Bosna i Hercegovina
Ministarstvo sigurnosti
Državna agencija za istrage i zaštitu

Босна и Херцеговина
Министарство безбједности
Државна агенција за истраге и заштиту

Financial Intelligence Department

GUIDELINES FOR RISK ASSESSMENT AND IMPLEMENTATION OF THE LAW ON PREVENTION OF MONEY LAUNDERING AND FINANCING OF TERRORIST ACTIVITIES FOR OBLIGORS

February, 2011

Istočno Sarajevo, Nikole Tesle 59; Telefon; 057/326-100; Fax:057/326-105
Источно Сарајево, Николе Тесле 59; Телефон: 057/326-100; Факс: 057/326-105

Pursuant to the Article 5 Paragraph (2) of the Law on Prevention of Money Laundering and Financing of Terrorist Activities („Official Gazette of B&H No 53/09), and in conjunction with the provisions of the Book of Rules on risk assessment, data, information, documents, identification methods and minimum other indicators required for efficient implementation of the Law on the Prevention of Money Laundering and Financing of Terrorist Activities („Official Gazette of B&H, No 93/09), the Head of the Financial Intelligence Department of the State Investigation and Protection Agency, e n a c t s:

GUIDELINES FOR RISK ASSESSMENT AND IMPLEMENTATION OF THE LAW ON MONEY LAUNDERING AND FINANCING OF TERRORIST ACTIVITIES FOR OBLIGORS

SECTION ONE – MAIN PROVISIONS

Article 1
(Scope)

The Guidelines for Risk Assessment and Implementation of the Law on Prevention of Money Laundering and Financing Terrorist Activities for Obligors (hereinafter referred to as: the Guidelines) regulate the manner of risk assessment, identification of the risk level for group or individual customers, business relations or transactions, customer due diligence, implementation of measures to detect and prevent money laundering and financing of terrorist activities in business subjects and companies seated in a third country where the obligor holds a majority share or majority voting in decision-making, monitoring of business activities of the customer, providing data to the Financial Intelligence Department, professional education and training, establishment of internal controls and audits by obligors, protection and maintenance of data that are available to obligor, appointment of authorised persons for the prevention of money laundering and financing of terrorist activities, as well as other issues significant for implementation of the provisions of the Law on Prevention of Money Laundering and Financing of Terrorist Activities (hereinafter referred to as: the Law).

Article 2
(Customer Due Diligence)

(1) When establishing business relation with customer or in the course of transactions amounting to or above the amount prescribed by the Law, the obligor, referred to in Article 4 of the Law shall determine or verify the identity of the customer on the basis of documents from credible and objective sources such as valid identification documents for physical persons and documentation from the court or other public registers for legal persons. The obligor shall neither establish business relation nor perform transaction if it is not possible to determine or verify the identity of the customer (entity).
(2) The obligor is required to obtain information about the purpose and intended nature of the business relationship or transaction, as well as to monitor regularly the business activities of the customer by applying the principle of "know your client", including information about the origin of the funds which are the subject of business activities.

Article 3
(Implementation of the Law and Standards)

When performing registered business activity, the obligor shall be required to comply the business operations with the provisions of the Law, Book of Rules on Risk Assessment, Data Information, Documents, Identification Methods and minimum other indicators required for efficient implementation of the Law on Prevention of Money Laundering and Financing Terrorist Activities (hereinafter: the Book of Rules) and other primary and secondary legislations and standards governing detection and prevention of money laundering and financing terrorist activities which are an integral part of business activities of the obligor.

Article 4
(Cooperation with Financial Intelligence Department)

The obligor shall ensure full cooperation with the Financial Intelligence Department of the State Investigation and Protection and special agencies and supervisory authorities in terms of submission of information, data, documentation pertaining to customers and transactions that could be indicative of a possible criminal offence of money laundering and financing of terrorist activities and detrimental to the stability, security and reputation of the financial system of Bosnia and Herzegovina. Accepted internal procedures of obligors must not, directly or indirectly, limit the previously mentioned cooperation between obligors.

Article 5
(Risk Assessment Programme)

Obligors shall be required to adopt a written internal programme to determine the risk levels of group or individual customers, their geographic areas of operations, business relations of transactions, products or services, the manner of provision of services to customers, new technological developments related to the possible misuse for the purpose of money laundering and financing terrorist activities. The Programme includes procedures of receipt and dealing with the customer, preparation of risk analysis, training of employees, conducting internal audits, procedures for recognizing and reporting suspicious transactions, and accountability of employees to implement measures to detect and prevent perpetration of criminal offence of money laundering and financing of terrorist activities. Employees must be familiar with the risk assessment program, apply it in their work, and act in accordance with it.

Article 6
(Training of Employees)

The obligor shall be required to ensure regular professional education, training and development of employees who directly or indirectly perform the tasks of prevention and detection of money laundering and financing of terrorist activities, as well as of third entities entrusted with the activities of customer due diligence.

SECTION TWO – RISK ASSESSMENT

Article 7
(Risk and Risk Analysis)

(1) The risk of money laundering and financing of terrorist activities is a risk that the customer will abuse the financial system of Bosnia and Herzegovina or business activity of the obligor to perpetrate criminal offence of money laundering and financing of terrorist activities or use directly or indirectly the business relationship, transaction, service or product for perpetration of the aforementioned criminal offence.
(2) The obligor shall be required to develop risk assessment based on which the risk levels of the customer, business relationship, product or transaction will be determined. Risk analysis is a prerequisite for implementation of the prescribed measures of customer due diligence while type of customer due diligence performed by the obligor pursuant to the Law (standard, enhanced, simplified) shall depend on the risk categories of customers, business relations, products or transaction.

