Regulation on requirements for prevention and combating money laundering and terrorist financing in the activity of banks No. 200 of 09 August, 2018

Note: *The translation is unofficial, for information purpose only*

The Executive Board of the National Bank of Moldova
DECIDES
on the approval of the Regulation on requirements for prevention and combating money laundering and terrorist financing in the activity of banks
no. 200 of 9 August 2018
(*in force as of 24.08.2018*)

Published in the Oficial Monitor of the Republic of Moldova no. 321-332 of 24.08.2018. art. 1311

REGISTERED
At the Ministry of Justice
Of the Republic of Moldova
no. 1354 of 21.08.2018

Pursuant to art. 11 par. (1), art. 27 par. (1) letter c) and art.44 letter a) and c) of the Law no. 548-XIII of 21 July 1995 on the National Bank of Moldova (republished in the Official Monitor of the Republic of Moldova, 2015, no. 297-300, art. 544) and 95 of the Law on banking activity no.202 of 6 October 2017 (Official Monitor of the Republic of Moldova, 2017, no. 434-439, art. 727) and art. 13 par. (3) and (14), art. 15 par. (2) of the Law no. 308 of 22 December 2017 on the Prevention and combating of money laundering and terrorist financing (Official Monitor of the Republic of Moldova, 2018, no. 58-66, art. 133), the Executive Board of the National Bank of Moldova

DECIDES:

1. To approve the Regulation on requirements for prevention and combating money laundering and terrorist financing in the activity of banks, in accordance with the attachment.

2. This decision shall enter into force at the date of publication in the Official Monitor of the Republic of Moldova.

Chairman
of the Executive Board
Sergiu CIOCLEA

Attachment
Approved by the Decision of the
Executive Board of the
National Bank of Moldova
no. 200 of 9 August 2018

REGULATION
on requirements for prevention and combating money laundering and terrorist financing in the activity of the banks

This Regulation partially transposes the (EU) Regulation No 2015/847 of the European Parliament and of the Council of 20 May 2015 on the information accompanying transfers of funds and repealing the Regulation (EC) No 1781/2006 (Text with EEA relevance), published in the Official Journal of the European Union L 141 of 5 June 2015.

Chapter I
GENERAL PROVISIONS

1. The Regulation on requirements for prevention and combating money laundering and terrorist financing in the activity of banks (hereinafter - Regulation) establishes requirements for: identification and assessment by banks of the risks associated with money laundering and terrorist financing; application of provisions on customer due diligence (CDD), including simplified and enhanced CDD measures; reporting suspicious activities and transactions; data storage; application of financial sanctions related to terrorist activities and the proliferation of weapons of mass destruction as well as for putting in place and implementation of the elements related to the internal control system.

2. All banks, including their branches in foreign countries, shall apply the provisions of this Regulation in business relations with their customers or when conducting transactions and bank operations.

3. The terms and expressions used in this Regulation shall have the meanings provided in the Law nr. 202 of 06 October 2017 on Banks' activity, the Law no. 308 of 22 December 2017 on the Prevention and combating money laundering and terrorist financing, the Law no. 114 of 18 May 2012 on the Payment services and electronic money, the regulatory acts of the National Bank of Moldova and of the Office for the Prevention and Fight against Money Laundering, which were issued in the application of the provisions for prevention and combating money laundering and terrorist financing. In addition, for the purposes of this Regulation, the following terms and expressions shall be used:
significant transaction shall mean a transaction (bank operation) that exceeds the value limit set in the Bank's internal policies, taking into account the risks associated with the customers and the transactions performed;
electronic means shall mean all electronic devices used for processing (including digital compression), storage and transmission of data, by wires, optical radio technologies or any other electromagnetic device (eg. computer, ATM, cash terminals, mobile phone, etc.).
transfer of funds shall mean any transaction made, at least in part, by using electronic equipment on behalf of a payer through a payment service provider, to provide funds to the payee through a payment service provider, regardless of whether the payer and the payee is the same person and regardless of whether the payer and the payee's payment service providers are the same person, including such transaction as: loan transfers, direct debiting, money transfers and payments made by using payment cards;
legal entity identifier shall mean a 20-character alphanumeric code that uniquely identifies a legal entity and is developed in accordance with ISO Standard 17442;
batch funds transfer shall mean multiple transfers of funds made by a single payer to several payees, which form a group (batch) for the purpose of that transfer;
batch file shall mean a text file containing a sequence of commands for a computer operating

