According to Article 5, item (2) Law on prevention of money laundering and terrorism financing (Official Gazette of BiH, No. 53/09) Articles 4, 9, and 25 of the Law on the Banking Agency of Federation of Bosnia and Herzegovina ("Official Gazette of the Federation of BiH", Number 9/96, 27/98, 20/00, 45/00, 58/02, 13/03, 19/03, 28/03, 47/06, 59/06, 48/08 and 34/12) and Article 47 of the Law on banks ("Official Gazette of the Federation of BiH", Number 39/98, 32/00, 48/01, 41/02, 58/02, 13/03, 19/03 and 28/03), the Management Board of the Banking Agency of the Federation of BiH, at the meeting on 15.05.2012., declares

DECISION
ON MINIMUM STANDARDS FOR BANK'S ACTIVITIES IN PREVENTION OF MONEY LAUNDERING AND TERRORISM FINANCING

I – INTRODUCTORY PROVISIONS

Article 1

This Decision prescribes in more details minimum scope, form and content of activities of banks on prevention of money laundering and terrorism financing.

Article 2

1) Banks are required to have a written Program of implementation of activities stated in Article 1 of this Decision, that is the Program for prevention of risk of money laundering and terrorism financing, as well as for implementation of adequate internal controls that will ensure that the Program, policies and procedures are fully implemented in practice.

2) The money laundering and/or terrorism financing risk presents a possibility that the client misuses the bank for money laundering and terrorism financing and that a business relation, transaction or product are directly or indirectly used for money laundering and/or terrorism financing activities.

3) Banks, including their head office and all of their branches and other organizational units located in the country and in abroad, are required to fully implement provisions stated in the Program, as well as all policies and procedures. Banks are required to pay special attention to activities of their branches and other organizational units located abroad.

4) Implementing the provisions form the paragraph 3 of this Article the banks are required to ensure that high ethical and professional standards exist with their employees and to provide for efficient prevention of any possibilities for the bank to be, consciously or unconsciously, misused by any criminal elements, which includes prevention, detection and reporting of authorities on criminal actions and frauds, that is reporting the suspicious information and activities.

Article 3

1) It is required that the Program mentioned in the Article 2 of this Decision includes the following policies:

   1. policy on customer suitability;
   2. policy on customer identification;
   3. policy on permanent monitoring of accounts and transactions; and
   4. policy on managing the risk of money laundering and terrorism financing.

2) The policies and procedures for the implementation of policies must be based on the evaluation of the risk from the money laundering and terrorism financing activities and implementation of the principle 'know your customer'.

Article 4

1) Banks are required not only to determine the identity of their customers, but also to constantly monitor their account activities and to verify and determine whether transactions are performed in a normal and expected manner taking into account the nature of the account.
2) "Know Your Customer" principle should be a central element of the procedures for managing the risk and for performing adequate controls, but it is necessary to amend the same with regular internal reviews and internal audit of compliance of bank's operations with requirements stated in the law and other regulations which define the standards for prevention of money laundering and terrorism financing activities.

II CLIENT ACCEPTANCE POLICY

Article 5

(1) Based on the client acceptance policy, the bank is required to establish a clear policy on the issues like which and what kind of customers are suitable for the bank, as well as to prescribe overall procedures for implementation of this policy. This policy needs to especially encompass a description of benchmarks for specific risk categories which the customers and products or services can bear and based on which the risk evaluation will be performed, in other words it is necessary to define the categories of risk. Those categories are: low, moderate and high risk.
(2) Procedures for implementation of this policy would be adjusted to a requirement that customers need to be reviewed and rated based on the level of risk the customer represents in a way to have the clients with moderate risk have a standard identification and monitoring procedure and customers with the low risk level be subject to the simplified identification procedure.

Determining client acceptance

Article 6.

In the client acceptance policy the banks are obliged to define factors based on which they determine the acceptance of a client, taking into account the geographic risk factors, risk

factors which refer to the client, as well as risk factors which refer to products and services which are offered to the clients. In this policy the banks are obliged to, at a minimum, include following risk factors:

1. Country of origin for the client, country of origin of the majority owner, which is the real owner of the client, country of origin of the client, country of origin of the majority owner or the real owner of the client, whether or not the country is on the list of the non-cooperative states and territories issued by the international body for control and prevention of money laundering, on the list of countries listed as off-shore zone or non-cooperative countries which are developed and updated by the Financial Intelligence unit of the State Agency for investigations and protection (henceforth: FOO) or on the list of countries which the bank considers risky based on its own assessment;
2. The country of origin of the individual which performs transactions with the client, independently where the country is on the lists from the item a) of this Article;
3. Client, majority owner or the real owner of the client, individual which performs the transactions – against which issued are measures in order to establish international peace and security in compliance with the resolutions of the Security Council of the United Nation and Council of Europe;
4. Unknown or unclear source of funds of the client, that is the funds which source the client cannot prove;
5. Cases when there is a doubt that the client is not acting for its account, or it is acting according to orders or instructions of a third entity;
6. Uncommon flow of transactions, especially when you take into account its base, amount and execution manner, purpose of opening the account, as well as the activity of the client – if the client is an individual which performs a business activity;
7. Cases when there is a doubt that the transactions which the client is performing can be connected with the money laundering and terrorism financing activities;
8. The client is a politically exposed individual;
9. Accounts of other individuals related to the client;
10. Specifics of the operations which the client performs.

Article 7.

(1) The banks determine the acceptance of the client, depending on the risk factor, in the following manner:
    1. Perform client classification with a description of those types of clients which could be risky clients for the bank and determine the types of products which they can offer to individual client categories;
    2. More closely determine the condition under which they will establish the contract conditions or the business cooperation with the client and reasons for cancelling the existing contracted relation.

(2) In order to determine the client acceptance, the banks are obliged to prescribe:
    1. The procedure for determining the risk factors in relation to the new clients;
    2. Procedure for determining risk factors while in existence are business relations with the client;
    3. Manner of treating different clients.

(3) The banks will not establish business relations nor cooperate with banks or other institutions which are registered in the countries in which they do not perform their operations nor are a part of the financial group, and they will be under the supervision in

order to detect and prevent the money laundering and terrorism financing activities (banks shells).

Determining the risk of the products and services

Article 8.

(1) The banks determine the risk product and services in order to evaluate its products and services and determine the risk which they carry taken the possibility of being misused for money laundering and terrorism financing activities.
(2) The part of this Decision is also the Attachment about the guidelines for risk evaluation.

III CUSTOMER IDENTIFICATION POLICY

Article 9.

In the sense of this Decision, bank customers are:

1. individuals and legal entities opening or have opened accounts with banks;
2. individuals and legal entities in whose name and in whose behalf bank accounts are being opened or are opened, that is end user/holder of account;
3. individuals and legal entities intending or performing financial transactions through the bank;
4. individuals and legal entities performing transactions through different kinds of intermediaries; and
5. any individual and legal entity that is related to the financial transaction that can expose the bank to the reputation risk or to some other type of risk.

1. Customer identification

Article 10.