Article 8
(Risk Management Policy)

(1) If required for an efficient implementation of the Law and Guidelines, prior preparation of the risk analysis, the obligor may accept an adequate risk management policy in relation to money laundering and financing of terrorist activities. The objective of accepting the risk management policy is to define at the level of obligors, the domains of business operations, which are more or less vulnerable given the possibility of misuse for the purposes of money laundering and financing terrorist activities. The obligor shall establish and identify major risks in these areas and measures to address them.
(2) Criteria for creating an initial basis for accepting risk management policy for money laundering and financing of terrorist activities are defined in more detail as follows:

a) the purpose and objective of risk management for money laundering and financing of terrorist activities and their connection with the business goal and strategy of the obligor,
b) the area and business processes of the obligor which are exposed to risk of money laundering and financing of terrorist activities,
c) the risks of money laundering and financing of terrorist activities in all key business areas of the obligor,
d) measures to address the risks of money laundering and financing of terrorist activities
e) the role and responsibility of the obligor's management in the introduction and acceptance of risk management policy for money laundering and financing of terrorist activities.

Article 9
(Preparation of Risk Analysis)

Risk analysis is a procedure in which the obligor shall define:

a) the evaluation of the likelihood that its business can be abused for money laundering and financing of terrorist activities,

b) the criteria based on which a certain customer, business relationship, product or transaction may be classified as more or less at risk of money laundering and financing terrorist activities,
c) establishment of consequences and measures to effectively manage such risks.

Article 10
(Criteria for Preparation of Risk Analysis)

When preparing the risk analysis, the obligor shall consider the following criteria:

a) the obligor shall derive the risk category from risk criteria in a manner that a certain customer, business relationship, product or transaction are classified into one of the risk categories;
b) the obligor, in determining risk categories, in accordance with the risk criteria set out in the Guidelines and its risk management policy, may classify a certain customer, business relationship, product or transaction as high- risk for money laundering and financing of terrorist activities and conduct enhanced customer due diligence;
c) in determining a customer risk category, the obligor shall not in any way classify a customer, business relationship, product or transaction, defined as a high-risk under the Law and Guidelines, as middle (average) or negligible risk.

Article 11
(Initial Risk Identification)

Prior to establishment of a business relationship based on the risk analysis, the obligor shall prepare a risk rating of the customer, business relationship, product or transaction by:

a) verifying the identity of the customer against the required data collected about the customer, business relationship, product or transaction and other data, that the obligor should collect for the preparation of risk rating,
b) evaluating the collected data in terms of risk criteria for money laundering and financing of terrorist activities (risk identification),
c) determining risk rating of a customer, business relationship, product or transaction in accordance with the previously developed risk analysis and classifies them under one of the risk categories,
d) implementing customer due diligence (standard, enhanced, simplified).

Article 12
(Subsequent Risk Identification)

Within the measures of regular monitoring of customer business relationship, the obligor shall re-check the grounds for the initial rating of risk or business relationship determined by the obligor, and if necessary, determine a new risk rating (identifies the risk subsequently). The obligor shall subsequently check the grounds for the initial risk rating of the entity or business relationship in the following situations:

a) if the circumstances have considerably changed based on which the risk rating of an entity or business relationship was made, and if the circumstances, which substantially affected the classification of the entity or business relationship in a certain risk category, have changed;

b) if the obligor doubts the truthfulness of the information based on which the risk rating was made for a certain entity or business relationship.

Article 13
(Criteria for Determining Entity Risk Category)

(1) In determining risk rating of a particular customer, business relationship, product or transaction, the obligor shall take into account the following criteria:

a) type, business profile and structure of the customer,
b) geographic origin of the customer,
c) nature of the business relationship, product, transaction,
d) previous experiences of the obligor with the customer.

(2) In addition to the above defined criteria, the obligor, in determining risk rating of customer, business relationship, products or transaction, may specifically observe other criteria such are:

a) size, structure and activity of the obligor including scope, structure and complexity of the operations performed by the obligor on the market,
b) status and ownership structure of the entity,
c) presence of the entity at the establishment of a business relationship or execution of transaction,
d) origin of the funds which are the subject of a business relationship or transaction in the event that the entity is considered a foreign politically exposed person according to the criteria set out in the Law,
e) purpose of establishment of business relationship or execution of transaction,
f) customers' knowledge of the product and their experience and knowledge in that domain,
g) other information indicating that the customer, business relationship, product or transaction may be a higher risk.

Article 14
(Entity Risk Categories)

According to risk categories, customers, business relationships, products or transactions may be divided into three categories:

a) higher (high) risk,
b) medium (average) risk,
c) low (negligible) risk.

Article 15
(Higher risk – Criteria, Type, Business Profile and Structure of Entity)

(1) Entities posing a higher risk for money laundering and financing of terrorist activities, given the criteria, type, business profile and structures of the entity, are:

a) entities included in the lists that are subject to certain measures, sanctions, embargoes imposed by the United Nations,
b) entities with residence or headquarters in the countries which are not subjects of the international laws and which do not apply internationally accepted standards of prevention and detection of money laundering and financing of terrorist activities, countries that finance or provide support to terrorist activities, countries in which terrorist organisations operate or there is a high corruption rate, countries which are not internationally recognized as states (provide opportunities for fictitious registration of legal entity, enable issuance of fictitious identification documents, etc.).

(2) Entities – physical persons posing a higher risk for money laundering and financing of terrorist activities are:

a) entity which is a politically exposed foreign person and/or person who performs or performed a distinguished public duty during the last year and has a permanent residence in the EU Member State or third country and a person who performs or performed in the last year a distinguished public duty in the EU member state or third country, including her/his immediate family members and close associates:

1) presidents of states, presidents of governments, ministers, deputy ministers and assistant ministers
2) elected representatives of legislative authorities,
3) holders of the highest judicial and constitutional – court positions,
4) judges of financial courts and members of central bank councils,
5) consuls, ambassadors and high-ranking officers of the armed forces,
6) members of managing and supervisory boards of legal entities majority-owned by the state,

b) entity whose immediate family members are politically exposed foreign persons: spouse or common-law partner, their children and their spouses or common-law spouse, parents, brothers and sisters,
c) entity whose close associate is a politically exposed foreign person and/or any natural person who shares profits from property or an established business relationship or another type of closer business contacts with politically exposed foreign person,
d) entity who is not personally present at the identification and verification of identity before the obligor in terms of physical presence before the obligor when submitting valid identification documents for the purpose of establishing its identity.