system;
payable-through accounts shall mean a bank service, which allows the customers of a foreign correspondent bank to use directly their correspondent accounts opened for the purpose of conducting direct transactions on their behalf;
international organizations shall mean entities established through formal political agreements signed between Member States that have the status of international treaties, their existence being recognized by law in the member countries, which are not treated as resident institutional units of the countries in which they are located (example: United Nations Organization, The Council of Europe, the OSCE, etc.)

Chapter II
RESPONSIBILITIES

4. The Bank shall have in place and implement an effective internal programme on the prevention and combating of money laundering and terrorist financing.

5. The Bank shall have in place an adequate internal control system to identify, assess, monitor and understand the risks of money laundering and terrorist financing. The Bank shall apply all necessary measures and use sufficient resources to minimize the identified risks.

6. The Board of the Bank shall be responsible for, approving and ensuring the implementation of the internal programme on the prevention and combating of money laundering and terrorist financing. The Executive organ of the Bank shall be responsible for the effective implementation of the programme on the prevention and combating of money laundering and terrorist financing.

7. The Bank shall appoint persons, including members of the Board of the Bank/ or the Executive organ of the Bank entrusted with responsibilities to comply with those requirements with regard to the prevention and combating money laundering and terrorist financing.

8. The Internal Audit subdivision of the Bank shall perform, at least annually, an independent assessment of the adequacy and compliance of the Bank's activity with the Programme on prevention of money laundering and terrorist financing, taking into account the provisions of item 93 sub-item 1) specified hereto. The Bank, by decision of the Board of the Bank or at the request of the authorities with supervisory functions shall designate an audit firm/ external auditor to perform an assessment of the adequacy and compliance of the Bank’s activity with the prevention and combating of money laundering and terrorist financing program considering the provisions of item 93 sub-item 1) and the criteria established at the request of the National Bank of Moldova. The results of the assessment shall be communicated to the Board and the Executive organ of the Bank, whereas the Bank shall inform the National Bank of Moldova on the assessment’s outcomes in accordance with the Guidelines on the preparation and presentation of banks’ reports for prudential purposes, approved by the Decision of the Board of Administration of the National Bank of Moldova no.279 of 1 December 2011 (Official Monitor of the Republic of Moldova, 2011, no. 216-221, art. 2008), with subsequent amendments and completions.

Chapter III
REQUIREMENTS REGARDING THE INTERNAL PROGRAMME ON THE PREVENTION AND COMBATING OF MONEY LAUNDERING AND TERRORIST FINANCING

9. The internal programme on the prevention and combating of money laundering and terrorist financing represents a series of policies, procedures and internal controls including the customer due

diligence procedures, promoting ethical and professional standards in the banking sector, that aim to prevent organized criminal groups or their associates from using the bank for money laundering or terrorist financing purposes. This programme must ensure that banking operations are carried out in a safe and prudent way.

10. The Bank shall draw up the internal programme on the prevention and combating of money laundering and terrorist financing in accordance with the provisions of the Law no.308 of 22 December, 2017 on the Prevention and combating of money laundering and terrorist financing, the present Regulation, other regulatory acts of the Office for Prevention and Fight against Money Laundering, issued in the application of this law, taking into account the generally-accepted practices in the domain, including the documents issued by the Basel Committee and the international Financial Action Task Force (FATF).

11. The internal programme shall take into account the size, complexity, nature and volume of the bank's activities, the identified risks of money laundering and terrorism financing, the types (categories) of customers, the products and services rendered, the geographical area covered by the Bank, the degree (level) of risk associated with customers and/or with the transactions (operations) performed by them.

