a step towards limiting the hostilities and the destruction and criminal behavior towards monuments of ancient architecture and international heritage.

The last event of economics and financial sanctions were caused by annexation of territory of Crimea from Russia last March redirect the efforts of the United States and the European Union reacted by with economic weapon - sanctions.

The first measures were implemented in March and April of 2014 directed and Russian officials from the Crimea, and businessmen who are considered to have close ties with Russian President Vladimir Putin with travel bans and freezing of assets. Since then, the West continues to expand its sanctions against Russian entities aimed at large enterprises and parts of Russia by the financial industry, energy and military industries.

The sanctions imposed by the United States came in two stages. The first concerned the Crimea, and they were only personal sanctions for the Crimean and Russian leaders involved in the Crimean drama.

First imposed sanctions important to July 16, 2014, called sectorial sanctions.

This leads to a determination to stop the cash inflows as investments in Russia after the introduction of sanctions. Russia's GDP is expected to shrink by 6.5 per cent in 2015, inflation to rise to over 13% and it is estimated that more than $ 135 billion is possible to leave the country after the marked outflows flows last year. Rating agency S & P reduced the sovereign rating of Russia to BB +, or below investment grade. The point is that by the middle of this year, the financial sanctions have worked as caused far more severe their effect than anyone imagined.

There are three main reasons for the economic problems of Russia. The first reason is corruption and bad economic policies that Putin pursues that alone will lead to stagnation, or at most 1 percent growth.

The second element is market volatility and a decline in oil prices. Oil prices have now fallen so much that the total revenues of Russia's exports this year will be two-thirds of what they were before. This means that Russia will have to reduce their imports by half.

Table no. 1. List of countries to which has introduced sanctioning actions

Country, sanctioned by EU	***Country, sanctioned by USA***	***Country, sanctioned by other countries***
Afghanistan, Belarus, Bosnia and Herzegovina, *Burundi, Central African Republic, Congo (Democratic Republic of), Cote d'Ivoire, Crimea,* *Croatia, Egypt, Eritrea, Guinea (Republic of - Conakry), Guinea-Bissau (Republic of), Haiti, Iran, Iraq, Korea (Democratic People's Republic of), Lebanon, Liberia, Libya , Moldova, Russian Federation, Somalia, South Sudan, Sudan, Syria, Tunisia, Ukraine, Yemen,*	*Belarus, Bosnia and Herzegovina, Central African Republic, Congo (Democratic Republic of), Cote d'Ivoire, Crimea, Cuba, Iran, Korea (Democratic People's Republic of), Somalia, South Sudan, Sudan, Syria, Venezuela, Yemen,*	*Arabic countries prohibit transactions involving Israel, Informal sanctions against The Netherlands, Syria,*

Sources: http://www.bscn.nl/sanctions-consulting/sanctions-list-countries

Economics sanction
freezing of funds and economic resources, restrictions on admission, embargo on arms and related materiel, ban on provision of certain services, ban on exports of equipment for internal repression, prohibition to satisfy certain claims in accordance with UN Security Council Resolution No 917(1994) *- prohibition to satisfy claims with regard to contracts and transactions whose performance is affected by the measures taken in accordance with UN Security Council Resolutions 917(1994), 841 (1993), 873 (1993) and 875 (1993), embargo on telecommunications monitoring and interception equipment, embargo on nearly all dual-use goods and technology, embargo on certain goods and technology which could contribute to enrichment related, reprocessing or heavy water-related activities, or to the development of nuclear weapon delivery systems or to*

the pursuit of activities related to other topics about which the IAEA has expressed concerns, controls on export of certain other sensitive goods and technology, control on provision of certain services, - control on certain investment , ban on certain Iranian investment (nuclear industry), ban on new commitments for grants, financial assistance and concessional loans to the Government of Iran ,

