NATIONAL BANK OF THE REPUBLIC OF NORTH MACEDONIA

Pursuant to Article 48 paragraph 1 item 3 of the Law on the National Bank (Official Gazette of the Republic of Macedonia No. 158/10, 123/12, 43/14, 153/15, 6/16 and 83/18), Article 10 paragraph 7 of the Law on Anti-Money Laundering and Combating the Financing of Terrorism (Official Gazette of the Republic of Macedonia No. 120/18), Article 68 paragraph 1 item 8 of the Banking Law (Official Gazette of the Republic of Macedonia No. 67/07, 90/09, 67/10, 26/13, 15/15, 153/15, 190/16, 7/19 and 101/19) and item 47 of the Decision on the Methodology for managing the risk of money laundering and terrorist financing (Official Gazette of the Republic of Macedonia No. 78/18 and 241/18), the Governor of the National Bank of the Republic of North Macedonia adopted the following

INSTRUCTIONS
for assessing the risk of money laundering and terrorist financing with banks, savings houses, fast money transfer service providers and licensed currency exchange operators
(Official Gazette of the Republic of North Macedonia No. 122/19)

I. GENERAL PROVISIONS

1. These Instructions set forth the method of assessing the risk of money laundering and terrorist financing with banks, savings houses, fast money transfer service providers, subagents and licensed currency exchange operators on which the National Bank of the Republic of North Macedonia (hereinafter: "the National Bank") conducts inspection of the implementation of the measures and actions determined by the Law on Anti-Money Laundering and Combating the Financing of Terrorism (Official Gazette of the Republic of Macedonia No. 120/18) (hereinafter: "the Law on AMLCFT").

2. The main objectives of these Instructions shall be:
- to contribute to a single understanding of the risk-based approach at a level of an entity;
- to help each entity separately in defining the risk profile at a level of an entity in order to take measures and actions proportionate to the nature, the size and the complexity of the activities it performs;
- to help each entity to channel the resources and activities of the entity in the area of anti-money laundering and combating the financing of terrorism (hereinafter: "ML/FT") appropriately to the identified threats, weaknesses and conclusions determined by the National Assessment of the Risk of Money Laundering and Financing of Terrorism, in order to support the implementation of the National Strategy for Combat against Money Laundering and Financing of Terrorism.

3. The terms used in these Instructions shall denote the following:

3.1. "Entity" shall denote a bank, a savings house, a fast money transfer service provider, a subagent and a licensed currency exchange operator.

3.2. "National Bank regulation" shall denote the Decision on good corporate governance rules for banks (Official Gazette of the Republic of Macedonia No. 24/18 and 113/19), the Decision on the risk management (Official Gazette of the Republic of Macedonia No. 42/11, 165/12 and 113/19) and the Decision on the Methodology for managing the risk of money laundering

and terrorist financing (Official Gazette of the Republic of Macedonia No. 78/18 and 241/18).

3.3. "Risk assessment" shall denote a process where the entity, by using risk factors, determines the inherent risk level at a level of an entity.

3.4. "Risk factors" shall denote the factors on the basis of which one can assess the risk of ML/FT at a level of an entity, such as types of clients, products/services/transactions, distribution channels and geographical locations.

3.5. "Threats in the context of ML/FT" shall denote sources of the inherent risk by individual risk factor at a level of an entity.

3.6. "Vulnerability in the context of ML/FT" shall denote the quality of internal regulations (policies and procedures), the activities of the authorized person/department and of the Internal Audit Department at a level of an entity in order to prevent or reduce the threats of ML/FT.

Issues not defined by these Instructions shall be regulated by the meaning of the terms determined by the Law on AMLCFT, the Decision on the Methodology for managing the risk of money laundering and terrorist financing (Official Gazette of the Republic of Macedonia No. 78/18 and 241/18) (hereinafter: "the Decision on AMLCFT") and the instructions for assessing the risk adopted pursuant to Article 146 paragraph 1 of the Law on AMLCFT for the entities that are subject to these Instructions.

4. The entity shall be obliged to use a risk-based approach when assessing the risk of money laundering and terrorist financing at a level of an entity.

5. The entity shall include the results of the conducted risk assessment in the policies, procedures and other internal regulations.