12. Internal programme on the prevention and combating of money laundering and terrorist financing shall include, without being limited to, the following:
1) the responsibilities of the bank's executive and supervisory board, which shall include at least:
a) determination of the Bank's areas of activity exposed to the risk of money laundering and terrorist financing, with a precise delimitation of the competences of each subdivision responsible for the prevention and combating of money laundering and terrorist financing. Areas of activity exposed to the risk of money laundering and terrorist financing may be those related to: acceptance of deposits, loans granting/repayment operations, international payments (transfers), use of payment instruments, correspondent bank operations, private banking services, the accounts opened by professional intermediaries for the provision of mediation services, automated remote service systems, money remittance systems, alternative trade financing operations (letters of credit, bond issuance, etc.), brokerage, trust management, etc.;
b) determination of the mechanism for identifying, evaluating and taking actions to control and minimize the risks of money laundering and terrorist financing;
c) development of necessary measures to implement customer due diligence policies and procedures, including for high-risk customers;
d) allocation of sufficient resources for the effective performance of activities aiming to prevent and combat money laundering and terrorist financing;
e) appointment of persons responsible for the application of the provisions of the Law no. 308 of 22 December 2017 on the Prevention and combating of money laundering and terrorist financing;
f) determination of the lines of responsibilities of the Bank's staff at different hierarchical levels;
g) granting, within reasonable time limits, to the responsible persons, appointed in accordance with the provisions of letter e), of access to the information required for the application of provisions of the Law no. 308 of 22 December 2017 on Prevention and combating money laundering and terrorist financing and of this Regulation;
h) address the deficiencies identified in the field of the prevention and combating of money laundering and terrorist financing;
2) procedures for identifying, assessing, controlling and undertaking measures to minimize the risk of money laundering and terrorist financing;
3) customer acceptance procedures that describe at least the categories of customers whom the Bank

intends to attract as well as the staff levels that shall be authorized to approve the initiation of a business relationship with such customers, depending on the degree of associated risk and the types of products and services that are to be provided to them;
4) methods to be used to identify, verify and monitor customers and beneficial owners according to the degree of associated risk (CDD procedures), the criteria and the procedure of moving customers from one risk category to another;
5) CDD measures to be developed for each category of customers, products, services or transactions (operations) performed;
6) the procedures to be applied to monitor customer transactions for detecting significant, complex and unusual transactions, or suspicious activities and transactions;
7) the procedures and requirements set for the application of simplified customer/transaction due diligence measures when, by their very nature, they may present a lower-level risk of money laundering and terrorist financing, including risk management measures in case of establishing the business relationship until the verification of the identity of the client and the beneficial owner
8) the procedures and requirements set for the application of enhanced CDD measures in the cases of complex and unusual transactions performed without a clear legal or economic purpose, as well as significant and suspicious transactions;
9) the procedures describing the collection and storage of information as well as the conditions of granting access to them;
10) the procedures describing the internal and external (to competent authorities) reporting on suspicious activities and transactions;
11) the procedures and measures aiming to ascertain compliance with relevant standards and to assess their effectiveness;
12) the standards developed for the personnel's recruitment, employment and training programmes in the CDD field;
13) the procedures for identifying and analyzing the risks of money laundering and terrorist financing, including the measures to minimize them, by using information technologies, including modern ones, procured or developed within the Bank's products or services.

13. Whenever required, but at least annually, the Bank shall review (update) its internal programme on prevention and combating money laundering and terrorist financing, taking into account relevant legal provisions in force.
[Item 12 completed by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]

Chapter IV
ASSESSMENT OF THE RISKS OF MONEY LAUNDERING AND TERRORIST FINANCING. THE RISK-BASED APPROACH

14. The Bank shall be responsible to identify and evaluate the existing risk exposure to money laundering and terrorist financing, taking into account the threats and vulnerabilities identified in the national, regional and sectoral evaluation reports, as well as the criteria and risk factors elaborated for that purpose by the National Bank of Moldova and the Office for the Prevention and Fight against Money Laundering. The results of the assessment shall be approved by the designated person who is responsible for ensuring the compliance of the Bank's policies and procedures with the legal requirements established for the prevention and combating of money laundering and terrorist financing, and shall be presented to the Board of the Bank.