Financials and related sanction
freezing of funds and economic resources, restrictions on admission, embargo on arms and related materiel, ban on provision of certain services, ban on exports of equipment for internal repression, prohibition to satisfy certain claims in accordance with UN Security Council Resolution No 917(1994) *- prohibition to satisfy claims with regard to contracts and transactions whose performance is affected by the measures taken in accordance with UN Security Council Resolutions 917(1994), 841 (1993), 873 (1993) and 875 (1993), embargo on telecommunications monitoring and interception equipment, embargo on nearly all dual-use goods and technology, embargo on certain goods and technology which could contribute to enrichment related, reprocessing or heavy water-related activities, or to the development of nuclear weapon delivery systems or to the pursuit of activities related to other topics about which the IAEA has expressed concerns, controls on export of certain other sensitive goods and technology, control on provision of certain services, - control on certain investment , ban on certain Iranian investment (nuclear industry), ban on new commitments for grants, financial assistance and concessional loans to the Government of Iran .*

A central part in the activity of Basel Bank Supervision Committee, European Committee of Security, FATF, and other international institutions is taken by the role of the financial institutions, by studies on the methods of money laundering (Stavrova, 2007, p. 42) and their use for terrorist organisations financing (Valkanov, 2005, p. 18). A priority place is taken by the alternative payment forms (Stanley, 1998), drug traffic, telegraphic transfers, money laundering in regard to financial support for terrorist organisations (Ganchev, 2004, p. 22-29), (Nikolov, 2004, p. 30-36) and in connection with human rights and conditions of life, illegal immigration, the threat of legalization in the insurance sector (FAT, 2004-05, p. 11).

The role of the financial institutions in the prevention and exposure of money laundry has been a matter of investigation governed by the Basel Committee of Bank Supervision, the European Union and the International Committee of Security. The large-scale international private banks, among which ABN AMRO Bank, Banko Santander, Central Hispano S.A., Chase Manhattan Corporation, Citibank, N.A. Credit Suisse Group, Deutsche Bank AG, HSBC, J.P. Morgan Inc., Societe Generale UBS AG, adopted

common principles as an important global guide for steady management in the international private banking (GAL, 2004, pp. 12-14).

The aim of the bank policy is to prevent the use of banks' global operations for criminal and illegal acts. The banks make efforts to accept only the clients whose sources of property and funds can be proved and legitimised.

2. Conceptual framework

The correspondence accounts opened with foreign banks, with which correspondence relations have been established, can become conductors of "dirty" money. The correspondence bank accounts concern the services offered by a particular bank to other banks for funds transfer, currency exchange or other financial transactions. Foreign banks can open correspondence accounts with any bank having a permit to carry out bank activities in the country. These accounts provide a direct approach to the bank system and freedom for funds transfer anywhere in the world for the owners and customers of badly regulated, managed and sometimes corrupt foreign banks with an insignificant or no control against money laundering.

In the banking industry it is considered as a normal for the banks to have dozens, hundreds and even thousands of correspondence relations, even a certain number of relations with a foreign banks of high risk.

Without the presence of an automated observation and control system to report suspicious features of accounts or acts concerning money transfer and if relying only on manual methods to review the activity in the accounts, the limited supervision on the money transfers cannot ensure a serious review on the relations and result into particular actions for the prevention of money laundering. In many cases foreign banks of high risk are granted access to the national financial system not by opening their own correspondence accounts, but through correspondence accounts in some other banks.

The Bulgarian banks seldom ask their bank-customers of their correspondence practices and in most of the cases they are in total ignorance of the correspondence relations of their partners.

Many cases of money laundry through the use of correspondence accounts have been proved by documents in the world practice. They find manifestation in the following acts, operations and deviations from the general bank practice:

1. Telegraphic transfers of large sums, when the correspondence account is not used.
2. Unusually great number of telegraphic transfers.
3. Telegraphic transfer operations with unreasonable reiterations or of unusual character.
4. Unusually high volume of unrealised or rejected operations.

5. Inquiries from correspondent banks for establishment of relations with financial institutions that do not maintain contacts with an international bank, have not been notified of expressed intentions of such operations or of operations carrying out through this institution.

6. Organising the route of transfer operations via several countries of different jurisdiction and/or financial institutions up to or after their entry into the bank without a clear goal concerning the disguised operation, the funds source or their holder or sender.

7. Frequent or numerous bank transfers without the physical presence or correspondent bank of high risk.

8. Obtaining benefits from operations in accounts with a foreign bank that has participated in such suspicious acts related to bank transfers of considerable sums or other operations with considerable sums.