(1) the banks are obliged to determine detailed and comprehensive procedure for identification of new clients. These procedures will depend on the risk categories to which the clients belong and products and services which the clients will use. Depending on these categories the bank will apply proportional measures for client identification. These identification measures can be: simplified, enhanced or standard.
(2) The identification process is implemented at the beginning of the establishment of the business relation. However, in order to secure that the documents are still valid and relevant, the banks are obliged to implement regular reviews of already existing documents. At the same time the banks are obliged to implement such reviews in all the cases when significant transactions are being performed, when significant changes appear in the manner in which the client uses the account for transactions, and when the bank significantly changes the standards for documenting the identity or the transaction of the client.
(3) In establishing the business relation with the new clients, as in the cases form the paragraph (2) of this Article, the banks are obliged to perform verification of the client's identity using reliable, independent sources of documentation, data and information (identification data). The client identity verification must be finalized before the establishment of the business relation, or during the banking day in which the business relation is being established. Exclusively, the verification can be performed after the establishment of the business relation, but in the case a transaction

is to be performed, the verification will have to take place before the transaction is complete, or approval of the account of the user or payment of funds in the case of the random transactions which present the inflows (accepting money or loro payments). If the business relation is established without a performed verification, than in the case of the transactions which present outflow (sending money or nostro payments) the verification must be done before the transaction is initiated.

(4) In the cases when the verification cannot be performed within the deadlines in the paragraph (3) of this Article the initiated business relation is terminated and the authorized body is informed about that.

Article 11.

(1) The documents from which the bank determine the identity of the client and based on which it performs the verification of the client's identity in general should be of such nature that they are hard to obtain in an illegal manner or falsified, as well as the document prescribed by other appropriate regulation. Special attention the banks should give to the nonresident clients and they should not restrict or incompletely implement the procedures for determining the identity in the cases when the new client is not capable to present himself at the interview.

(2) When the client is a nonresident the bank should always ask the question to itself and the client: why did that client choose a bank in a foreign country to open an account.

(3) In the cases when the bank learn that they do not have enough documentation about an existing client they are obliged to take urgent measures in order to collect such information in a fastest manner possible, and until they get them they cannot perform market transactions, or they are obliged to perform the verification of the changed identification data.

(4) The banks are obliged to prescribe for the client identification and each individual product standards about the type of documentation needed and time period for maintaining the documentation, and at least in compliance with the appropriate regulations for safekeeping of the documents.

(5) The banks cannot open an account nor perform operations with a client which insists on his anonymity or who in identification uses a false name, present incorrect identification data and falsified documentation. In such cases the banks can refuse the opening of the account, or the establishment of the business relation with the clients without an obligation to give explanation. In these cases it is necessary to develop a note about the business contact with the client and about that inform FOO.

(6) In the cases of inactive accounts the banks are obliged to be especially prudent in the case they become suddenly active, especially if their activation is through transactions of significant amounts or show some of the indicators of the suspicious activities. In such cases, apart from other, it is necessary that the banks perform a repeated review of the client identity.

(7) In all cases the banks are obliged to perform a review of the documentation as well as checking if the client really exists, if he is at the registered address, does it really perform listed business activities.

Simplified identification and monitoring measures

Article 12.

(1) The bank can apply simplified identification when establishing a business relation with the following clients:
    1. Management bodies;
    2. Institutions with public authorities;
    3. Financial and other institutions which are by law obliged to implement measures in prevention of money laundering and terrorism financing activities, with the head office in Bosnia and Herzegovina or a country which accepted international standards for prevention of money laundering and terrorism financing activities, and which are identical or more strict than those implemented in Bosnia and Herzegovina;
    4. Companies which shares can be traded on the regulated capital markets and
    5. Other clients who are assigned in the category of law risk level.

1. Government bodies and institutions, independent of the level of the organization state structure (state, entities, district, cantons, municipalities),
2. Public companies and institutions which founders are state bodies and institutions form the Item 1. of this Article,
3. Parties obliged to implement measures on prevention of money laundering and terrorism financing activities, which are supervised in accordance with the implementation of the legal and other regulations in reference to the prevention of money laundering and terrorism financing activities by bodies and agencies which are organized in compliance with the laws,
4. other clients, legal entities and individuals for which the bank, based on the analyses determines that have a low risk of money laundering and terrorism financing activities, such as individual who open accounts which serve for paying the regular monthly payments (salaries, pensions, etc.) as well as saving accounts.

Article 13.

Low level of risk from money laundering and terrorism financing activities can be carried by clients which come from the countries members of the European Union or other countries which, according to the data of the Financial intelligence department, fulfill the internationally accepted standards for prevention of money laundering and terrorism financing activities.

Article 14.

(1) The banks, as a part of the simplified client identification and monitoring, is obliged to gather following data and information about the client:
    1. Name, address and the head office of the legal entity, that is name, surname and address of the individual which is establishing the business relation;
    2. Name and surname of the legal representative or authorized individual which is establishing the business relation for the legal entity;
    3. Purpose and intention for the business relation and source of funds;
    4. Date for establishing the business relation and
    5. Other in compliance with the appropriate regulations.

(1) The bank is obliged to secure verification of the gathered data and information about the client by reviewing the documents in which the gathered data are recorded and information about the client such as: personal identification document, certifications from appropriate registers, documents on which the client or the authorized individual deposited his signature and other in compliance with the risk analyses performed by the bank.

Standard identification measures

Article 15.

The bank will assign into moderate risk category those clients, business relations, products or services which based on the analyses and risk evaluation cannot be defined as high or low risk.

Article 16.

(1) Within the standard identification measures the banks are obliged to collect following data and information about clients:
   1. individuals:
      a) name and surname;
      b) date and place of birth;
      c) unified citizen identification number or the number of the identification card;
      d) home address;
      e) title and location of the employer where the individual is employed;
      f) description of other sources of funds and other data based on bank's evaluation.
   2. Legal entities
      a) title and head office of the client;
      b) title and head office of the founder and real owners of the client;
      c) number and the date of the license (special consent), if a special law prescribes an obligation to obtain a consent for performing client's operations;
      d) identification data about the individuals authorized to represent and present, as well as individuals authorized to dispose with the funds on the client's accounts;
      e) identification numbers received from the tax and other authorities and institutions to which the client, in accordance with the law, is performing his operations;
      f) data about the business and financial solvency and other data based on the bank's assessment.

(2) Confirmation, that is the verification of the collected data and information about the client the bank is obliged to provide through reviewing and gathering documentation in which written are data and information about the client:
   1. For the individuals:
      a) Personal identification documents (personal ID, driver's license, passport or other identification document from which it can be without doubt and with certainty determine the identity);
      b) Confirmation of the living location (CIPS registration or other document from which the living arrangement can be confirmed);
      c) Confirmation and/or certificate of employment issued by the employer;
      d) Possibly the documents about other sources of funds (rental contract etc.);
      e) Copy of the signature of the client and the document on which the client deposited its signature and other documentation in compliance with the bank's evaluations;
      f) Documents created by the bank – analyses of the financial capability of the client.
   2. For the legal entities:
      a) Certification from an appropriate register as an evidence of a legal status;

b) Document of establishment (Decision or a Contract);
c) Identification documents of the founders and real owners if they are physical individuals, or the certificates from appropriate registers if they are a legal entity;
d) License for operations if it is needed for the operations which the client is performing;
e) Personal identification documents and copy of the signature of the individuals authorized to present and represent, as well as individuals authorized to dispose with the funds on the accounts of clients;
f) Confirmation and other documentation from the bodies and institutions needed to perform the operations;
g) financial reports about the performance and other documentation in compliance with the bank's evaluations.