(3) Entities – legal persons posing a higher risk for money laundering and financing of terrorist activities are:

a) entity is a foreign legal person not performing or not permitted to perform trade, production or other activities in the country of registration (legal person seated in the country known as off-shore financial centre and which is subject to certain limitations in direct performance of the registered activity in that country),
b) entity is a fiduciary (trustee) or other similar legal arrangement of the foreign legal entity with unknown or concealed owners or directors (a legal arrangement of the foreign legal entity offering representation services to a third person, i.e. company, founded by a contract concluded between the founder and the manager that manages

the assets of the founder, to the benefit of certain persons, beneficiaries or users, or for other specific purposes (private, acquired, general and non-acquired assets)

c) entity having a complex statutory structure or complex ownership chain (complicated ownership structure or complex ownership chain hinders or do not enable identification of beneficial owner or person exercising control over the legal person),
d) entity is a financial organisation which is not required to be licensed by a relevant supervisory authority for performance of its activities, and/or pursuant to the national legislation is not subject to AML and CFT measures
e) entity is a non-profit organisation (institution, company or other legal entity, i.e. entity established for publicly useful, charitable purposes, religious communities, associations, foundations, non-for-profit associations and other entities not performing economic activities) and meeting one of the following conditions:

   1) entity seated in a country known as an off-shore financial centre,
   2) entity seated in a country known as a financial and tax heaven,
   3) entity seated in a country that is not a member of the EU, European Economic Area (EEA) or Financial Action Task Force on Money Laundering – FATF, and in a country that does not have in place adequate regulations and internationally accepted standards for the prevention of money laundering and financing of terrorist activities,
   4) there is a natural or legal person among its members, resident of any of the countries listed under the previous point

f) entity is a legal person established using bearer shares.

Article 16
(Higher Risk – Criterion of Customer's Geographic Position)

(1) Entities posing an enhanced risk for money laundering and financing of terrorist activities according to the criterion of geographic position are those with permanent or temporary residence or seat in:

a) country which is not a member of the EU, EEA or FATF, and/or country which does not have adequate regulations in place and/or internationally recognised standards in the area of prevention of money laundering and financing of terrorist activities,
b) country, which is, based on the assessment of relevant international organisations, known for production or well organised and developed drug trafficking (states of Near, Middle and Far East known for heroin production: Turkey, Afghanistan, Pakistan; states of the Golden Triangle: Myanmar, Laos, Thailand; states of South America known for cocaine production: Peru, Columbia and neighbouring countries; states of the Middle and far East and Central America known for production of Indian cannabis: Turkey, Lebanon, Afghanistan, Pakistan, Morocco, Tunis, Nigeria and neighbouring countries and Mexico).
c) country, which is, based on the assessments of relevant international organisations, known for high level of organised crime stemming from corruption, trafficking in weapons, human beings and violation of human rights,
d) country, which is, based on the assessments of the FATF, classified among non-cooperative countries or territories (these are countries or territories which, according to the assessment of the international working group FATF, do not have adequate legislation on the prevention and detection of money laundering or financing of

terrorist activities, state control over financial institutions do not exist or is inadequate, establishment or operation of financial institutions is possible without the approval or registration with state regulatory authorities, the state encourages opening of anonymous accounts and other anonymous financial instruments, there is an inadequate system of identification and reporting of suspicious transactions, legislation does not recognize obligation to identify a beneficial owner, international cooperation is inefficient or does not exist),

e) country subject to measures of the United Nations, which particularly include complete or partial interruption of economic relations, rail, sea, air, postal, telegraphic, radio and other communication links, interruption of diplomatic relations, military embargo, travel embargo etc.,

f) country known as a financial or tax haven; for these countries, it is particularly important that they provide full or partial exemption from taxes or tax rate is significantly lower compared to other states. Such states typically does not have in place the agreements on double taxation avoidance, and if they signed these agreements, they do not implement them; the legislation of these countries allows and requires strict respect of banking and business secrets; fast, discreet and low-cost financial services are ensured. Countries that are generally known as financial or tax havens include: Dubai (Jebel Ali Free Zone), Gibraltar, Hong Kong, Isle of Man, Lichtenstein, Macau, Mauritius, Monaco, Nauru, Nevis Islands, Island (Norfolk Area), Panama, Samoa, San Marino, Sark, Seychelles, St. Kitts and Nevis, St. Vincent and Grenadine, Switzerland, (Vaud and Zug Cantons), Turks and Caicos Islands, United States of America (federal states of Delaware and Wyoming), Uruguay, Virgin Islands and Wanatu),

g) country generally known as an off-shore financial centre (it is significant that these countries determine the limitations in direct performance of registered activities of companies in the country, ensure a high level of protection of banking and business secrets, implement liberal control over foreign trade operations, provide fast, discreet and low-cost financial services and registration of legal entities. A characteristic of these countries is also not having adequate legislation in the field of prevention and detection of money laundering and financing of terrorist activities. States that are known as offshore financial centres are: Andorra, Angola, Anguilla, Antigua and Barbuda, Aruba, Bahamas, Barbados, Belize, Bermuda, British Virgin Islands, Brunei Darussalam, Cabo Verde, Cayman Islands, The Cook Islands, Costa Rica, Delaware (SAD), Dominica, Gibraltar, Grenada, Guernsey, the Isle of Man, Jersey, Labuan (Malaysia), Lebanon, Lichtenstein, Macao, Madeira (Portugal), Marshall Islands, Mauritius, Monaco, Montserrat, Nauru, Nevada (SAD), the Netherlands Antilles, Niue, Palau, Panama, Philippines, Samoa, Seychelles, St. Kristofer and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Zug (Switzerland), Tonga, Turks and Caicos Islands, Uruguay, Vanuatu and Wyoming (SAD).

(2) Obligors should consider the following international organizations as competent international organizations to monitor the effectiveness of implementation of measures in the area of prevention of money laundering and financing of terrorist activities in compliance with the provisions of international standards:

a) The Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL),

b) Financial Action Task Force on Money laundering - FATF),

c) International Association of Financial Supervisory Bodies dealing with detection and prevention of money laundering and financing of terrorist activities – Financial Intelligence Units (Egmont Group),
d) the European Commission Committee for the Prevention of Money Laundering *and* Terrorist Financing,
e) European Bank of Reconstruction and Development,
f) International Monetary Fund,
g) the World Bank,
h) International Organization of Securities Commissions - IOSCO,
i) Committee of European Securities Regulators - CESR,
j) European Insurance and Occupational Pensions Supervisors - CEIOPS,
k) International Association of Insurance Supervisors - IAIS.