9. Repeat appearance of beneficiary banks in offshore areas with correspondent accounts one of which in the event has been closed down for a suspicious activity.

10. A considerable number of foreign currency transactions or transactions with documents of the beneficiary of the correspondence accounts or correspondence account of a correspondent bank.

11. Presentment of a correspondence account or removal from an account of a correspondent bank of considerable sums with financial documents (traveller's checks, payment orders, bank-bills), especially if the amount is just below the amount, subject to report in one day, or if they are collateralized with documents with consecutive numbers.

12. Receiving mail transfers of funds that have passed through a correspondent bank.

13. Bank transfers in accounts of persons, suspected by the law-enforcing authorities in the commitment of similar acts.

14. Correspondent bank's inquiries about exceptions in the requirements of reporting, stipulated in the Bank Secrecy Act or in other Rules, requiring information of suspicious transactions.

Measures have to be undertaken to limit the risk of using the correspondence relations between banks for laundering money of criminal origin, as follows:

1. Accounts in trust must be managed only after finding out if the customer acts on behalf of somebody else in the capacity of an agent (trustee). This is a necessary prerequisite for gathering of sufficient information to identify any persons or agents, for releasing information about them, as well as for gathering information about the character of the fiduciary relations.

2. Corporate mechanisms – vigilance for use of physical persons by legal entities to manage anonymous accounts. For the banks it is necessary to be aware of the company structure, origin of funds, to find out the beneficiary owners and the persons holding the right to control the funds, as well as to verify the documents for transactions management in the Internet. (Basel BCBS, 2003).

3. A special caution in regard to companies with nominal shareholders or bearer shares. It is impossible to carry out a thorough investigation on the ownership. The bank is responsible to develop procedures for the establishment of identification information of the large-scale beneficiary shareholders.

4. If services were provided to new companies the identification procedures would go against the endeavour to diminish the inconvenience they would suffer as new customers.

5. The persons, subject to political risk – occupying significant public positions, as well as persons and companies in direct link with them that can bring the bank reputation under threat and juridical risk. These are persons occupying significant public positions as a head of state, head of government, leaders of political parties, representatives of military and court institutions. There is always, especially in the countries with high risk of corruptive pressure, a hazard of abuse of public authority of such persons with the purpose of an illegal enrichment. Usually, such cases are largely reported by the mass media and bring to vigorous political reactions, even if the illegal character of the act can hardly be proved. The bank can suffer considerable expenses to gather information and order by law-enforcing or judicial body. The bank employees can be accused of legalisation of funds received illegally during election campaigns, funds raising raids, etc.

6. The due diligence process of the accounts and transactions can result into a clear vision of the normal and reasonable activity in the bank clients' accounts. Without such information they probably would not meet their obligations to report suspicious information to the authorised organs when required. The volume is determined with taking the risk into account and the grade of recognition of unusual and suspicious schemes is found out. This is implemented through the establishment of limits for particular classes of accounts. Some types of transactions have to give rise to bank employees' keen attention and suspicion (for example, those irrational from the position of the economic potential of the client).

Adequate analysis systems for managing board information and efficient monitoring are necessary for the accounts of clients of high risk. Reporting the lack of documents for opening of accounts for the transactions via the clients' accounts and the general information of their operation could be used.

One of the most important tasks, connected with the implementation of the legal acts, is the automation of the processes of selection of information from the available databases concerning the clients and geographical regions of high risk. In implementation of the Law all funds-lending organisations are obliged to establish databases containing information of transactions that could be an evidence of legalisation of criminal incomes. The considerable data arrays, and particularly the companies' foreign economic turnovers can hardly be controlled, but in accordance with the requirements of the control organs the bank of account must receive and keep the data contained in the database. The essential elements of the foreign counterparties comprise their complete address, the

name of the country of registration, address activity, number of the supply contract, and term of validity, amount and the price in the settlement currency, manner of payment. According European law foreign currency transactions to the amount exceeding BGN up to 30 000 without cash and up to BGN 10 000 in cash of residents. Concerning foreign currency loans granted to non-resident, as well as the right of granting foreign currency loans to non-residents, are the major part of the database kept with the bank of account. The commercial banks have no right to debit/credit a bank account unless they submit to the BNB data of the transaction character and the foreign counterparty, fixed in the database.