(3) Documentation submitted by the client and the documentation that the bank obtained itself, the bank is obliged to maintain in the original or a photocopy, if it is not allowed to keep the original document.

(4) The bank's are obliged to, in addition to the client, perform identification and verification of the individuals which are acting in the name and account of the client.

Enhanced identification measures

Article 17.

(1) Enhanced measures of identification the bank will implement in the cases when the business relation is established with:
1. banks or similar credit institutions with the head office abroad;
2. politically exposed individuals and
3. clients who are not present in person during the establishment of the business relation, or the implementation of the identification measures.

(2) Enhanced identification and monitoring measures the banks will implement in other cases when through the review of risk they determine that it is a question of a client who for the bank carries a high level of risk from money laundering and terrorism financing.

1.1. Business relations with banks or similar credit institutions with a head office abroad (Correspondent banking relations)

Article 18.

1) When the operations of the international payment system are performed through a network of other banks or similar credit institutions with a head office abroad, with which the bank has some relations (correspondent relations), and when the bank is performing these operations in the country for banks or similar credit institutions, it is obliged to implement enhanced measures for identification and monitoring of the business relation in order to avoid situations where it is exposed to risks of holding the money and/or transfers of money which is tied to money laundering and terrorism financing activities .
2) In regard to the paragraph 1 of this Article, the banks are required to gather all necessary information on their correspondent banks in order to have a full knowledge of the nature of operations of their correspondent banks. Necessary factors and information are:
   1. location (country) of correspondent bank;
   2. management of correspondent bank;

3. major business activities of correspondent bank;
4. efforts of correspondent bank in area of prevention of money laundering and prevention of terrorist financing, as well as adequate customer acceptance policies and know your customer policies;
5. purpose, that is the reason for account opening;
6. identity of third party to be using the correspondent banking services;
7. condition of bank regulations and supervision function in the correspondent bank's country, etc.

(1) Banks are allowed to establish correspondent relationships only with those banks that are located in countries where authorized institutions perform efficient bank supervision. The bank is not allowed to establish a business relation with a "bank shell" and should develop procedures which will ensure that and which will disable the establishment of a business relation with banks which are famous in allowing that their accounts are used by "banks shells".
(2) Banks are required to prevent the risk of correspondent accounts being used, directly or indirectly, by third parties to perform activities on their own behalf.
(3) Special attention the banks are obliged to devote to the payable-through accounts, which they have for foreign banks, in order to avoid the possibility of direct access of the clients of these banks (sub holders of accounts) to those accounts with an aim to perform transactions such as issuing checks, withdrawing and payments of cash etc., and that these clients were not subject of their identification procedures and monitoring during opening the accounts, that is establishment of this type of business relation, where the bank at the request, of the bank the holder of the account, must provide relevant data about the executed identification and monitoring of the sub-accounts.

Politically exposed individuals

Article 19.

(1) When establishing a business relation or performing transactions, in the cases when establishing is not a longer business relation, the banks are obliged to define adequate procedures, in order to determine if the client is a politically exposed individual.
(2) Politically exposed individuals, are individuals who are assigned exposed public functions of a high rank in the country and abroad, including the members of the closer family and close colleagues. Individuals who were assigned these duties and who terminated them less than a year ago are also considered politically exposed individuals. Individuals on the functions of a middle or lower rank are not considered as politically exposed individuals.
(3) The procedures will allow the banks to directly from the clients and/or publically accessible registers and data bases gather data and information about the client's political exposing. In regard to that the banks are obliged to:
   1) Have adequate procedures based on risk in order to determine whether the client is a politically exposed individual;
   2) Have an approval from the management to establish business relations with such clients;

3) Take adequate measures in order to determine the source of funds which is included in the business relation or transaction;
4) Implement an enhanced monitoring of the business relation.

(4) The same measures of identification and monitoring the banks are obliged to implement in the cases when the founders, real owners and the individuals authorized to represent the legal entity are politically exposed individuals.

Establishing a business relation without a physical presence by the client

Article 20.

(1) When the banks establish business relations with the clients which are not physically present they are obliged to apply enhanced measures of identification, in order to decrease and manage with good quality the risk which can be present in the performance with the clients. These measures can include:
   1. Requesting additional documents which are not requested from other clients;
   2. Verification of the submitted documents;
   3. Independent contacting the clients by the bank;
   4. Engaging specialized firms for control and evaluation of the clients with an aim to additionally test the clients;
   5. Requesting that the first payment (installment) is performed over the account in the name of the client in some other bank which has an obligation to implement similar standards for control and evaluation of the client.

(2) If the bank does not implement the enhanced measures of the identification it will not establish a business relation with the client which is not physically present during the establishment of the business relation.

2. Special identification issues

Preventing the misuse of the technological development

Article 21.

(1) The banks are obliged to adopt policies and procedures and take measures which are needed for preventing the misuse of the technological development for the purpose of money laundering and terrorism financing activities.

(2) In these policies and procedures the banks are obliged to define specific risks which refer to establishing a business relation for performing transaction electronically, over Internet or other interactive computer system, over telephone, using ATM, using electronic cards which are tied to the accounts of the clients (debit and credit) for payments and withdrawals of cash.

(3) Within management of these risks the bank is obliged to:
   1. In establishing the business relation with the client applies identification measures from the Article 17 of this Decision;
   2. Provide that the inter-banking electronic transfers (SWIFT etc.) and transfers performed by the clients from special terminals through free telecommunication lines (POS banking, electronic and internet banking), as well as for other transfers

listed in the paragraph (2) of this Article, through the complete transfer flow monitor the identification data about the party ordering the transaction and party receiving the transaction as well as the purpose of the transfer;

3. Establishment, regular reviews and testing of the security measures and control process and system;
4. Secure that the verification of the client includes combinations of at least two manners for client identity confirmation;
5. Application of a secure and efficient measure for verification and confirmation of identity and client's authority;

(4) When performing these transfers the bank is obliged to provide respect of all these obligations for the local as well as for the international transfers.

(5) In the cases when the bank cannot secure needed identification data and information about the clients it will refuse to provide these types of banking services.

Third party

Article 22.

(1) In fulfilling the requirements of the identification and verification of the client's identity the banks can rely on a third party, but the final responsibility for implementing the conditions is with the banks which rely on the third party. The banks are obliged to provide the needed identification data and information about the client. The banks must fulfill the conditions such as that the copy of the documentation with the identification data and information based on which the third party performed the verification of the client's identity is available at the bank's request, without delay.

(2) The third party, in this sense, presents all the parties in implementing the measures of the prevention of money laundering and terrorism financing activities defined by the Law on prevention of money laundering and terrorism financing activities which are regulated and supervised by special regulatory bodies. Third party can be an equivalent institution form a foreign country, for which the bank must provide evidence that it meets the defined conditions, and it can use the international institutions reports with authorities in prevention of money laundering and terrorism financing activities (Financial Action Task Force-FATF, Moneyval committee, Council of Europe, World Bank; International Monetary Fund etc.).