Article 17
(Higher Risk – Criterion of Business Relationships, Products and Transactions)

(1) Business relationships posing a higher risk of money laundering and financing of terrorist activities based on the criterion of business relationships, products and transactions include:

a) Business relations including constant or large payments of money from and/or to the customer's account opened with a credit or financial institution in the country which is not the member of the EU, EEA or FATF, and/or a country that does not have in place adequate legislation and internationally accepted standards for the prevention of money laundering and financing of terrorist activities,
b) business relationships established by a foreign credit/financial or other fiduciary institution seated in a country which is not a member of the EU, EEA or FATF, or a country which does not have in place adequate regulations and internationally accepted standards for the prevention of money laundering and financing of terrorist activities, on its own behalf and for the account of the customer
c) Business relationships established in the absence of the customer at the obligor's, where simplified due diligence was not performed,
d) Business relationships established in favour of the person or entity on the list of persons or entities subject of measures, sanctions and embargoes in force introduced by the UN.

(2) Products posing a higher risk of money laundering and financing of terrorist activities are all bearer negotiable instruments, but also negotiable instruments that are either in bearer form, made out to a fictitious payee, endorsed without restriction, or otherwise in such form that title thereto passes upon delivery and all other incomplete instruments signed, but with the payee's name omitted.
(3) Transactions posing a higher risk of money laundering and terrorism financing include:

a) Transactions intended for persons, i.e. entities against which there are measures, sanctions and embargoes in force introduced by the United Nations,
b) Transactions which a customer would execute for and on behalf of the person or entity against which there are measures, sanctions and embargoes in force introduced by the United Nations,

c) Payments of money from/to the customer's account, other than the customer's account stated when the customer was identified, i.e. its usual business account (especially when involving international transactions),
d) Transactions intended for persons domiciled or registered in a state known as a financial or tax haven or off-shore financial centre,
e) Transactions intended for non-profit organisations seated in a country known as an off-shore financial centre, or a country known as a financial or tax haven or a country which is not a member of the EU, EEA or FATF, and a country which does not have in place adequate regulations and internationally accepted standards for prevention of money laundering and financing of terrorist activities.

Article 18
(Enhanced Risk – Criterion of Previous Experience of Obligor with Entity)

Entities representing high risk of money laundering or financing of terrorist activities, based on obligors' experience, shall be:

a) persons for whom the Financial Intelligence Department requested information from obligors due to suspicion of money laundering or financing of terrorist activities with reference to a transaction of person in the past three years,
b) persons against whom the Financial Intelligence Department issued a written order to the obligor for temporary suspension of a transaction or transactions in the past three years,
c) persons for whom the Financial Intelligence Department ordered the obligor in writing to continuously monitor a customer's business operations in the past three years,
d) persons about whom the obligor submitted information to the Financial Intelligence Department due to suspicion of money laundering or financing of terrorist activities due to suspicion of money laundering or financing of terrorist activities with reference to that person or a transaction executed by that person in the past three years.

Article 19
(Medium – Average Risk of Money Laundering and Financing of Terrorist Activities)

The obligor shall classify as medium (average) risky an entity, business relationship, product or transaction, which based on criteria set out in the Guidelines cannot be classified as highly risky or negligibly risky and in this case act in line with provisions on regular monitoring of a customer business activities defined by the Law.

Article 20
(Negligible Risk of Money Laundering and Financing of Terrorist Activities)

The obligor shall consider the following entities to represent a negligible risk of money laundering or financing of terrorist activities:

a) obligors referred to in Article 4, Paragraph 1, Items a), b), c), d) and e) of the Law, namely:

    1) banks,

2) post offices,
3) investment and pension companies and funds, regardless of their legal form,
4) authorised mediators trading in financial instruments, foreign currency, exchange, interest rates, index instruments, transferrable securities and commodity futures,
5) insurance companies, insurance mediation companies, investment representation companies and insurance representatives possessing an operating licence in the domain of life insurance,

b) authorities of Bosnia and Herzegovina, Federation of Bosnia and Herzegovina, Republic of Srpska, Brčko District or institutions with public mandates,
c) company whose financial instruments have been accepted and traded in the stock market or regulated public market in one or more member countries, in line with the European Union regulations and/or companies with main offices in a third country whose financial instruments have been accepted and traded in the stock market or regulated public market in a member country or third country, provided that requirements for information disclose in line with the European Union regulations are valid in the third country,
d) persons engaged in business activities and performing transactions as set out in Article 9 of the Book of Rules.

SECTION THREE – CUSTOMER DUE DILIGENCE

Article 21
(Regular Customer Due Diligence)

(1) Customer due diligence is a key preventive element in a system for detection and prevention of money laundering and financing of terrorist activities. The purpose of customer due diligence measures is to determine and verify credibly the true identity of a customer. The customer due diligence measures shall include determination and validation of a customer's identity, obtainment of information about the purpose and intent of the nature of a business relationship or transaction, regular monitoring of customer's business activities through an obligor.
(2) An obligor shall determine and verify the identity of an entity based on documents, data or information obtained from authentic and objective sources (upon an inspection of a customer's valid identification document in their presence, from other valid public documents submitted by a customer or directly from a customer or otherwise, upon an inspection of the original or certified copy of documents from judicial or other public registry, submitted on behalf of a legal person by a legal representative or a person authorised by a legal person).
(3) It shall be prohibited to enter into a business relationship or execute a transaction when it is not possible to determine a customer identity or when an obligor has a founded doubt as to accuracy and authenticity of information and/or documents verifying the entity’s identity, and in a situation when an entity is not prepared or willing to cooperate with an obligor in determining correct and complete information required by the obligor for the entity analysis. In such instances, the obligor shall not enter a business relationship and already existing business relationship or transaction shall be terminated and the Financial Intelligence Department shall be informed about that. The obligor can simplify customer due diligence measures in specific cases stipulated in Article 14 of the Law. The Law is based on a primary assumption that some entities, business relationships, products or transactions represent higher and other represent lower risk of abuse for money laundering

or financing of terrorist activities, and stipulates enhanced and simplified customer due diligence.