In compliance with the BNB's requirements the commercial banks are obliged to establish detailed data files for each foreign currency transaction of their corporate clients. This way it can be ascertained that nowadays the commercial banks and the BNB keep regularly updated databases with actual information of the foreign currency transactions. Of course, it has to be mentioned that only a part of the information concerning the clients' infringement of the currency control acts that is kept with the banks is submitted to the BNB. A disadvantage of the established base is the restriction in stating only the transactions, settlement instruments, in which there is a partial appearance of free traded currencies. Therefore the barter transactions, the settlements in BGN, and in exotic, seldom used currencies, does not come into the range of vision.

The major aims set before the specialised database processing, established on the basis of the regulative documents for the implementation of the strategy of counteraction to the legalisation of the criminal incomes and fight with the tax offences can be formulated, as follows:

1. Searching for the counterparties of the companies in suspicious business, assessment of their foreign business contacts and the character of the transactions following the submission of information by the commercial bank.

2. Defining the schemes of assets transfer from one company to another by investigating their foreign counterparties that are regularly losing in their foreign economic activities on the basis of schemes of VAT recovery, fictitious export, etc.

3. Investigating schemes of transactions between connected persons with the purpose of additional assessment of taxes, if the deal price differs substantially from the market price.

The solution of similar problems supposes the use of efficient information technologies for knowledge discovery capable of retrieving non-trivial information from the established database, known as KDD-technologies (Knowledge Discovery in Database). These technologies, integrating the capacities of standard technologies as Systems of Databases Management and of the outselling Data Mining, give an opportunity to use a systemised database for models building, for formulation of classification database relating rules, for definition of clusters based on classification rules.

The standard operational diagram of KDD comprises:

1. Selection of elements according to a defined attribute
2. Preliminary processing
3. New database conversion
4. Self-construction of the demanded model of interrelation between the analysed elements.

The major part consists of a relational basis with a structure formed by linked tables, with each column corresponding to stored data of the counterparties in the correspondent banks' network. The analysis of actually existing data associations is the most efficient way to discover information in the database. Data association is known as data set, united integrated information content. Association analysis asks for a reply of a typical question for search of uniformity among the assigned objects' data. All the information stored in the database of particular physical persons, organisations, documents, payment transactions can be related to such data. To the end of analysis completion the user of the database cannot suppose which data exactly contain the information he is interested in. In future comparisons with other types of relations connected in some other functional interdependence the data form a subset containing new non-trivial information, i.e. knowledge.

Practically, the only means of access are the SQL-inquiries as a universal means for manipulation of data contained in the relational database, maintained by all systems of manageable databases.

Q (C, Y) = (SELECT<Y>WHERE<C>),

Where: <C> is the set of restrictions of SQL

<Y> - the relation forming attributes

The system for knowledge discovery in database has a module structure, as follows:

3 –inquiries; 4 – results; 5 – objects; 6 – association rules;

7 – Objects; 8 – relations; 9 – database structure; 10 – association rules;

11 – Semantic information; 12- database structure;

13- Knowledge; 14 - objects

The module implements the basic iteration procedure for search definition and assessment of the results from the work with the database. The results from each SQL-inquiries are assessed on the basis of the eligibility functions analysis.

$F = \Sigma f(a)$; $f a = (m. n)/q$

Where:

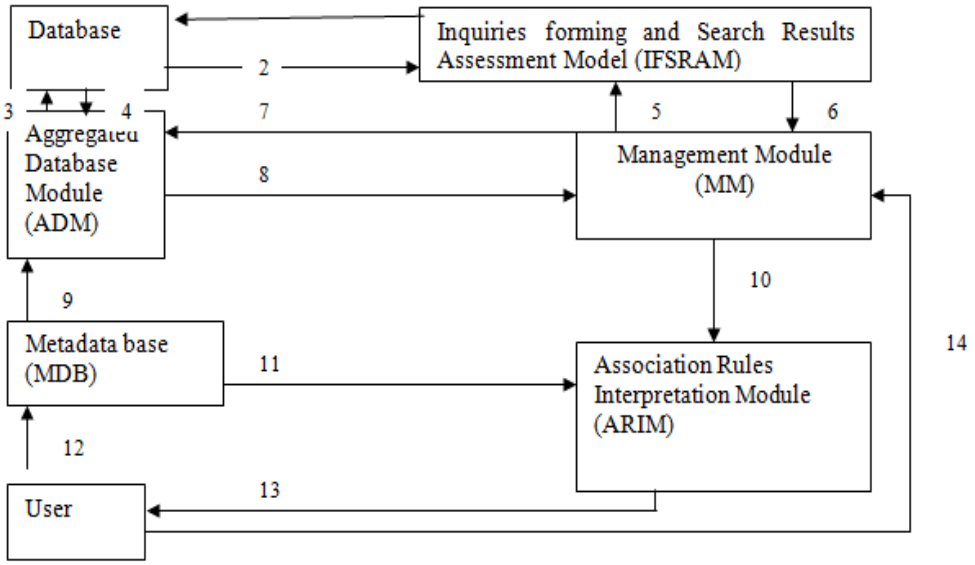
F - Complex function of quality, taking into account the influence of the data in each column of the database table

F (a) intermediate function of eligibility of the results for analysis of the influence of "j" column of the table.

A - Set of restrictions in a particular inquiry

M - the number of objects assigned for search
N - Factor of reading/accounting the records in the database table
Q - The number of appearances of the object throughout the process of search

Figure no.1. Inquiries Forming and Search Results Assessment Module (IFSRAM)



The F function provides and opportunity to take into account the quality of the search results in each column by taking the restrictions (a) into account. The value of f (a) is maximal when m = q, e.g. when all the assigned objects participate in the search, including the new data and taking into account the results of previous inquiries. In such procedure the number of the restricting conditions increases in reply to alterations in the data values (for example close dates or large sums as transaction volumes) or equation in the data value (for example coincidence in the name or registered address of the beneficiary).

Although essentially represent the cash transactions, transfers via systems for fast money transfers deserve further attention. Offered on the used market systems (such as Western Union and Money Gram) than useful for many customers products are cause for further concentration of risk of money laundering[1]. The related obstacles resulting from the fact that underlying these systems principles for funds transfers do not require a complete set of reliable credentials. For example required for each unique transfer control number and any transaction entered names and addresses of the parties to it are insufficient for KYC identification. The only unique and absolutely reliable details are

identification numbers (MTCN - Money Transfer Control Number at Western Union and Reference Number in Money Gram). Also, this type of money transfers are carried out without the need for a bank account, which is an additional facility for their illegal. (See the Law on Payment Services and Payment Systems ", Art. 3, para 1 and Art. 4 pt. 6)

By 2009, the system for fast money transfers are allowed to offer their services only through a bank or exchange office, but after the adoption of the Payment Services and Payment Systems providing this type of services is liberalized, as the same may be offered by other entities such. The Electronic money, persons licensed to provide postal services and payment institutions under this act. For companies that provide such services, the law creates an opportunity to expand their points of sales. This would lead to a reduction in banks carried by fast transfers at the expense of other licensed providers of payment services.

Unlike the business side of this decision (which will inevitably be positive due to increased competition in the market), in the fight against money laundering raises fears that new suppliers of fast transfers are not prepared to effectively counter ML. This can be explained in two ways. First, due to their recent entry into this new market intermediaries in the supply of these remittances have no basis and practice relevant countermeasures. Here, given the special rules and procedures, staff training, specialized software, etc. Secondly, even in the implementation of the above requirements firms that are not banks, not enough information resource to compare with other databases with negative information.

The performed within the banking non-cash (non-cash) transfers include remittances made by debiting the bank account of the payer and crediting the bank account of the recipient. They can be classified as three separate types:

1) Within the same bank;

2) Within another bank in the country and

3) Transfers aimed at abroad.