(3) The third party is not presented by the institutions with which the bank concluded a contract for performing certain activities (outsourcing-externalization), nor in the cases when those institutions do meet the third party criteria. In these cases it is considered that the bank performed alone the identification and verification of the client's identity.

Vaults – safe-keeping

Article 23

In activities related to the vault, that is safe keeping of certain items, envelopes or packages, banks are required to establish special procedures to adequately identify individuals and/or companies that are not their customers and that do not have accounts opened with them. An important element of these procedures is providing for the identification of the true owner of items in the vault

Custodian accounts and „private banking"

Article 24.

(1) Since the custodian accounts can be used for avoiding or evading the banks procedures for client's identification, the banks must establish such procedures so that they can efficiently determine the real owner or owner of the account. In that they are obliged to look for and obtain evidence about the identity of each agent, custodian and representation employee, but also the individuals which they present or the real user or user of the account.
(2) The banks are obliged to be especially prudent in preventing the business firms (with a special purpose), especially business companies, which the individuals use as a method for work of anonymous accounts. Since the identification of such clients or final owners is extremely difficult, the banks are obliged to with special attention understand and discover the structure of the organization of such a company, in order to determine which the real sources of funds are and to identify the final users and owners or individuals which have a real control over funds.
(3) When the bank discovers or has reasons to believe that the account opened by the professional agent on behalf of the client it is obliged to perform the identification of such client. In the cases when the professional agent opens accounts for more clients, whether they are not open or when they are sub –accounts of the sum of the accounts, the banks are obliged to determine identity of all individual clients.
(4) In the cases which follow the banks are obliged to reject the request for opening an account:
    1. When the agent is not authorized to provide to the bank needed information about the real owners of the funds, for example lawyers restricted with the code of professional secret; and
    2. When the agent is not subject to the standards of examination and evaluation which are equivalent to the standards set in this Decision.

IV POLICY ON CONTINUOUS MONITORING OF ACCOUNTS AND TRANSACTIONS

Principle "Know Your Customer" and Development of the Customer Profile

Article 25.

1. In every day operations and relations with customers, bank must find out and get to know their customers' activities, to thoroughly understand their operations, to know their financial and payment habits, important information and documentation on customers' business relations and cash flows, types of business relations that customers maintain and to know their business contacts, their local and international market practices, common sources of debits and credits within their accounts, use of various currency, frequency and size, that is scope of transactions, etc. Banks are especially required to:
    1) in the case of business companies to get to know the ownership structure of the company, authorized decision makers and all other persons who are legitimately authorized to act in their behalf;
    2) request from its customers to submit information in advance and in timely fashion and to document any expected and intended changes in form of and in way of performing its business activities;
    3) pay special attention to well known customers and publicly known persons and to ensure that their possible illegal or suspicious operations do not jeopardize bank reputation.
2. Based on the elements from the previous paragraph, banks are required to develop a

profile of its customers. This profile will be included in the special registry of all customer profiles, as organized by banks themselves. The customer profile developed by the bank will be used as general additional indicator in the process of monitoring operations with customers and is also used for determining:

1. orderly, continuous and easy way of conducting operations and relations between the bank and the customer; and
2. unusual behavior and differences in customer's behavior already determined in the profile or in account turnover with an aim to initiate adequate procedures.

Irregular and Uncommon Behavior Giving Basis for Suspicion

Article 26.

(1) The banks are obliged to pay special attention to complex, irregular or uncommon forms of transactions which do not have clearly visible economic or legal purpose.

(2) Banks are required to ask their customers to explain every significant change in behavior. In the case that customers cannot provide or gives a poor founded explanation, banks should find such behavior suspicious and should initiate procedures for a detailed review, including sending reports about the client's suspicious activity to the authorities (Financial Intelligence unit).

(3) Irregular and uncommon behaviors giving the basis for suspicion are:

1. unexpected change in financial behavior of the customer that cannot be explained with business or financial motives;
2. unexpected new persons, businesses and/or geographical areas introduced by the customer, that do not fall into already known way and type of operations, business and financial network of the customer;
3. special characteristics of certain transactions that do not fit into the regular practice of the customer;
4. use of funds from customer's account for irregular and that are not included the bank-customer arrangement;
5. explanation of transactions given by customers is poor and seems to be false;
6. frequent transactions in amounts below the amount required to be reported by the law to authorized institutions;
7. when a customer closes the account by taking the entire account balance in cash or dividing that amount to several smaller amounts and distributing them to several newly opened accounts;
8. when bank employees do not have clear evidence of criminal activities, but suspect that possibility.

(4) This Decision also includes an Attachment stating indicators of suspicious financial transactions.

1. Monitoring for Purposes of Prevention of Money Laundering

Article 27.

1) Banks are required to perform an on-going monitoring of accounts and transactions as a basic aspect of efficient "Know Your Customer" procedures. For this reason, banks are required to previously receive and define responses to one of the most important questions of what is the nature of normal and reasonable or normal or regular activities within their customer accounts. When they accomplish that, banks are required to

provide for means or instruments, methods or procedures for detection of transactions that do not fit into such nature of customers' behavior and are also required to use these procedures to efficiently control and minimize the risk in operations with customers.

2) Scope of bank's work on monitoring activities on customer's accounts must be adjusted to needs for adequate risk sensitivity. For all of its accounts, banks are required to establish a system that would enable them to detect all unusual, irregular and suspicious types of activities.

Article 28.

In order to ensure fulfillment of goals stated in the Article 27, banks are required to:

1. establish limitations to certain types or categories of account transactions;
2. pay special attention to and verify all account transactions that exceed the established limitations;
3. define types of transactions that will alert the banks to a possibility of customers performing some unusual, irregular or suspicious transactions;
4. define types of transactions that, by their nature, mainly don't have economic or commercial purpose;
5. define benchmarks and/or nature of amounts of cash deposits that are inconsistent with normal or expected transactions performed by certain types of customers;
6. define bank actions in cases of large turnover on accounts where account balances are usually not too high;
7. develop official and comprehensive list of examples of suspicious transactions and examples and methods of possible money laundering and terrorism financing cases;
8. establish adequate information system which will allow creation of the bookkeeping and documentation and records off the books with all the data which in a satisfactory manner describe the occurred event which will a sufficient tool to perform the analyses and monitoring of the turnover on the account, or all clients business activities.

Article 29.

As for accounts that represent higher level of risk, banks are required to establish a more intensive monitoring process. In order to identify the categories of accounts with higher level of risk, it is necessary for the banks to establish a package of key indicators based on which accounts will be categorized in groups, taking into account background information and other information of the customer such as sources of funds for the account, type and nature of transactions themselves, customer's home country, etc. For the accounts with higher risk level, banks are required to:

1. create an adequate system for information management that will assure that bank's management and officers authorized to monitor compliance of bank's performance with the requirements prescribed by the Law and regulations for this area have timely information necessary for identification, effective monitoring of customers' accounts with higher level of risk and their analysis. As minimum, this system has to include the following:
    a) reporting about the documentation that is missing in order to have a full and safe customer identification;
    b) reporting about strange, unusual and suspicious transactions performed through customers' accounts; and

c) reporting about overall information regarding all customers' business relationships with bank.