15. For the purpose of implementing item 14 the Bank shall evaluate the risks of money laundering and terrorism financing in its own area of activity which shall include at least:
1) preparation of a written report describing the countries or geographical areas, products, customers and transactions (bank operations) presenting a high degree of risk, their share and impact on the

Bank's activity;
2) drawing up of an action plan aiming to minimize the identified risks of money laundering and terrorist financing;
The Bank shall update the assessment under this item after each national risk assessment carried out by the Office for Prevention and Fight against Money Laundering and each update of the criteria and risk factors established by the National Bank of Moldova and the Office for Prevention and Fight against Money Laundering.

16. The Bank shall identify and assess existing risks of money laundering and terrorist financing before:
1) it develops and launches new products and services;
2) it starts using new or developing technologies for both new and existing products and services.

17. While assessing its risk exposure to money laundering and terrorist financing, the Bank shall analyze different elements and characteristics of available variables, such as: the destination of the account, the purpose of the business relationship, the volume of transacted assets or the number of transactions conducted, the frequency and duration of a business relationship, etc.

18. Following the assessment of its risk exposure to money laundering and terrorist financing, the Bank shall use the risk-based approach to determine and implement actions plan aiming to manage and minimize the identified risks, including through the allocation of appropriate technological, material and human resources.

19. In accordance with the requirements of the internal programme, the Bank shall retain and update statistical data, required to identify and assess the risk exposure to money laundering and terrorist financing.

20. The Bank shall apply simplified and enhanced CDD measures based on the degree of risk identified, taking into account the type of the customer, the identified degree of risk exposure to money laundering and terrorist financing, the country (jurisdiction), the type of business relationship, the product / service provided or the transaction performed, the distribution network, etc.

Chapter V
CUSTOMER DUE DILIGENCE MEASURES

Section 1

Customer acceptance procedures

21. The customer acceptance procedures will contain provisions on customers who appear to expose the Bank to an increased risk of money laundering and terrorist financing. In order to minimize this risk, the customer information should be examined under a number of aspects, such as: the customer’s business experience, the country of origin, the activities run by the customer or other risk indicators set by the bank, taking into account the recommendations of the National Bank of Moldova on the implementation of the risk-based approach. .
[Item 21 amended by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]

22. The customer acceptance procedures will include several steps depending on the degree of the risk associated with each customer. The decision to start, continue or terminate a business relationship with a customer who is associated with an increased degree of risk shall be taken by the Bank’s designated responsible person or by the senior manager of a branch, by coordinating the

decision with the Bank's internal subdivision responsible for the implementation and compliance with the requirements for the prevention and combating of money laundering and terrorist financing.

23. The Bank shall not enter into business relations with persons, groups or entities involved in terrorist activities and proliferation of weapons of mass destruction, specified in art. 34 sec. (11) of the Law No 308 of 22 December 2017 on the prevention and combating of money laundering and terrorist financing. The Bank shall communicate immediately, but not later than within 24 hours, to the Office for the Prevention and Fight against Money Laundering its decision to refuse entering into business relationship with a customer, providing all supporting data.