A major highlight in most reported cases of money laundering are a series of transactions from countries in the regime of international sanctions aimed both at domestic and at foreign banks. Most often they are used during the phase "disguise" (layering). Such transfers shall be effected by cashless bank transfers, which in modern conditions, are carried by automated banking accounting and computer software. So looking suspicious transfers can be allowed to perform smoothly. That is why monitoring this type of banking operations is an essential tool for combating within the banking AML policies and practices in the monitoring of incoming and outgoing cash flows from countries in the regime of economic sanctions.

The interbank transfers aimed at overseas implemented through correspondent banks, under the rules of the organization SWIFT[1], which includes all registered banks in our country. The technology for making transfers through the system allows the availability of data on the payer beneficiary banks in the chain and their locations, but also allows the receipt of orders by ordering that the beneficiary's bank cannot identify. Also, the system does not allow the broadcasting of translation empty requisites, but cannot counteract the introduction of meaningless or incorrect data[2].

A preventive innovation in this respect is the introduction by SWIFT's new format of payment messages MT 202 COV (in using from 21.11.2009), used in correspondent bank transfers such "cover payments". Previously used standard (MT 202) does not correspondent banks the same level of information about the parties to a transfer, as has the sender's bank. Thus practically from correspondent banks downstream to the institution of effective monitoring of translated through these means (a more detailed schematic illustration of technology transfers through the new format is presented in Appendix 14).

The preventive action in relation to non-cash transfers are carried out both by the respective internal procedures, and with the help of specialized software for monitoring and analysis of transactions. Internal procedures, part of the overall AML Policy Bank are subjective in this type of prevention. For example, an internal procedure, after the establishment of dubious translation, a high counterparty or correspondent bank, the relevant employee (usually the back office level) should be alerted about their supervisor or responsible for AML operations officer. They in turn verify the validity of the claim, and when affirmative submit suspicious transaction reports to the security services. According to the internal rules prohibiting entry into and correspondent relations with banks of high-risk countries, countries in the regime of economic sanctions and territories as listed in the instructions themselves.

The automated nature of cashless transfers requires the use of specialized software for monitoring and analysis of operations. Thus, within its policy against money

[1] Society for Worldwide Interbank Financial Telecommunication. Founded in 1973 in Brussels today at the Society for Worldwide Interbank Financial Telecommunication has more than 9000 banks, investment firms and corporate clients from 209 countries. The Company has established standards for international bank transfers on the principle of exchange of electronic messages between financial institutions. Today, SWIFT is global intermediary in making international bank transfers by 2010 per day through the system were implemented in nearly 16 million transactions. In 2006, after a series of publications in the US print management organization recognizes that after the September 11 attacks was provided access to the SWIFT data for various US law enforcement bodies within the program for tracking the financing of terrorism (Terrorist Finance Tracking Program) contrary to current EU legislation and Belgium.

[2] European Regulation 1781/2006 on information on the payer accompanying transfers of funds to the payment service provider requires payment service providers to bring complete information about the payer to funds transfers made electronically.

laundering banks install additional modules for tracking operations. They can operate: 1) real-time parallel with the core banking and accounting software or 2) with a time lag. Operating in real time alarm modules allow for suspected money laundering before finalizing the transaction. This allows making timely and flexible solutions. The second type of information modules from the core banking system is extracted during a given period, usually this happens after processing the data at the end of the working day - "end of day data processing". Then extracted information is filtered and analyzes and displays information about suspicious transactions. The main flaw in the analysis of data with a time lag is reduced reaction time. Extracted from software suspicious transactions provide for subjective analysis only on the next working day and very often it is after the finalization of the transaction.

In this case the software for analysis of the various bank transfer software product Siron® Financial Solutions, is developed by the companies Siemens and Tonbeller[1]. The system was implemented in several European banking groups, including operating in the country Société Générale and Raiffeisenbank, as of 2007 the system is applied in the Bulgarian practice. The product integrates module for filtering the information system for checking identity and analytical modules for comparison and interpretation of the information gathered. To the system can connect to databases negative information. In summary, analysis of operations goes through the following sequence: data entry identification of counterparty's translation categorize the information gathered evaluation arrive at the conclusion. The system allows the creation and introduction of the "rules" of each bank, according to the specifics of its activities, national legislation, etc[2].