Article 22
(Obligation of Customer Due Diligence)

The obligor shall take customer due diligence measures when:

a) entering a business relationship with a customer,
b) executing a transaction in the amount of BAM 30.000 or more, regardless whether the transaction is executed in a single operation or several clearly connected transactions,
c) doubting authenticity and adequacy of previously obtained information about a customer or beneficial owner,
d) suspecting of money laundering or financing of terrorist activities in terms of a transactions or client, notwithstanding the amount of the transactions.

Article 23
(Enhanced Customer Due Diligence)

The obligor shall apply the customer due diligence measures in cases when, due to the nature of a business relationship, form and method of executing a transaction, customer business profile or other circumstances related to a customer, there is or could be a higher risk of money laundering or financing of terrorist activities. Article 20 of the Law stipulates that the enhanced customer due diligence measures shall be applied when entering a correspondent relationship with a bank or other similar credit institution with main offices abroad, when entering a business relationship or executing a transaction with a foreign politically exposed person, with a non-face-to-face customer at determining and verifying the identity during the application of the customer due diligence measures.

Article 24
(Enhanced Customer Due Diligence of Foreign Politically Exposed Persons)

A foreign politically exposed person shall include any physical person to whom a prominent public function is or was entrusted in the previous year, including the closest family members and close associates.

When a customer entering a business relationship or executing a transaction is a foreign politically exposed person or when a customer on whose behalf they enter a business relationship or execute a transaction is a politically exposed person, employees of the obligor, in addition to enhanced customer due diligence measures, will take the following measures:

a) collect information about the source of funds and assets which are or will be a subject of a business relationship or transaction;
b) mandatorily provide a written approval from a superior or responsible person before entering into a business relationship;
c) after entering into a business relationship, through a due diligence procedure, monitor transactions and other business activities of a foreign politically exposed person, performed through the obligor.

Article 25

(Non Face-To-Face Customers)

The obligor shall perform enhanced customer due diligence when a customer is not physically present with an obligor when determining and verifying identity when entering a business relationship, where an obligor, with an exception of measures stipulated in Article 7 of the Law, shall take one or more of the following measures:

a) collection of additional documents, data or information based on which the identity of a customer shall be additionally verified,
b) additional verification of submitted documents or additional verification by a credit or financial institution,
c) first payment in a business activity to be made through an account opened on behalf of a customer with a different credit institution.

Article 26
(Other High Risk Entities)

The customer due diligence measures can also be applied in other cases of high risk entities, business relationships, products or transactions, including:

a) mandatory previous written approval by a superior with the obligor for entering into such a business relationship or execution of a transaction,
b) mandatory taking of one of the following measures:

    1) obtainment of documents, data or information, based on which the obligor shall additionally verify and confirm authenticity of identification documents and data determining and verifying a customer identity,
    2) additional verification of information obtained about a customer in public and other available data records,
    3) obtainment of adequate references of credit or financial institutions with which a customer entered into a business relationship (e.g. opened account), whereby it needs to be taken into account that in this case only institutions respecting internationally accepted standards and measures for the prevention of money laundering and financing of terrorist activities pursuant to national legislation can be treated as credit or financial institutions,
    4) additional verification of data and information about a customer with relevant state bodies or other relevant supervisory institutions in a country where the customer has a permanent place of residence or main offices,
    5) establishment of a direct contact with a customer by telephone or visit by an authorised person of obligor to a house or main office of the customer,

c) mandatory monitoring of transactions and other business activities performed by a customer with an obligor.

Article 27
(Simplified Customer Due Diligence)

(1) The obligor shall perform a simplified customer due diligence when, after an assessment by the obligor, there is a low (negligible) risk of money laundering or financing of terrorist activities with the customer, when information about a customer that is a legal

person or its beneficial owner is transparent and publically available. This means that in some cases the obligor determines and verifies the identity of a customer, but the procedure is simplified in comparison with the enhanced customer due diligence.

(2) The obligor shall not enter into a business relationship or execute a transaction before determining all facts required for the customer risk assessment.

(3) The simplified customer due diligence shall not be allowed when there is a suspicion of money laundering or financing of terrorist activities with the customer, or if a customer, in line with the risk assessment, is classified in a high risk customer category.

Article 28
(Customer Analysis through Third Person)

(1) Pursuant to requirements of the Law and secondary legislation, when entering a business relationship with a customer, the obligor can entrust determination and verification of a customer identity, determination of the identity of a beneficial owner and collection of information about the purpose and intent of a business relationship or transaction to a third person, whereby they shall first be required to verify whether the third party entrusted with the application of these measures meets the requirements stipulated by the Law, since the obligor shall bear the final responsibility for the application of the customer due diligence measures assigned to the third person.

(2) The obligor shall provide a written consent by a third person confirming reliability of the third person for a customer identification which will be determined separately. An exception is regular monitoring of customer activities set out in Article 18 of the Law and in case the customer is a foreign legal person that does not deal or is not allowed to deal with trade, production or other activity in the country of registration and if the customer is a fiduciary or other similar foreign legal person with unknown or hidden owners or managers.

SECTION FOUR – APPLICATION OF DETECTION AND PREVENTION OF MONEY LAUNDERING AND FINANCING OF TERRORIST ACTIVITIES MEASURES IN BUSINESS UNITS AND COMPANIES IN WHICH OBLIGOR HAS MAJORITY SHARE OR MAJORITY RIGHT IN DECISION MAKING, WITH MAIN OFFICES IN THIRD COUNTRY

Article 29
(Obligation to Apply Measures)

The obligor shall establish a system for the management of a unified policy for the detection and prevention of money laundering and financing of terrorist activities. To this end, particular attention shall be paid to implementing detection and prevention measures for money laundering and financing of terrorist activities stipulated by the Law in conjunction with the customer due diligence, reporting suspicious transactions, keeping records, internal audit, appointment of an authorised person, storage of data and other important circumstances related to detection and suppression of money laundering or financing of terrorist activities to the same or similar scope in business units and enterprises where the obligor has a majority share or majority voting rights in decision making, and which have main offices in a third country.