6. In carrying out the risk assessment, the entity shall undertake the following activities:

- document its risk assessment;
- take into account all risk factors before determining the risk level and the types of measures that should be implemented in order to mitigate the identified risk;
- update the risk assessment at least once a year;
- establish mechanisms for adequate recordkeeping and
- give an explanation for the conducted risk assessment at the request of the authorities of the entity.

II. RISK FACTORS

7. When identifying the risks of money laundering and terrorist financing, the entity shall take into account the following risk factors:

- client;
- countries or geographical locations;
- products, services or transactions;
- distribution channels.

8. The entity shall determine the data that it will use for each risk factor.

For the purposes of paragraph 1 of this item, the entity shall take into account the following data sources:

- the national assessments of the risk of ML/FT of the country and other countries;
- instructions, circulars and information issued by the competent authorities in the country, as well as imposed corrective measures and misdemeanors, if they are publicly available;

- reports on threats, warnings and typologies and other information issued by the Financial Intelligence Office and other government authorities competent for criminal prosecution;
- information obtained from due diligence of the client/s;
- own knowledge and professional experience;
- information from the associations or the chambers to which the entity belongs in relation to typologies and information about the risks that arise;
- information from reports of international bodies in charge of establishing standards for prevention of ML/FT or lists of sanctions and
- information from secure databases.

9. By adopting an internal regulation, the entity shall prescribe the risk factors and the manner of carrying out a risk assessment.

10. In assessing the risk of occasional transactions, the entity shall not be obliged to identify all the risk factors prescribed by these Instructions, but only those that are relevant to the particular transaction.

11. By adopting an internal regulation, the entity shall prescribe the keeping of records and the recording of the risk assessment and all the changes in the assessment of the risk of ML/FT.

III. Matrix for assessment of the risk of ML/FT at a level of an entity

12. When determining the importance of the risk factors, the entity shall provide data on individual elements within each risk factor that need to be analyzed according to the guidelines given in these Instructions, and are typical for the specific entity.

The entity shall determine the risk level by individual element, using certain variables, such as: data on the number of clients, the number of accounts, balance on the account at the end of a certain period, the number of transactions, the average transaction value, etc.

These variables shall determine the risk level by element, and then all the elements taken into account by individual factor (client, product/service/transaction, distribution channels and geographical locations) shall determine the risk level by factor.

The entity shall determine the vulnerability by element and by factor based on the vulnerability criteria defined in these Instructions and in the matrix given in Annex 1 which is an integral part of these Instructions.

Taking into account the type and volume of threats (identified inherent risk) and the level of vulnerability of the sector arising from the adequacy of the setup of the internal control systems, the entity shall be obliged to determine the level of residual (aggregate) risk and to appropriately allocate the resources necessary for combat with money laundering and financing of terrorism.

The entity needs to be sure that the assigned risk assessment reflects its understanding of the risk of ML/FT. At the request of the National Bank, the entity shall explain the risk assessment.

IV. RULES APPLICABLE TO BANKS

Risk factors that refer to the client

13. When identifying the risk associated with the client, the bank shall take into account the risks associated with the activity or professional activity of the client, his/her/its reputation, as well as the nature of his/her/its behavior.

14. The risk factors related to the activity or professional activity of the client that the bank analyzes shall be the following:

- whether the client is associated with activities or activities that are exposed to a greater risk of corruption, such as: construction, pharmacy, health, arms trade, defense, mining industry or public procurements;
- whether the client is associated with activities or activities that are exposed to a greater risk of ML/FT, such as: money transfer, organizers of games of chance or trade in precious metals;
- whether the client is associated with activities or activities that involve significant amounts of cash as part of the regular operations (such as: restaurants, gas stations, licensed currency exchange operators, organizers of games of chance, etc.);
- whether the client trades in goods and services with great value (cars, art works, oil, precious metals, etc.) or value whose amount is difficult to estimate (software, consulting services, market research, etc.);
- whether the client is a legal entity, what the purpose of its establishment is and what its activity is;
- whether the client and its beneficial owner are politically exposed persons or are close associates with politically exposed persons;
- whether the client is a legal entity with a disproportionately small number of employees in terms of the volume of activities and the activity they perform;
- whether the client is a legal entity that is required to disclose data which provide publicly available information about the beneficial owner of the client (such as: joint stock company whose shares are traded on a regulated market);
- whether the client is a bank or another type of financial institution operating in a country that has no efficient system for prevention of ML/FT and that is not subject to supervision in terms of the obligation for anti-money laundering and combating the financing of terrorism and
- whether the client is a bank or financial institution against which sanctions or other measures have been imposed by a competent authority in the past 5 years due to non-fulfillment of the obligations for prevention of ML/FT.