After the events of 2001, most banking groups begin to install filtering systems in order to prevent automated execution of suspicious transfers. With these systems pre-compiled data set with negative information, which collated all incoming and outgoing transfers. Upon detection of a match (full or partial) system temporarily "detained" for the transfer and return it for further consideration by the operator. Belonging to the main part of our banking system to a major European bank holding companies contributes to the implementation of such filtering systems at national level. Although each of our banks has its own SWIFT address the possibility of own choice of correspondents in international transactions, most banks use the infrastructure for translations of their mothers' owners. So dubious translation broadcast by our banks, "halt" and returned for further identification of the filtering systems in their respective plants.

[1] More product information is available at http://www.tonbeller.com/, in Section SIRON® Financial Solutions. List of leading AML software see. In Annex 15.

[2] Another example embedded in Bulgarian banking practice software is applied by DSK software "Norkom", created by the company Detica (www.baesystemsdetica.com)

Another positive point is the introduction of the single standard for numbering bank account - IBAN[1] in 2006, a bank account number allows for easy identification when checking and analysis of suspicious transfers. In recent years, the share of ordered through alternative banking channels (Internet, telephone, text massage) operations. Their comfort with a view to saving time and cost of translation is indisputable, both the customer and the bank. On the other hand, the technology determines their greater degree of anonymity. Anonymity, which can be used in operations in money laundering and terrorist financing and transfers of cash flows from countries in the sanctions regime ordered by distance. Along remotely transfer is performed directly without the involvement of front office staff, its accounting in the back office, in most cases follow, once the operation was completed. This requires the introduction of additional controls in the monitoring of remote operations ordered. Such a measure example is the requirement for additional identification and subjective operations above a certain threshold

The management of the process of alteration of the values of columns in case of inquiries is carried out with a procedure implementing the algorithm of random search with an adaptation.

Heuristic methods (Methorn, 1983, p. 12-79) are the methods based on the intellectual activity of a person who has found a creative solution of a particular problem and is able to make this process accessible and include these methods in solving a particular problem. The knowledge acquired at school and professional environment, the transfer of received information, and the personal qualities developed by experts give an opportunity of a statement and taking a decision on any specific practical case.

Trial-and-error method is one of the most applied methods for a system search and coming to specific intellectual results. It is carried out through "trials" on a randomly chosen object of full test. Its major disadvantage is the practically unlimited number of possible tries, but there is a possibility of elimination of particular objects from the database and this way of limitation of the array of possible operations to be tested. The advantage of the method when applied for studying the correspondence relations between banks with partial or full tests and the results from the studies is the fact that it is actually utilisable.

Aphthonius's Method was developed in the 3rd century and is a modern algorithms structured with the help of "questions and definitions".

For example: Algorithm of studying transactions between banks

1. Who? – Who initiates the transaction?
2. What? – What type of contract is it – episodic or systematic?
3. Why? – What is the grounding for the implementation of the transaction?

[1] IBAN-number is 22 characters in the format: BGkk BBBB 1111 2233 3333 33 where: kk - control numbers; BBBB - BIC code, 1111 - Number of branches (BAE), 22 - type of account, and 33 3333 33 - account number.

4. Against? – Are there any doubts (+) or (-)?

5. Analogy – Have there ever been any similar, equivalent or comparable cases of transactions?

6. Examples – Are there any examples in historic, chronological or regional plan?

7. Proofs? – Are there any proofs in support or denial of the doubt?

An algorithm of this type for studying the relations between correspondent banks establishes a prerequisite of systematic investigation and at the same time of purposeful expansion of the sphere of search in the database for cases that come within the provisions of law.

Thorough knowledge in various field of human cognition are necessary to apply the Method of Aphthonius, they are compared in searching for particular decisions.

Sinitics Method.

Its name is of Greek origin and means "interdependence". The known, i.e. the start position – the aggregate database, the methods of funds transfer, the search for answers of the questions concerning the correspondents banks system, the assigned final aims, i.e. mobilisation of these funds – is put into interdependence with something new or is used in a new manner, is included into a system with outer subjects, indifferent to the system, for the achievement of some other effects.

In case of unsuccessful tries for solving a particular problem, the use of former experience is rejected and new ways and decisions are sought.