Article 30

(Types of Risk Elimination Measures)

In case that the implementation of standards for the detection and suppression of money laundering and financing of terrorist activities, which are incorporated in activities of business units and an enterprise in which the obligor has a major share or majority voting rights, explicitly contrary to the legislation of a third country in which the business unit or enterprise have their main offices, the obligor shall inform the Financial Intelligence Department about this and implement appropriate measures for the elimination of the risk of money laundering and financing of terrorist activities, including:

a) introduction of additional internal procedures for the prevention or reduction of possibilities for abuse with the aim of money laundering or financing of terrorist activities,
b) implementation of additional internal control of business operations of obligors in all key areas exposed the most to the risk of money laundering and financing of terrorist activities,
c) introduction of internal risk assessment mechanisms for entities, business relationships, products and transactions in line with the Guidelines,
d) implementation of strict entity classification policy according to their exposure and consistent application of measures accepted based on this policy,
e) additional training of personnel.

Article 31
(Obligor Management Obligations)

The obligor management shall:

a) ensure that all business units and enterprises in which the obligor has a majority share or majority voting rights and which have main offices in a third country, as well as their personnel, are familiar with the policy of detection and prevention of money laundering and financing of terrorist activities;
b) through an authorised person of a business unit and enterprises in which the obligor has a majority share or majority voting rights in decision making, ensure that internal procedures for detection and prevention of money laundering and financing of terrorist activities are incorporated into their business process to the largest extent possible;
c) perform ongoing monitoring of appropriate and efficient application of measures of detection and prevention of money laundering and financing of terrorist activities in business units and enterprises in which the obligor has the majority share or majority voting rights, and which have main offices in third countries.

Article 32
(Reporting to Parent Obligor)

Business units and companies in which the obligor holds a major share or majority voting in decision making and which have their main offices in a third country, shall report to the parent obligor, at least once a year, on accepted measures in detection and prevention of money laundering, particularly in terms of customer due diligence, risk assessment procedure, identification and reporting about suspicious transactions, security and storage of data and documents, keeping records on entities, business relationships and transactions.

SECTION FIVE – MONITORING CUSTOMER BUSINESS ACTIVITIES

Article 33
(Purpose of Monitoring Customer Business Activities)

Regular monitoring of customer business activities is important for the efficiency of the implementation of stipulated measures for detection and prevention of money laundering and financing of terrorist activities, and it shall be implemented by the application of the "meet your customer" principle, also taking into account the origin of the funds which are the subject of the transactions. The purpose of monitoring customer business activities is to determine legality of business operations and verification of compliance of business operations with a foreseen nature and purpose of a business relationship entered into by the entity and obligor, or with the entity's usual scope of operations. Monitoring customer business operations shall be divided into four segments of the entity's business operations with the obligor, including:

a) monitoring and verifying compliance of the entity's business operations with the foreseen nature and purpose of a business relationship,
b) monitoring and verifying compliance of the entity's source of funds with the foreseen source of funds which the entity stated when entering into a business relationship with the obligor,
c) monitoring and verifying compliance of entity business operations with their usual scope of business operations,
d) monitoring and updating collected documents and information about an entity.

Article 34
(Entity Business Activity Monitoring Measures)

(1) For monitoring and verification of compliance of customer business operations with prescribed nature and purpose of a business relationship entered into by the entity with the beneficiary, the following measures shall be applied:

a) analysis of data on purchase and/or sale of a financial instrument, or other transactions for a particular period, with the aim of determining whether there are potential circumstances for suspicion of money laundering or financing of terrorist activities related to a particular purchase or sale of financial instruments or other transaction. The decision on suspiciousness shall be based on suspicion criteria set out in the list of indicators for identification of suspicious entities and transactions;
b) development of a new entity risk rating, i.e. update of a previous entity risk rating.

(2) For compliance monitoring and verification of entity business operations and their usual scope of business operations, the following measures shall be taken into account:

a) monitoring purchase or sales value of financial instruments and/or other transactions exceeding a particular amount; the obligor shall decide on their own what is the amount above which they will monitor entity business operations, for every entity separately taking into account its risk category (for an efficient application of this measure, the obligor can establish an appropriate information support);

b) analysis of a purchase or sale of a financial instrument and/or other transaction on grounds of suspicion of money laundering and financing of terrorist activities, when a number of purchase or sale exceeds a particular value; suspiciousness analysis of a purchase or sale of financial instruments, and/or other transactions, shall be based on suspicion criteria set out in the list of indicators for identification of suspicious transactions.

(3) For monitoring and updating collected documents and data on an entity, the following measures shall be taken into account:

a) annual customer due diligence,
b) annual customer due diligence when there is doubt in authenticity of previously received information about an entity or entity beneficial owner (if the entity is a legal person),
c) verification of data on an entity or their legal representative in judicial or other public registry,
d) verification of data obtained directly from an entity, their legal representative or authorised person,
e) verification of lists of persons, countries and other subjects against whom measures, sanctions and United Nations embargo are in place.

Article 35
(Scope of Monitoring Entity Business Activities)

(1) A scope and intensity of monitoring entity business activities depend on an entity risk rating or entity risk category, wherefore the scope of monitoring entity business activity is as follows:

a) for a high risk entity, prescribed business activity monitoring measures rated as highly risky shall be applied by the obligor at least annually, and regularly and at least once a year measures of repeated customer due diligence shall be applied provided that requirements stipulated by the Law are met;
b) for a medium (average) risk entity, prescribed entity business activity monitoring measures, rated as medium (average) risky, shall be applied by the obligor at least every three years, and regularly and at least once a year repeated annual customer due diligence measures shall be applied provided that requirements stipulated by the Law are met;
c) for a low – negligible risk entity, stipulated entity business activity measures shall be applied by the obligor at least every five years and at least once a year repeated customer due diligence measures shall be applied provided that requirements stipulated by the Law are met.