24. The customer acceptance procedures should not hinder the public's access to banking services.

Section 2

Establishing the identity of the customer and the beneficial owner

25. The Bank shall take steps to establish the identity of the customer and the beneficial owner:
1) before it enters into a business relationship with the customer;
2) in the case of all occasional transactions, including those carried out by means of electronic equipment exceeding 20000 MDL, if the money transfer is performed in a single transaction, or in a series of transactions that appear to be linked if their value exceeds 300000 MDL;
3) when there is a suspicion of money laundering or terrorist financing, regardless of any applicable derogation, exemption or threshold;
4) when there are suspicions regarding the veracity, sufficiency and accuracy of the previously obtained customer identification data;
5) by way of derogation from sub-item 2), any currency exchange transaction conducted in cash, with a value exceeding 200000 MDL (according to the official exchange rate of the Moldovan leu against a respective foreign currency, applicable at the date of the currency exchange transaction) shall be carried out only against identity documents presented by a customer, the details of which should be recorded by the Bank;
6) by way of derogation from sub-items 1) and 2) hereto, based on a proper risk assessment demonstrating a low-level risk of money laundering and terrorist financing, the Bank as a payment service provider and issuer of electronic money under the Law no. 114 of 18 May 2012 on Payment services and electronic money, except for cases of redemption or withdrawal of cash exceeding the amount of 2000 MDL, may be exempted from the application of CDD measures, where electronic money or the prepaid payment instrument is used, provided the following conditions are met:
a) the maximum amount of electronic deposit does not exceed 5000 MDL;
b) the amount of monthly transfers does not exceed 5000 MDL; in the case of payment instruments that can be used only on the territory of the Republic of Moldova, the threshold can be increased up to 10000 MDL;
c) the payment instrument is used exclusively for the payment of goods or services;
d) the payment instrument cannot be funded with anonymous electronic money (which cannot be attributed to an identified person);
e) the issuer (bank) regularly monitors the transactions or the business relationship to enable the detection of suspicious transactions.

26. While performing customer identification as laid down in item 25, the Bank shall obtain at least the following information:
1) when dealing with a customer who is a natural person:
a) a customer's full name;
b) the date and place of birth;
c) citizenship and the ID card data (IDNP, series and number, date of issue, code of the issuing body

(if any) or other unique elements of an identity document containing the holder's photograph);
d) permanent and/or residence address;
e) the occupation, a public office held;
f) the source of income;
g) the intended use of the account (the number and volume of transactions, the type of transactions, the purpose and frequency of intended transactions);
h) the financial product and service requested;
2) when dealing with a customer who is a legal person or an individual entrepreneur:
a) the name, the legal form of organization, the articles of incorporation and the act on the state registration of the legal person;
b) the head office / business address;
c) the state identification number (IDNO) and the Taxpayer Identification Number, according to the registration certificate and / or the extract from the State Register issued by the competent authority with the right to carry out the state registration;
d) the mailing address other than headquarters (if any);
e) the identity of the natural person empowered to manage the account, the legality of the powers of attorney (in the absence of such a person, the administrator of the legal entity is indicated);;
f) the identity of the beneficial owner of the legal entity;
f)[1] the identity of the persons holding senior management positions, as well as their powers of representation;
g) the rights and obligations of the management body of the company arising from the primary registration documents or its constitutive act;
h) the nature and the purpose of the activity, their legitimacy;
i) the intended use of the account (the number and volume of transactions, the type of transactions, the purpose and frequency of intended transactions);
3) when dealing with customers who are persons providing fiduciary asset management services (trusts, investment funds, etc.):
a) the name and the proof of incorporation / registration, the fiduciary deed;
b) the headquarters / business address and the country of registration;
c) the nature, purpose and object of the activity (as an example: discretionary, testamentary, etc.);
d) the identity of the founder, administrator, protector (if any), beneficiaries or classes of beneficiaries and any other person who ultimately exercises effective control (in the case of other types of legal constructions similar to trusts - the identity of persons holding equivalent positions);
e) the description of the purpose / activity;
f) the intended use of the account (the number and volume of transactions, the type of transactions, the purpose and frequency of intended transactions);
[Item 26 amended by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]

27. While performing identification of high-risk customers, the Bank shall obtain the following additional information:
1) when dealing with natural persons:
a) any other name used (the married name, previously-held name or nickname);
b) business address, postal code, email address, mobile phone number;
c) the status of resident / non-resident;
d) gender;
e) the name of the employer, if any;
f) the information on the source of the customer's wealth;
g) the information on the source of funds that pass through the account and their destination;