The module implementing this method includes:

Step No 1 – introducing and analysing the problem known to a team of experts;

Step No 2 – the problem is changed to unrecognizability through analogies and metaphors;

Step No 3 – searching and finding dependence between the found algorithms, metaphors and the original problem.

Delphi Method.

The ancient Greeks asked for an advice the oracle who lived in Delphi. They achieved their goals with a better success after they had been pronounced by the oracle as they considered such an act a will of gods.

The major aim of Delphi method is the possible determination of future development of a particular problem. In our case we mean techniques of utilisation of the correspondence relations between banks for money laundering.

For this purpose it is necessary to form a team of experts with a long-year experience in this field and well acquainted with the possibilities for use of banks for legalisation of criminal origin funds. The experts must have a long-year experience in this business and possess skills in influencing and convincing the others in the rectitude of their opinion with the best argumentation.

Experts of all major banking sectors – investment lending, payment agency, securities trading, portfolio investment consultants, security service, and internal control –

took part in the first stage. For example – discussion is carried out on the following problem – if the formation of new tax oasis is expected with possibilities of legalisation of funds of criminal origin. The inquiry at this stage shows the quite distant positions of the immediate participants, and the head organises the statements and motivation of each member of the team. The opinions with greatest deviation from the general opinion are assessed and sent to all the members so they are able to make more precise their own statements and to acquaint themselves with the statements of the other experts in the group. During the second stage the answers are brought to criticising and assessment and the third stage is prepared. During this stage all the results are again announced to the experts so they can compare their answers and further specify them. Thesis argumentation is again required for the opinions with great deviation.

The value of this method is determined by the competency of the invited experts, by their commitment and intensive occupation with the problems of money laundry prevention.

Delphi methods provides good results if the contents of the inquiry is structured in a way that encourages the experts to re-consider their own positions and if it is specified and made clear for the experts.

3. Conclusions

The application of methods based on information technologies and heuristic methods provides new possibilities of due diligence to bank customers. In regard to the sudden increase of the banking operations of trans border transfers of cash flows, a special attention is to be paid to the automation of monitoring of in-going and out-coming flows, as well as to the bank staff's capability of identifying suspicious clients and their operations nature and to prepare operating file records.

The leaders in the banking business, mentioned at the beginning of this presentation, have directed their efforts to develop their own programmes for training their employees investing in their preparation and mobility.

REFERENCES

Financial Action Task Force, Annual Report, Paris 2004 – 2005.

Framework for Internal Control Systems in Banking Organisations – BCBS, Basel, (1998) Risk Management Principles for Electronic Banking – BCBS, Basel, May 2003.

Ganchev, G. (2004*). Terrorism as a Strategic Game: Duel of Antagonistic Unobservable Financial Strategies*, Finance and Financial Policy No 4, p. 22-29.

Global Anti-Laundering Guidelines for Private Banking, Wolfsburg AML Principles.

Methorn, H.G. (1983). Evrica, Berlin, pp. 12-79.

Nikolov, Ch. (2004). Economic Measurements of Global Terrorism, Finance and Financial Policy No 4, p. 30-36.

Organization", Eight International Scientific Conference "Investments In The Future – 2011", Varna.

Stanley, E. M., Electronic Money Laundering, (1998). Department of Justice, Canada.

Stavrova, E, (2005). Systems for prevent access of dirty money into the financial system, Blagoevgrad, 2005, PP 120.

Stavrova, E., Banking security net, (2009). Blagoevgrad, pp. 199.

Valkanov, N. (2007*). The International and Bulgarian Practice Fighting Money laundering*, Finance Journal, № 4, pp. 60-70.

Valkanov, N. (2007*). The International and Bulgarian Practice Fighting Money Laundering*, Finance Journal, № 4, pp. 60-70.

Valkanov, N. (2013). *Positioning of AML Compliance activities in the Architecture of Modern Banking Organizations,* Varna, 2013.

Valkanov, N. (2011). *AML Risk-based matrix in Contemporary Banking.*

Tsenkov, Vl. (2015). Crisis influences between developed and developing capital market – the case of Central and Eastern European countries, *Economic Studies*, № 3, 46-71.