2. make sure that the management responsible for bank's performance in the area of private banking has good knowledge of the situation of bank's customer that represents higher level of risk, to be alert and to evaluate the information that can be received from some third party. Significant transactions of those customers should be approved from the management.
3. adopt a clear policy, internal guidelines and procedures and to establish control with special task to control prudential performance in relation to a politically exposed individuals, other individuals and companies where it is confirmed or it is clear that they are connected to them.

Monitoring for Purposes of Prevention of Terrorism Financing

Article 30.

(1) Reporting to an authorized institution and blockade of financial assets where bank has suspicion or knows that they are used to finance terrorism or individuals who support terrorism represents the main precondition to fight against terrorism. The most attention, banks have to pay to the following:
   1. to the extent possible, check whether the funds coming from legitimate sources or businesses are, fully or partially, directed to support terrorist financing;
   2. implementation of procedures for prevention of financing terrorists and terrorist organizations, and entities related to them;
   3. attempts to discover a true identity and/or purpose of small transfers when purpose of the transfer and/or sender and/or recipient is precisely stated;
   4. cases where customer's order unexpectedly results in zero balance;
   5. the same like in the cases of money laundering where money is received and sent electronically, along with strange or unusual aspects, such as size of the amount, country where the money is sent, home country of the ordered, type of currency, etc.
   6. non-profit and humanitarian organizations, especially if the activities are not in accordance with the registered activity; if the source of funds is not clear; if organizations receive funds from strange and suspicious sources.

(2) Monitoring the accounts and the transactions of the clients the bank must determine if its clients, or the individuals making the orders or receiving the orders in the transactions performed without an established special business relation (opening of an account) individuals which are on the lists of individuals under suspicion of money laundering and terrorism financing activities due to the suspicion that they finance terrorism or due to a suspicion that they are related to those individuals, which are created by relevant institutions (international: Security Council of the United Nation, appropriate bodies of the European Council and local: Security Ministry and FOO).

(3) In the cases when the individuals from the paragraph (2) of this Article attempt to establish a business relation with a bank or with the existing bank clients (existing accounts), the bank is obliged to, in compliance with the provisions of the Law on prevention of money laundering and terrorism financing activities inform FOO and temporarily freeze the assets of such individual.

V. POLICY ON MONEY LAUNDERING AND TERRORISM FINANCING RISK MANAGEMENT

Article 31.

Policy on money laundering and terrorism financing risk management (henceforth: Policy on risk management), the banks are obliged to define the responsibility of the bank's bodies, development and thorough implementation of clear and precise procedures for reporting to adequate internal bodies as well as the authorized institutions in compliance with the law and regulations about all legal regulations and suspicious transactions of the clients and the obligation to appoint the individual for coordination of the activities of the bank on prevention of money laundering and terrorism financing activities.

Responsibility of Bank's Bodies and Reporting

Article 32.

(1) With the Policy on risk management the banks are obliged to define the choice of the bank's bodies (management board and the bank's management) towards a high corporate management in their banks. This choice promotes a high level of compliance with international standards, as well as with national laws and regulations and it is necessary for obtaining compliance of their performance with the prescribed standards in prevention of money laundering and terrorism financing activities. This supposes that the bank's bodies promote the integrity of the individual appointed for the coordination of the activities on prevention of money laundering and terrorism financing activities and in general a high level of standards for the corporate management in the communication with the bank employees and corporate participants, all with an aim to establish a good quality management of risks which can derive from the money laundering and terrorism financing activities.
(2) Bank's Supervisory Board is responsible to adopt an effective Program and to ensure that banks are implementing adequate control procedures that will provide for program, policies and procedures, as well as their composite part, to be fully implemented in practice.
(3) Bank's policies and procedures should be effective and should include regular procedures for adequate and successful supervision by management board, internal control system, internal audit, delegation of duties, training of adequate employees and other segments that are in close connection with this area.
(4) In order to implement bank's policies and procedures, bank's Program has to clearly define responsibilities and delegation to adequate carriers, that is, delegation to adequate organizational units or functions, management board, other management and other employees of bank.

Article 33.

Line of reporting about strange, unusual and suspicious transactions of customers that are prescribed in the law must be clearly defined in written form. This reporting in practice has to be regular, effective and available to all parts of the bank and individuals, and fully in accordance with internally prescribed reporting policies and procedures.

Article 34.

1) Along with the requirement from the Article 33 of this Decision, banks are required to adopt internal procedures for reporting to the authorized bodies outside of bank, which is in accordance with applicable laws and regulations, all prescribed information and data.
2) Banks are required to fully perform their reporting requirements according to the law of the prescribed institution.

Article 35.

Banks are required to keep the documentation for all transactions performed by customers and in relationship with the customers, sorted by type, way they were performed and deadline prescribed by applicable law.

Appointment of Activities Coordinators

Article 36.

(1) Bank's Supervisory Board is required to ensure that banks in their management appoint persons who will have responsibility for coordination of all activities of the bank in monitoring compliance with all laws and other prescribed requirements subject to this Decision and effective implementation of the Program.
(2) Coordinator for bank's compliance with prescribed requirements for anti-money laundering activities and terrorism financing (the Coordinator) should:

1. be responsible for regular functioning of reporting function towards the authorized institutions, prescribed laws and other regulations, all transactions over the prescribed amount, all related and suspicious transactions;
2. be responsible for regular functioning of lines of reporting in accordance with the Program;
3. have required qualification, knowledge, experience and good working and moral reputation;
4. have necessary funds to perform its functions including at least two officers, where one of the is responsible for monitoring the process of detection of suspicious customers and the other is responsible for monitoring the line of reporting of authorities and internal lines of reporting, and they also have authorizations for making independent decisions and seeking legal support. With larger banks, it is necessary to estimate the need for several such officers;
5. on day-to-day basis, have full access to the customer monitoring system;
6. receive daily reports on suspicious activities of customers;
7. have authority to issue an order for implementation of procedures stated in the law, regulations and the Program, and inform the management and supervisory board of the bank on the same;
8. have ability to monitor local procedures and procedures on relations with abroad in order to confirm certain suspicions;
9. undertake certain steps to improve its knowledge and skills, as well as the knowledge and skills of his subordinates and of other relevant bank staff;
10. at least once every quarter, submit report to the supervisory board and management of the bank on bank's actions and bank's compliance with the Law on Prevention of Money Laundering and Terrorist Financing, as well as on actions taken against certain suspicious customers;

11. at least once a year, perform a review of adequacy of the existing Program, policies and procedures and provide supervisory board with recommendations to update or improve the same;
12. if necessary, provide full support to activities performed by the bank's internal auditor;
13. in his procedures, include elements related to internal investigation of liability of bank staff who neglected their duties in this area;

Internal and external bank audit

Article 37.