15. The risk factors related to the client's reputation that the bank analyzes shall be the following:

- whether there are negative reports from credible and reliable media or other sources of information about the the client, such as facts about crimes or links with terrorism or financing of terrorism. These facts do not require the adoption of an effective court decision;
- whether due to administrative or criminal proceedings or facts about terrorist activity or financing of terrorism, the assets of the client, its beneficial owner or of any person for whom it is known that he/she is closely related thereto, have been frozen or the bank has grounds for suspicion that the assets of the client are frozen;
- whether the bank has other negative information about the integrity of the client and its beneficial owner, which were obtained by the bank during the business relation.

16. The bank shall bear in mind that some of the risk factors related to the nature and behavior of the client or its beneficial owner can not be determined when establishing the business relation, i.e. they may arise once the business relation is established.

17. Risk factors related to the nature and behavior of the client that are analyzed by the bank shall be the following:

- whether the client has a complex ownership structure (more than two levels of legal entities in the ownership chain);
- whether the client issues bearer shares or has nominee shareholders;
- whether the ownership or management structure of the client changed more than three times in the last three years;
- whether there are frequent notifications (alert) on the client, indicating an existence of complex and unusual transactions;

- whether the client carries out transactions below the thresholds referred to in Article 12 paragraph (1) indent b) and c) and Article 52 of the Law on AMLCFT;
- whether the provided information about the source of wealth or the source of funds of the client is typical of that type of natural persons (such as: salary, inheritance, loans) or legal entities (such as: inflows are related to the client's activity).

Risk factors that refer to the country or geographical locations

18. When identifying the risk that relates to the country or geographical locations, the bank shall take into account the risks associated with the head office/residence of the client, his/her/its activity/profession, the purpose and nature of the business relation, the effectiveness of the system for prevention of ML/FT and the level of transparency and tax discipline of the country in which the client and its beneficial owner have their own head office/residence.

19. When identifying the risk associated with the countries and geographical locations, the bank shall analyze the risks associated with the countries and geographical locations in which the client and its beneficial owner:
- have their own head office or residence;
- have a geographical location where they predominantly perform their activity;
- have significant business activities.

20. In assessing the geographical risk, the bank shall take into account the nature and purpose of the business relation of the client, such as:
- when it comes to transactions with high-risk countries or countries in which terrorist groups act;
- when the bank's client is another bank, the bank shall analyze the appropriateness of the system for prevention of ML/FT in the country in which this client has a head office;
- when the client is a legal entity, the entity shall analyze the degree of meeting the international standards for tax transparency in the country where the client and its beneficial owner are registered/have their own residence (such as: the list of the OECD, etc.);
- the beneficial owner of the client has his/her own residence in a high-risk country (offshore state, tax haven, state under sanctions);
- whether the client is a state body or legal entity from a country with a low level of corruption (such as: according to the index of Transparency International).

21. The sources of information for determining the effectiveness of the system for prevention of ML/FT in a particular country shall include the following: high-risk countries determined by the National Assessment of Risk of ML/FT of the Republic of North Macedonia, the assessment reports of the FATF or other regional bodies similar to the FATF; the FATF list for high-risk countries, etc.

22. The sources of information that the bank takes into account when determining the level of risk of financing of terrorism related to a particular country shall be the following:
- existence of information from bodies competent for criminal prosecution or other information from independent media that that country finances or supports terrorist activity or it is generally known that terrorist organizations act within that country or territory and
- whether that country is subject to international restrictive measures related to money laundering, terrorism, financing of terrorism or armaments established by the UN or the European Union.

23. The sources of information that the bank analyzes when determining the level of transparency and tax discipline of the countries shall be the following:

- information from more reliable sources that the country is complied with the international tax standards for transparency and exchange of information, as well as evidence that these rules are properly applied in practice;
- the notifications from the Global Forum on Transparency and Exchange of Information for Tax Purposes of the OECD where the countries are assessed for the purposes of tax transparency and exchange of information; assessment of the compliance with the recommendations of the FATF or of the regional bodies within the FATF, as well as the assessments of the International Monetary Fund;
- whether the country has established registries for a beneficial owner for the needs of the entities and state bodies.