(2) Application of entity business activity monitoring measures shall not be required if an entity did not perform business activities (purchase or sale of financial instruments or other transaction) upon entry into a business relationship. In such case, the obligor shall apply business activity monitoring measures during the next purchase or sale of a financial instrument or the next transaction.
(3) In its internal documents, in line with its policy on risk management for money laundering and financing of terrorist activities, the obligor can opt for more frequent business activity monitoring for a certain type of entities, other than set out in the Guidelines and determine

additional measures for entity business activity monitoring and verifying the legality of its operations.

SECTION SIX – OTHER OBLIGOR DUTIES

Article 36
(Reporting Cash Transactions)

(1) Immediately and not later than three days after executing a transaction, the obligor shall submit information set out in Article 44 Paragraph (1) of the Law on the cash transaction and connected cash transactions in the amount of BAM 30.000 or more to the Financial Intelligence Department.
(2) A cash transaction is any transaction in which an obligor physically receives cash from a customer or gives cash to the customer and connected transactions are two or more transactions originating from an account or directed to an account or legal or physical person, where the amount of individual transactions is below the amount required for performing due diligence pursuant to the provisions of the Law, and which jointly exceed the amount set out in Article 6 of the Law and can be regarded as mutually connected due to a time period in which they were executed, transaction receiver or orderer, transaction execution methods, reasons behind transaction executions or other factors on the basis of which the transactions can be regarded connected. The obligor shall regard as connected such transactions which are being executed within a time period of more than 24 hours if it can be determined that each transaction is one in a series of transactions.
(3) In cases of frequent cash transactions, which are a part of usual business activities of successful customers that operate legally and whose activities are familiar to the obligor, the obligor can, in line with the Book of Rules, exclude from reporting to the Financial Intelligence Department such large and connected cash transactions. The obligors shall not be required to report large or connected transactions to the Financial Intelligence Department when customers are persons specified in Article 39 of the Book of Rules.

Article 37
(Suspicious Transactions Reporting)

(1) The Law stipulates that a suspicious transaction is any transaction assessed by the obligor or relevant authority, with reference to the transaction or person executing the transaction, to be suspicious in terms of the perpetration of a criminal offence of money laundering or financing of terrorist activities and that the transaction contains funds originating from illegal activities. Suspicious transactions are also those that differ from normal customer activity models and every complex or unusually large transaction lacking obvious economic, business or legal purpose.
(2) A suspicious transaction is the transaction clearly differing in its characteristics related to the customer status or other characteristics of the customer or funds from usual transactions by the same customer if it corresponds to a required number and type of indicators for reasons to suspect of money laundering or financing of terrorist activities and if the transaction is aimed at avoiding regulations governing preventive measures for money laundering and financing of terrorist activities.

(3) A suspicion assessment of a customer, transaction or business relationship is based on suspicion criteria, set out in the list of indicators for the identification of customers and transactions suspicious of money laundering or financing of terrorist activities and list of indicators raising suspicion, both general and specific, as set out in the Book of Rules. The List of Indicators for identifying suspicious transactions and persons is the basic guide for employees and persons authorised by the obligors in recognising suspicious circumstances related to a specific entity, transaction executed by an entity or business relationship entered into, whereby employees of the obligor must be familiar with the indicators in order to be able to use them in their work. In terms of the evaluation whether a transaction is suspicious, an authorised person shall be required to provide all professional assistance to the employees.

(4) Employees of the obligor who determine there are reasons for suspicion of money laundering or financing of terrorist activities shall inform a person authorised for the prevention of money laundering or their deputy. The obligor shall organise a suspicious transaction reporting procedure among all organisational units and authorised person in line with the following instructions:

a) determine data submission method in detail (by telephone, fax, secure electronic method, etc.),
b) determine type of data to be submitted (information about an entity, reasons for suspicion of money laundering, etc.),
c) determine a method for cooperation between organisational units and authorised person,
d) determine a procedure for an entity when the Financial Intelligence Department temporarily suspends a transaction,
e) determine the role of an authorised person of the obligor when reporting a suspicious transaction,
f) prohibit disclosure of information about whether data, information or documents are submitted or whether they will be submitted to the Financial Intelligence Department,
g) determine measures with reference of the continuation of business operations with an entity (temporary termination of business operations, termination of a business relationship, and enhanced customer due diligence and more detailed monitoring of future business activities of an entity, etc.).

Article 38
(Reporting to Financial Intelligence Department)

(1) Pursuant to the Law, the obligor shall submit information about any attempted or executed transaction, customer or person to the Financial Intelligence Department if there is suspicion of money laundering or financing of terrorist activities, except by usual means (through application software for electronic suspicious transaction reporting, through persons authorised for postal service operations, person authorised for documentation delivery – courier), also by telephone or telefax. However, the Financial Intelligence Department shall be informed about a transaction in writing as well, not later than the next working day in the manner previously described.

(2) The obligor shall submit information, data and documents to the Financial Intelligence Department immediately after the occurrence of suspicion and before the execution of a transaction, stating a period in which the execution of a transaction is expected.

Article 39

(Professional Education and Training)

(1) The obligor shall provide regular professional education and training to all employees who directly or indirectly perform prevention and detection of money laundering and financing of terrorist activities, which also includes introduction to relevant laws and secondary legislation, relevant professional literature, list of indicators for the identification of clients and transactions suspected of being for the purpose of money laundering or financing of terrorist activities.
(2) The obligor shall develop an annual programme for professional education, training and development of employees by the end of March of the current year, including:

a) contents and scope of educational programme,
b) objective of educational programme,
c) educational programme implementation method (lectures, workshops, exercises, etc.),
d) range of employees for whom the educational programme is intended,
e) duration of educational programme.

Article 40
(Internal Control and Audit)

(1) The obligor shall ensure regular and ongoing internal control and audit of legality when performing tasks and duties of prevention and detection of money laundering and financing of terrorist activities. The purpose of the internal control and audit activities shall primarily be a verification of compliance of business operations with the provisions of the Law in the assessment of the adequacy of obligor policies and procedures in identifying transactions or entities for which there are reasons for suspicion of money laundering or financing of terrorist activities, in order to take measures for their removal due to possibly identified deficiencies.