1) Internal auditors in banks are required to perform regular controls and to ensure that the program, policies and procedures for prevention of money laundering and terrorism financing, that is "Know Your Customer" policies and procedures, are fully implemented and complied with all requirements stated the Law and other regulations.
2) Compliance of banks' operations with requirements stated in the Law and regulations should be a subject of independent review performed by the bank's internal auditors, which includes evaluation of adequacy of bank's policies and procedures from the aspect of legal requirements and other regulations.
3) A required function of internal audit in banks is to continuously monitor whether and how does bank staff perform and implement requirements stated in the program, policies and procedures, by using compliance tests if there is an adequate sample of customers, accounts and transactions, as well as to test the correctness of reporting of irregular, uncommon and suspicious transactions defined in the Law and other regulations.

Article 38.

Internal audit function in banks should represent a full independent evaluation of risk management and performance of internal control systems in banks. Internal audit is required to periodically report the Audit Board and/or Supervisory Board of the bank on its findings and evaluations based on the law. These reports should include findings and evaluations of efficiency of banks regarding all issues prescribed by the law and regulations, program, policies and procedures of the bank which regulate bank's responsibilities in prevention of money laundering and terrorism financing. One important part of these reports is evaluation of adequacy of bank staff training in this area.

Article 39.

(1) Bank's supervisory board is required to ensure that its internal audit function is technically equipped with such personnel who have thorough knowledge of the program, policies and procedures, as well as who possess high ethical and expert capabilities, especially in the "Know Your Customer" area.
(2) In addition to this, internal audit staff has to be fully proactive in monitoring activities that banks are required to perform on the basis of findings and evaluations done by the internal audit, external audit and enforcement bodies.

Article 40.

In the process of performing independent external audit of their financial statements, banks are required to arrange with independent external audit firms to also work on evaluation of

implementation of legal and regulatory requirements of banks, implementation of the program, policies and procedures, internal control systems and performance of internal audit in banks, as well as to evaluate whether bank's operations are in compliance with requirements related to prevention of money laundering and terrorism financing, by using testing technique.

Training of the bank's employees

Article 41.

(1) Banks are required to provide for continuous training of all its employees involved in their program of prevention of money laundering and terrorism financing activities. Content of this training should include, at the minimum, the following topics from the mentioned area which is the subject of this Decision:
   1) legal requirements of banks and responsibilities stated in other regulations;
   2) program, policies and procedures of the bank;
   3) detailed elements of "Know Your Customer" policy;
   4) exposure of banks to money laundering and risks to the bank and duties of bank staff;
   5) strengths and weaknesses of financial institutions in prevention of money laundering and terrorism financing;
   6) duties and authorities of the Coordinator;
   7) internal control system;
   8) internal audit system;
   9) Banks are required to adjust the frequency of training and training topics mentioned in the previous paragraph to realistic needs of their organizational units, functions and/or its staff, and for purposes of timely compliance with new requirements and for purposes of learning about new events, as well as for the purposes of maintaining the existing knowledge and experience of its staff, banks are required to establish a regular training program
   10) In deciding on training needs and on types and scope of training mentioned in the previous paragraph, banks are required to adjust their training focus depending on whether training is intended to a newly employed staff, to staff directly working with customers, staff working with new customers, staff ensuring that bank's operations is complied with requirements of the law and other regulations, other executives, management and/or supervisory board, etc.
   11) Through their training program, banks are required to ensure that all relevant staff fully understands the importance of and necessity for an efficient implementation of "Know Your Customer" policy and for such understanding to be a key of success in its implementation.

Article 42.

In order to improve technical skills and efficiency of all staff, banks are required to develop a comprehensive manual that would include the laws and regulations prescribing prevention of money laundering and terrorism financing. Bank program, including all policies and procedures, rules for staff performance, methods of detection of illegal and suspicious activities, duties and authorities of the Coordinator, descriptions of some notable misuses, employee training program and attachments to this Decision.

VI FINAL PROVISIONS

Article 43.

The leasing companies are obliged to comply their policies and procedures with this Decision within 90 day from the day this Decision came into effect.

Article 44.

The day this Decision comes into effect, the Decision on the minimum standards for banks' activities on prevention of money laundering and terrorism financing activities ("Official Gazette of the Federation of BiH", Number: 3/03, 18/04, 5/05 and 13/05) will cease to be effective .

Article 45.

This Decision comes into effect on the eighth day from the day it is issued in the Official gazette of the Federation of BiH.

Number: U.O.-40-11/12

PRESIDENT
of the
MANAGEMENT BOARD

Sarajevo, 15.05.2012.

Mr.sc. Haris Ihtijarević, M. Sc (Econ)

ATTACHMENTS
To the Decision on Minimum Standards for Banks' Activities on Prevention of Money Laundering and Terrorism Financing

1. INDICATORS OF SUSPICIOUS FINANCIAL TRANSACTIONS

In addition to the already known and worldwide common indicators of suspicious financial transactions, that were also stated in the Decision on Minimum Standards for Banks' Activities on Prevention of Money Laundering and Terrorism Financing (the Decision), this Attachment to the Decision gives an overview of specific indicators such as:

I GENERAL

a) Customer does not want correspondence sent to home address;
b) Customer appears to have accounts with several financial institutions in one area for no apparent reason;
c) Customer repeatedly uses one address, but frequently changes the names involved;
d) Customer uses a post office box or General Delivery address or other type of mail drop address, instead of a street address when this is not the norm for that area;
e) Customer starts conducting frequent cash transactions in large amounts when this has not been a normal activity for the customer in the past;
f) Customer makes cash transactions of consistently rounded-off large amounts (e.g., KM 20,000, KM 15,000, KM 9,900, KM 8,500, etc.);
g) Customer consistently makes cash transactions that are just under the reporting threshold amount (KM 30,000);
h) Customer conducts a transaction for an amount that is unusual compared to amounts of past transactions;
i) Customer asks the bank to hold or transfer large sums of money or other assets when this type of activity is unusual for the customer.

1. TRANSACTIONS INVOLVING ACCOUNTS

a) Opening accounts when the customer's address is outside the local service area;
b) Account with a large number of small cash deposits and a small number of large cash withdrawals;

c) Funds are being deposited into several accounts, consolidated into one and transferred outside the country;
d) Customer frequently uses many deposit locations outside of the home branch location;
e) Customer makes multiple transactions on the same day;
f) Activity far exceeds activity projected at the time of opening of the account;
g) Dormant account suddenly sees significant activity;
h) Unexplained transfers between the customer's company and accounts;
i) Multiple deposits are made to a customer's account by third parties.

2. TRANSACTIONS INVOLVING AREAS OUTSIDE OF BOSNIA HERZEGOVINA

a) Customer and other parties to the transaction have no apparent ties to BIH;
b) Transaction crosses many international lines;
c) Transaction involves a country where illicit drug production or exporting may be prevalent, or where there is no effective system for prevention of money-laundering and terrorism financing;
d) Transaction involves a country known for highly secretive banking and corporate law (e.g., British Virgin Islands, Cyprus, etc);
e) Transaction involves a country known or suspected to facilitate money laundering activities or to support terrorism (See up-dated FATF black list: www.fatf-gafi.org).

3. TRANSACTIONS RELATED TO OFFSHORE BUSINESS ACTIVITY

a) Accumulation of large balances, inconsistent with the known turnover of the customer's business, and subsequent transfers to overseas account(s);
b) Loans to or from offshore companies;
c) Unexplained electronic funds transfer by customer on an in-and-out basis.