Risk factors that refer to products, services or transactions offered by the bank

24. The risk factors that the bank analyzes when identifying the risks associated with products, services or transactions shall be the following:
- the degree of anonymity of products, services or transactions;
- the complexity of products, services or transactions;
- the value or scope of products, services or transactions.

25. A risk factor that the bank analyzes when identifying the risks associated with the anonymity of a particular product, service or transaction is the extent to which a product or service ensures anonymity or facilitates the concealment of the identity of the client or beneficial owner (such as: anonymous accounts, virtual assets, etc.)

26. The risk factors that the bank analyzes when identifying the risks associated with the complexity of a particular product, service or transaction shall be the following:
- the degree of complexity of a particular transaction and involvement of multiple clients or countries;
- whether the bank has knowledge of the risks when launching a new or innovative product or service, especially when it involves using new technologies or payment methods (such as: to take into account the requirements in this section according to the National Bank regulation).

27. The risk factors that the bank analyzes when identifying the risk associated with the value or size of a particular product, service or transaction shall be the following:
- the extent to which products or services enable using cash;
- the extent to which products or services facilitate or encourage the high value transactions;
- existence of certain limitations in terms of the maximum value of the transaction or of the price of the service which would limit the use of products or services for the purposes of ML/FT.

Risk factors that refer to distribution channels

28. When identifying the risk associated with the manner in which products or services are delivered to the client, the bank shall analyze the risk in situations when the client is not physically present when delivering a particular product or service, as well as the nature of the business relation between the intermediary and the entity.

29. Risk factors that are considered when identifying the risks associated with the distribution channels shall be the following:
- presence of the client during the identification;
- application of new technologies such as: m-commerce; using virtual assets, for example bitcoin (based on the method of consecutive execution of transactions); payment over the Internet - "PayPal", "Amazon Pay", "Google Wallet", etc.

30. When determining the vulnerability for banks one should take into account the requirements of the National Bank regulation.

V. RULES APPLICABLE TO FAST MONEY TRANSFER SERVICE PROVIDERS

31. The provisions of item 14 paragraph 1 indents 1, 2, 3, 4 and 6; item 15; item 17 paragraph 1 indents 4, 5 and 6; item 19 paragraph 1 indent 1; item 20 paragraph 1 indent 1; item 21; item 22, item 24 paragraph 1 indent 3 and item 27 of these Instructions that refer to natural persons shall be properly applied by the fast money transfer service provider in the area of executing occasional transactions and monitoring the business relation with the client.

32. When determining the vulnerability arising from the content of internal regulations (policies and procedures), one shall take into account:

- the procedures for identifying the natural person by prescribing the minimum documentation required for identifying the natural person in the moment of execution of the transaction;
- in the event when the fast money transfer service provider has a business relation with the client, whether the procedures include data that show whether the client's transactions are in accordance with the purpose of the business relation, the client's risk profile, his/her financial condition and his/her sources of financing (such as: profession of the client, employer, amount of the monthly salary, etc.).

33. The vulnerability arising from the activities of the authorized person/department for prevention of ML/FT shall include:

- identification and verification of the identity of the natural person by applying the standard documents for identification of natural persons specified by the Law on AMLCFT and verification of the identity of the natural person by using data and information from reliable and independent sources;
- permanent insight into the numbered register in order to determine the frequency of execution of transactions by a particular natural person, in order to require from him/her to submit additional documentation that will determine the purpose of execution of the transaction and its economic justification;
- client due diligence (in case of an existence of a business relation or in case of an occurrence of suspiciousness indicators) by gathering information on his/her profession, the source of his/her assets, the economic justification of the executed transaction, etc.;
- The Financial Intelligence Office shall be notified of suspicious transactions in a manner and deadlines specified by the Law on AMLCFT. The notification on suspicious transactions shall be documented, appropriately elaborated and supported by the indicators for identifying suspicious transactions adopted by the Financial Intelligence Office.