The obligor shall particularly pay attention to:

a) performing particular operational procedures of detection and prevention of money laundering and financing of terrorist activities pursuant to the policy of risk management for money laundering and financing of terrorist activities,
b) compliance of procedures for risk rating an entity, business relationship, product or transaction with the policy for risk management for money laundering or financing of terrorist activities and risk analysis,
c) appropriate protection of confidential information,
d) appropriate and complete professional education and training in detection and prevention of money laundering and financing of terrorist activities,
e) appropriate and frequent utilisation of the list of indicators for the identification of suspicious transactions,
f) appropriate and efficient system for the delivery of data, information, documents on entities and transactions, for which there are reasons for suspicion of money laundering or financing of terrorist activities,
g) appropriate measures and recommendations to obligors that need to be implemented on the basis of conclusions of a performed internal audit.

(2) In the framework of an internal audit, the obligor shall also determine the accuracy and efficiency control of the application of measures on detection and prevention of money

laundering and financing of terrorist activities with external associates and representatives, who are contractually authorised to perform certain business activities.

(3) The obligor will authorise an internal audit service or some other competent supervising authority to inspect independently the compliance of detection and prevention system functioning for money laundering and financing of terrorist activities with provisions of the Law, secondary legislation and Guidelines, which will inform the obligor management about its activities in a form of proposed measures and recommendations for the removal of deficiencies. The accuracy and efficiency control of the implementation of prescribed measures for detection and prevention of money laundering and financing of terrorist activities shall be applied by the obligor through regular and extraordinary supervision.

Article 41
(Data Protection and Storage)

(1) The obligor shall treat data, information and documents available to the obligor pursuant to the provisions of the Law as a business secret or secret information pursuant to the provisions of the Law on Protection of Secret Information ("Official Gazette BH", No. 54/05, 12/09). This implies that the obligor shall not be allowed to reveal to a customer or third person that an information, data or documents about a customer or transaction are submitted to the Financial Intelligence Department, or that the Financial Intelligence Department pursuant to provisions of Article 48 of the Law temporarily suspended the execution of a transaction and ordered ongoing monitoring of financial operations of a customer in relation to which there are reasons for suspicion of money laundering or financing of terrorist activities or other person for whom it is possible to conclude with certainty that they helped or participated in transactions or business operations by a person under suspicion and to inform regularly about transactions or business operations that these persons perform or intend to perform.

(2) The obligor or its personnel shall not be responsible for potential damage inflicted upon customers or third persons or be held criminally or civilly accountable for submitting information, data or documents to the Financial Intelligence Department or for executing an order from the Financial Intelligence Department on a temporary suspension of transactions or for acting upon an instruction issued about this order, provided that they acted pursuant to the Law or some other implementing document or that they acted only for the purpose of prevention and detection of money laundering and financing of terrorist activities, unless otherwise provided for by the Law.

(3) In its internal document, the obligor shall regulate procedures in detail and provide instructions to their personnel for acting and keeping relevant data, which includes the following:

a) data and documents shall be prepared in a method and form disabling access to and knowledge of their contents to unauthorised personnel (in appropriate and technically or physically secure premises, in locked cabinets, etc.);
b) right to inspection of information about suspicious entities and transactions shall be provided only to members of the management and supervisory board of an obligor, authorised person for prevention of money laundering and financing of terrorist activities and their deputies, managers of obligor business units and other persons appointed by the obligor management;
c) it shall be prohibited to photocopy, transcribe, modify, publish or otherwise reproduce relevant documents prior to a written approval from a responsible person;

d) in case of copying documents, the obligor shall ensure that it can be undoubtedly determined from the copy itself what documents or parts of documents the copy was made from; it needs to be specially indicated in a visible spot that it is a photocopy, number of copies made, date of making photocopies and the signature of a person who made the photocopies;
e) The obligor shall strictly provide electronic protection to ensure denial of access to data and documents for unauthorised persons;
f) any submission of data, information and documents shall be allowed only with a guarantee that unauthorised persons shall not be granted access to those, notwithstanding whether the delivery is made through their persons authorised for delivery – couriers or in a sealed envelope through registered mail, return receipt requested, etc., with an indication of a classification secret, and electronically it shall be required to use a secure business operation system (encrypted or coded messages, etc.);
g) application of provisions of the Law on the Protection of Secret Information by the obligor's personnel.

Article 42
(Authorised Person)

With the aim of performing tasks and duties pursuant to the provisions of the Law and secondary legislation, the obligor shall appoint an authorised person and one or more deputies of the authorised person and inform the Financial Intelligence Department about this within 7 days after the date of their appointment.

The authorised persons and replacements shall:

a) ensure establishment, functioning and development of the system for the detection and prevention of money laundering and financing of terrorist activities with the obligor, which shall also include cooperation with employees in the operational implementation of measures, monitor and coordinate activities of the obligor, provide recommendations to the obligor management on the development of the risk management policy for money laundering and financing of terrorist activities,
b) continually inform the obligor management about activities in detection and prevention of money laundering and financing of terrorist activities, participate in defining and modifying operational procedures and internal provisions and development of guidelines for the implementation of control, participate in the establishment and development of information support in terms of prevention and detection of money laundering or financing of terrorist activities,
c) participate in the preparation of professional education and training programme, participate with other obligors in the development of a unified policy for detection and prevention of money laundering and financing of terrorist activities,
d) ensure due and timely reporting to the Financial Intelligence Department pursuant to the Law and provisions deriving from it.

SECTION SEVEN – FINAL PROVISIONS

Article 43
(Obligor Duties)

Obligors shall harmonise their Guidelines and adapt internal documents not later than 60 days after the date of receiving the Guidelines and develop new documents in case they have not been adopted.

Article 44
(Entry into Force)

These Guidelines shall enter into force on the date of their adoption.

Number: 16-03-02-1014-1/11
Istočno Sarajevo, 22 February 2011

H E A D O F D E P A R T M E N T

Dragan Mumović