II EXAMPLES OF INDUSTRY-SPECIFIC INDICATORS

1. PERSONAL TRANSACTIONS

a) Customer appears to have accounts with several financial institutions in one geographical area;
b) Customer makes one or more cash deposits to general account of foreign correspondent bank (i.e., flow-through account);
c) Customer runs large credit card balances;
d) Customer wishes to have credit and debit cards sent to international or domestic destinations other than his or her address;
e) Customer has numerous accounts and deposits cash into each of them with the total credits being a large amount;
f) Customer frequently makes automatic banking machine deposits (when service available by the bank) just below the reporting threshold (KM 30,000);
g) Third parties make cash payments or deposit checks to a customer's credit card.

2. CORPORATE AND BUSINESS TRANSACTIONS

a) Accounts are used to receive or distribute large sums, but show virtually no normal business-related activities, such as the payment of payrolls, invoices, etc;
b) Deposits to or withdrawals from a corporate account are primarily in cash rather than in the form of debit and credit normally associated with commercial operations;

c) Customer pays in cash or deposits cash to cover bank drafts, money transfers or other negotiable and marketable money instruments;
d) Customer makes a large volume of seemingly unrelated deposits to several accounts and frequently transfers a major portion of the balances to a single account at the same bank or elsewhere;
e) Customer consistently makes immediate large withdrawals from an account that has just received a large and unexpected credit from abroad;
f) Small, one-location business makes deposits on the same day at different branches across a broad geographic area that does not appear practical for the business;
g) There is a substantial increase in deposits of cash or negotiable instruments by a company offering professional advisory services, especially if the deposits are promptly transferred;
h) Customer wishes to have credit and debit cards sent to international or domestic destinations other than his or her place of business;
i) There is a marked increase in transaction volume on an account with significant changes in an account balance that is inconsistent with or not in keeping with normal business practices of the customer's account;
j) Unexplained transactions are repeated between personal and commercial accounts.

3. ELECTRONIC FUNDS TRANSFERS

a) Customer transfers large sums of money to overseas locations with instructions to the foreign entity for payment in cash;
b) Customer receives large sums of money from an overseas location via electronic funds transfer that includes instructions or payment in cash;
c) Customer transfers funds to another country without changing the form of currency;
d) Large incoming wire transfers from foreign jurisdictions are removed immediately by company principals;
e) Size of electronic transfers is out-of-keeping with normal business transactions for that customer;
f) Customer conducts transactions involving countries known as narcotic source countries or as trans-shipment points for narcotics, or that are known for highly secretive banking and corporate law practices;
g) Customer makes electronic funds transfers to free trade or off-shore zones that are not in line with the customer's business.

4. LOAN TRANSACTIONS

a) Customer suddenly repays a problem loan unexpectedly;
b) Loan transactions are entered into in situations where the customer has significant assets and the loan transaction does not make economic sense.

5. INSURANCE TRANSACTIONS

a) Customer conducts a transaction that results in a conspicuous increase in investment contributions;
b) Customer cancels investment or insurance soon after purchase;
c) The duration of the life insurance contract is less than three years;
d) Transaction involves use and payment of a performance bond resulting in a cross border payment.

6. SECURITIES TRANSACTIONS

a) Accounts that have been inactive suddenly experience large investments that are inconsistent with the normal investment practice of the customer or their financial ability;

b) Customer wishes to purchase a number of investments with money orders, traveler's checks, cashier's checks, bank drafts or other bank instruments, especially in amounts that are slightly less than KM 30,000, where the transaction is inconsistent with the normal investment practice of the customer or their financial ability;
c) Customer uses securities or brokerage firm as a place to hold funds that are not being used in trading of securities or futures for an extended period of time and such activity is inconsistent with the normal investment practice of the customer or their financial ability;
d) Customer makes large or unusual settlements of securities in cash;
e) Transfers of funds or securities between accounts not known to be related to the customer. Proposed transactions are to be funded by international wire payments, particularly if from countries where there is no effective anti money-laundering system.

2. GUIDELINES FOR THE RISK ANALYSES AND EVALUATION

During the analyses and the evaluation of the risk from money laundering and terrorism financing activities, the banks classify their clients and products (transactions, ors business relations) in the following categories:

1. low risk
2. moderate risk and
3. high risk.

Risk criteria
The most frequent risk criteria are:

1. client risk,
2. product risk (transactions, that is business relation) and
3. geographic risk (country risk),

Risk elements
The bank's methodology based on the analyses and the risk evaluation can take into account the risk elements which are specific for a particular party, business relation, product or transaction, and can influence the increase or the decrease of risk. The risk elements include:

1. **Purpose of the account or the business relation** – accounts opened for the purpose of performing regular user transactions of small value can carry a smaller risk than the account opened for performing large cash transactions by an till then unknown party.
2. **Amount of funds or volume of the transaction** – oddly large amount of funds or strangely large transactions in comparison to those which could realistically be expected from the client of a similar profile can indicate that a client which is otherwise not considered a client with a larger risk, should be treated as such.
3. **Regulation level** or some other supervision or regiment of management that the client is subject to – financial institution regulated by law in a country which has a satisfactory regiment in prevention of money laundering and terrorism financing activities carries a lower risk than a client which is not supervised or which is subject to only a minimum prescribed regulations.
4. **Duration of the business relation** – long term business relations which include contacts with clients can carry lower risk from money laundering.

5. **Knowing the country of the client,** including its laws, regulations and rules as well as the structure and the volume of the legal framework will have an impact on the risk evaluation.
6. **Requesting transaction from** the client which do not have a clear commercial or other justification or which without need increase the complexity of the transaction, or in other manner decrease the transparency without an acceptable explanation increases the risk.
7. **Data about individuals which the banks submitted to the Financial Intelligence Department** – in relation to that individual or his transactions there existed reasons for doubt in regard to the money laundering and terrorism financing activities, which increases the risk.

Client risk

In analyzing and evaluating the risk from money laundering and terrorism financing activities, the banks especially review the characteristics of the clients, depending whether the client is a:

1. bank;
2. post office;
3. investment funds management company, investment fund (no matter of the tip), agent on the securities market;
4. insurance company, especially companies which have an approval to deal with activities related to the life insurance;
5. companies with authority to perform operations with financial instruments;
6. government body (independent of the level: state, entity, district, local);
7. public agency, public fund – public institute (PIO/MIO, ZZO etc.), chamber of commerce (independent of the level);
8. shareholders entity which has a position and which shares are traded at the stock market, or which financial reports are published;
9. other financial institution (leasing company, microcredit company, microcredit foundation);
10. shareholders company that does not have apposition in the market, or which shares are not being traded in the stock market;
11. company with a limited liability, or a company organized in another form;
12. dealers, with a special attention on the type of business (precious stones, precious metals and other goods of high value, persons trading with cars, persons trading with real estate etc.);
13. individual – citizen;
14. politically exposed individual;
15. individual not present at the establishment of the business relations;
16. individual on the lists of the individuals under suspicion for terrorism financing activities issued by the Organization of the United Nations and the Council of Europe;
17. company with an intense cash performance including:
    a) companies dealing with transfer of funds, authorized exchange offices, agents for transfer of funds as well as other companies offering services of the money transfer,
    b) casinos, betting offices and other operations related to gambling and
    c) company which do not have intense cash performance, but for performing certain transactions use larger cash amounts;
18. humanitarian and other nonprofit organizations;

19. accountant, lawyer, notary, tax consultant and other which have accounts in a particular credit institution, and act on behalf of their clients;
20. entity (legal or individual) which perform their operations or transaction under strange circumstances such as:
    a) significant and unexplainable geographic distance between the head office of the bank and the party,
    b) frequent and unexplained closing of the account in one, and opening in another bank or
    b) frequent and unexplainable transfer of funds between the institutions in different geographic locations;
21. entity (legal or individual) for which FOO in the past three years:
    a) requested from the debtor to submit data due to a suspicion of a money laundering or terrorism financing activity,
    b) issued to the debtor an order for a temporary prevention of the execution of a suspicious transaction or
    b) issued an order to the debtor for a continuous monitoring of the financial operations.