34. The vulnerability arising from the internal control systems shall include the following:

- in the event when the natural person is a politically exposed person, the fast money transfer service provider shall take the measures of enhanced due diligence specified by the Law on AMLCFT and shall assign a high risk level to the natural person;
- in the event when the natural person has residence in a high-risk country, the fast money transfer service provider shall take the measures of enhanced due diligence specified by the Law on AMLCFT and shall assign a high risk level to the natural person;
- in the event when the natural person carries out transactions with a high-risk country, the fast money transfer service provider shall take the measures of enhanced due diligence specified by the Law on AMLCFT and shall assign a high risk level to the natural person;
- implementation of the financial restrictive measures pursuant to the regulations that regulate the international restrictive measures;

- the training of staff shall be adequate to the nature of the activity of the fast money transfer service provider, adjusted to the type of clients and contain all the relevant provisions of the Law on AMLCFT and bylaws that regulate this matter.
- the Internal Audit Department shall analyze and test the adequacy of written policies and procedures; select a sample of clients, thus testing the appropriateness of the due diligence of the clients and their risk profile, as well as the submission of reports to the Financial Intelligence Office; reporting to the bodies of the fast money transfer service provider on the findings of the controls, etc.

VI. RULES APPLICABLE TO LICENSED CURRENCY EXCHANGE OPERATORS

35. The provisions of item 14 paragraph 1 indents 1, 2, 3, 4 and 6; item 15; item 17 paragraph 1 indents 4, 5 and 6; item 19 paragraph 1 indent 1; item 21; item 22, item 24 paragraph 1 indent 3 and item 27 of these Instructions that refer to natural persons/clients shall be properly applied by the licensed currency exchange operator in the area of executing occasional transactions and monitoring the business relation with the client.

36. When determining the vulnerability arising from the content of internal regulations (policies and procedures), one shall take into account:
- the procedures for identifying the natural person by prescribing the minimum documentation required for identifying the natural person in the moment of execution of the transaction;
- in the event when the licensed currency exchange operator has a business relation with the client, the procedures shall include an appropriate type of data that show whether the client's transactions are in accordance with the purpose of the business relation, the client's risk profile, his/her financial condition and his/her sources of financing (such as: the profession of the client, the employer, the amount of the monthly salary, etc.).

37. The vulnerability arising from the activities of the person authorized for prevention of ML/FT shall include:
- identification and verification of the identity of the natural person by applying the standard documents for identification of natural persons specified by the Law on AMLCFT and verification of the identity of the natural person by using data and information from reliable and independent sources;
- permanent insight into the numbered register in order to determine the frequency of execution of transactions by a particular natural person, in order to require from him/her to submit additional documentation that will determine the purpose of execution of the transaction and its economic justification;
- client due diligence (in case of an existence of a business relation or in case of an occurrence of suspiciousness indicators) by gathering information on his/her profession, the source of his/her assets, the economic justification of the executed transaction, etc.;
- The Financial Intelligence Office shall be notified of cash, obviously connected and suspicious transactions in a manner and deadlines specified by the Law on AMLCFT. The notification on suspicious transactions shall be documented, appropriately elaborated and supported by the indicators for identifying suspicious transactions adopted by the Financial Intelligence Office.

38. The vulnerability arising from the internal control systems shall include the following:
- in the event when the natural person is a politically exposed person, the licensed currency exchange operator shall take the measures of enhanced due diligence specified by the Law on AMLCFT and shall assign a high risk level to the natural person;
- in the event when the natural person has residence in a high-risk country, the licensed currency exchange operator shall take the measures of enhanced due diligence specified by the Law on AMLCFT and shall assign a high risk level to the natural person;

- implementation of the financial restrictive measures pursuant to the regulations that regulate the international restrictive measures;
- the training of staff shall be adequate to the nature of the activity of the licensed currency exchange operator, adjusted to the type of clients and contain all the relevant provisions of the Law on AMLCFT and bylaws that regulate this matter.
- the Internal Audit Department or the person authorized for internal audit shall analyze and test the adequacy of written policies and procedures; select a sample of clients, thus testing the appropriateness of the due diligence of the clients and their risk profile, as well as the submission of reports to the Financial Intelligence Office; reporting to the responsible person of the licensed currency exchange operator on the findings of the controls, etc.

VII. CLOSING PROVISIONS

39. The provisions of these Instructions that apply to banks shall also apply to savings houses.

Foreign bank branches shall properly apply the provisions of these Instructions, taking into account the provisions of the Banking Law governing the operation of foreign bank branches in the Republic of North Macedonia.