Product risk (for the transaction, or business relation)

As part of the analyzing and assessing the risk from money laundering and terrorism financing activities, the banks when analyzing and evaluating a product risk, especially review the characteristics of the product offered to the clients depending whether or not those products are (manner and form for their use) convenient for money laundering and /or terrorism financing activities. In that process, they especially review if the clients will use (in which manner and how much) following products:

1. deposit products,
2. credit products,
3. eletronic transfer of money,
4. phisically transferable means of payment,
5. payable through foreign accounts,
6. services of funds management,
7. documented operations,
8. brokered deposits,
9. correspondent accounts,
10. electronic banking,
11. private banking, etc.,

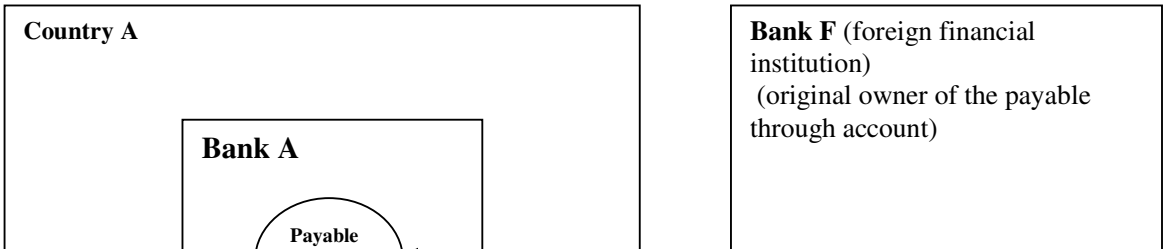
Which carry a different level of risk, depending on the use, each can individually carry a different level of risk.

In analysing and evaluating the risk products, the risk whould be assessed in correlation with the parameters:

1. volume,
2. average transaction amount,
3. profile of the client using a particular product,
4. existance of adequate specific controls,

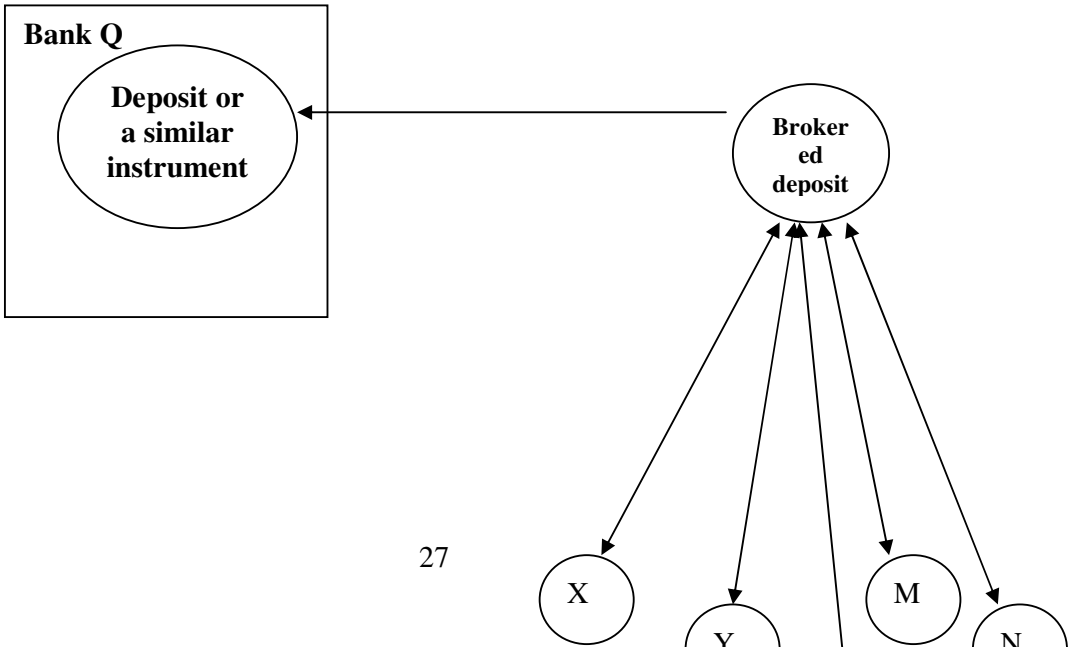
Taken the specific product: payable through accounts and brokered deposits, the following illustrations present basic functioning principles for these products:

1. Payable through accounts



Different from traditional corresponding accounts, payable through account allows to the clients of the financial institution which has the account (Bank F) a direct access to the account (write checks, withdraw funds and perform payments). For this type of accounts it is harder to determine the identity of the final user and they carry special risk from money laundering and terrorism financing activities. In order to decrease the risk which these types of accounts carry needed are specific controls.

1. Brokered deposits



Brokered deposits clients

Deposits broker gathers the deposits from the market and deposits the collected funds in a financial institution in his name. Using the advantage of the volume, the deposit broker can invest funds with an interest rate higher than individual depositors could do it. In most of the cases, requests for knowing and monitoring the client refer to the deposit broker and the bank does not need to know the final user or source of money. For this type of deposits there is a risk from money laundering and terrorism financing activities and needed are special controls to decrease this risk.

Country risk (geographic risk)

In the analyses and evaluation of the risk from the money laundering or terrorism financing activities the banks when analyzing and evaluating the country risk, especially evaluate if the client is a local or foreign legal entity and/or individual. Then they review the following characteristics which, directly or indirectly provide advantages to clients for money laundering and/or terrorism financing activities. In that they especially evaluate if the client comes from countries:

1. On which sanctions are enforced, embargo and similar measures by relevant international organizations (United Nations organization, Council of Europe, etc.);

2. For which trustworthy sources determined that:
   a) they do not have adequate laws and other measures for prevention of money laundering and terrorism financing activities;
   b) they finance or support terrorist activities and that determined terrorist organizations act in those countries;
   a) there is a significant level of corruption in those countries or other criminal elements;

3. which are not members of the European Union or do not implement relevant European Union directives;

4. which based on the data from the international organization FATF are among uncooperative countries or territories, or if it is a question of an *offshore* financial centre noted on the list developed by FOO.

In regard to the information on the risk countries, the countries or territories that do not cooperate or territories which do not fulfill the key international standards related to

prevention of money laundering or financing terrorism activities, the banks will follow the official internet pages of the international bodies.