40. The provisions of these Instructions that apply to fast money transfer service providers shall also apply to subagents.

41. These Instructions shall enter into force on the eighth day from the day of their publication in the Official Gazette of the Republic of North Macedonia.

I. No. 17-19545/1
11 June 2019

Governor
Anita Angelovska Bezhoska

ANNEX 1

MATRIX FOR ASSESSMENT OF THE RISK OF MONEY LAUNDERING AND FINANCING OF TERRORISM

Matrix for assessment of the risk of ML/FT at a level of an entity										
Threats at a level of an entity						Vulnerability at a level of the entity				Residual/aggregate risk (threats in terms of vulnerability) by factors
Risk factors	**Elements in an individual factor**	**Variables 1**	**Risk level of each element**	**Variables 2**	**Risk level of each factor**	**Vulnerability variables by element at a level of the entity**	**Assessment of vulnerability variables by element**	**Vulnerability variables by risk factor at a level of the entity**	**Assessment of vulnerability variables by risk factor**	**Level of residual risk (low, medium and high)**
		number of clients; number of accounts; balance on the account at the end of a certain period; number of transactions; average transaction value, etc.	*4 and 5 high risk, 3 and 2 medium risk, 1 and 0 low risk*	*It uses the risk level assigned to the specific element in an individual risk factor in the National Risk Assessment*	*4 and 5 high risk, 3 and 2 medium risk, 1 and 0 low risk*	*(to take into account the relevance of each individual variable for a specific element)*	*(it is filled in with number 4 and 5 if the answer is "yes", it is filled in 2 and 3 if the answer is "there is room for improvement" or it is filled in 0 and 1 if the answer is "no")*	*(to take into account the relevance of each individual variable for the specific factor)*	*(it is filled in with number 4 and 5 if the answer is "yes", 0 and 1 if the answer is "no" or "there is room for improvement" if the answer is 2 and 3)*	*4 and 5 high risk, 3 and 2 medium risk, 1 and 0 low risk*
						Active role of the Supervisory Board and the Management Board in the process of anti-money laundering and combating the financing of terrorism		*Active role of the Supervisory Board and the Management Board in the process of anti-money laundering and combating the financing of terrorism*		
Clients						There is documented assessment of the risk of ML/FT		There is documented assessment of the risk of ML/FT		
	politically exposed persons					Adequate policies and procedures for prevention of ML/FT		Adequate policies and procedures for prevention of ML/FT		
	non-residents					Adequate due diligence of the client and his/her/its adequate risk profile		Adequate due diligence of the client and his/her/its adequate risk profile		
	non-profit organizations					Adequate monitoring of the business relation and transactions		Adequate monitoring of the business relation and transactions		
	legal entities					Recognizing unusual and suspicious transactions - submission of reports to the Financial Intelligence Office		Recognizing unusual and suspicious transactions - submission of reports to the Financial Intelligence Office		
Products/services/transactions						Adequate execution of the obligations of the authorized person/department for		Adequate execution of the obligations of the authorized person/department for		
	cash transactions					Adequate reporting to the bodies of the entity		Adequate reporting to the bodies of the entity		
	cashless transactions					Adequate training of staff		Adequate training of staff		
	loan secured by deposit					Adequate software for efficient prevention of ML/FT that enables adequate due diligence of clients and recordkeeping		Adequate software for efficient prevention of ML/FT that enables adequate due diligence of clients and recordkeeping		
	fast money transfer					Adequate recordkeeping, as well as speed and comprehensiveness of their finding		Adequate recordkeeping, as well as speed and comprehensiveness of their finding		
	m-commerce					Adequate execution of the obligations of the audit (internal and external)		Adequate execution of the obligations of the audit (internal and external)		
Distribution channels										
	without physical presence									
	with the help of an intermediary									
Country or geographical locations										
	lists of sanctions									
	lists of off-shore countries									
	lists of countries - tax havens									
									TOTAL AGGREGATE RISK AT A LEVEL OF AN ENTITY*	

* for each individual element and risk factor, the entity shall determine a weight/significance that will be included in the final aggregate assessment of the risk of ML/FT at a level of an entity according to a methodology prescribed by the internal regulations of the entity.