2) when dealing with legal persons and individual entrepreneurs:
a) unique company identifier, if any;
b) telephone and fax numbers;
*[Letter c) repealed by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]*d) the financial situation;
e) the source of money received in the account and the destination of money that pass through the account.
3) when dealing with entities providing fiduciary asset management services (trust, investment fund, etc.):
a) telephone and fax numbers;
[Letter b) repealed by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]
c) the source of funds;
d) the destination of funds that pass through the account.
[Item 27 amended by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]

28. In the case of cash currency exchange transactions carried out by individuals through the banks' foreign exchange bureaux and / or currency exchange machines, the bank shall apply CDD measures, including enhanced CDD measures, in accordance with the provisions of Chapters III and IV of the Regulation on the activity of foreign exchange offices and hotels in the field of the prevention and combating of money laundering and terrorist financing.

29. The Bank shall identify the customer's beneficial owner and apply reasonable risk-based measures to verify his identity, using documents, information and data obtained from secure source, to be sure that it knows the ultimate beneficial owner and understands the property and control structures of the customer. In order to identify the beneficial owner, the bank shall collect information specified in item 26 sub-item 1) (a)-(f) and, additionally, depending on the risk identified, in item 27 sub-item 1) (a)-(f).
[Item 29 amended by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]

30. When identifying the beneficial owner for the customer who is a legal person, including entities with complex ownership structure (a legal person whose direct owners are not natural persons), the Bank shall determine the beneficial owner on the basis of the appropriate registration documents. If there are no grounds for suspicion regarding the concealment of the information on the beneficial owner and if after exhausting all possible measures specified in item 29, it is found that no person meets the legal conditions to be identified as the beneficial owner (no natural person is a majority shareholder or exercises direct or indirect control in other ways), as an exception, the natural person holding the position of administrator of the client is considered the beneficial owner.

In this latter case, the bank keeps all the information and documents accumulated while determining beneficial owner's legal status and presents them, upon request, to the Office for Prevention and Fight against Money Laundering and/ or the authorities with supervisory functions. When identifying the beneficial owner, the Bank shall take into account the identification criteria described in the Attachment.
[Item 30 amended by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]

31. When the client or holder of the controlling interests is a company whose securities are traded on a regulated market / multilateral trading system that imposes disclosure requirements, either by stock exchange rules or by applicable law, to ensure adequate transparency of to the beneficial owner, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any of the shareholders or beneficial owners of such companies. The bank

obtains the relevant identification data from public registers, from the client or from other reliable sources.

[Item.31 in the wording of the NBM Decision no.38 of 11.03.2021, in force 02.07.2021]

32. The Bank shall determine whether the natural or legal person who opens the payment account or initiates a business relationship acts on his behalf (the person's statement of the beneficial owner) and, where an account is opened or a business relationship is initiated by the authorized representative, the Bank shall request the Power of Attorney to be submitted, certified in the manner prescribed by the law. The Bank shall apply CDD measures to establish the identity of the authorized representative in accordance with the provisions of this Regulation. The statement of the person regarding the beneficial owner shall be completed by the beneficial owner or by his authorized representative and shall contain information specified under item 26 sub-item 1) (a)-(f) and, additionally, depending on the risk identified, in item 27 sub-item 1) (a)-(f) of this Regulation.

33. When performing the customer identification, the Bank shall verify the submitted information that relates to both the customer and the beneficial owner.

34. The Bank shall verify the identity of the customer and his beneficial owner prior to establishing a business relationship with the customer or at the moment of establishing such business relationship or conducting a transaction specified in item 25 sub-item2) or, in the case of a low level of risk, in accordance with item 51, sub-item1) of this Regulation.

35. In order to verify the identification information provided for the customers and the beneficial owners, the Bank shall use documents, data and information obtained from reliable and independent sources. Verification effort must be proportionate to the risk associated with the customer and the types of submitted documents. For this purpose, the Bank shall use documentary and non-documentary verification procedures:
1) when dealing with customers who are natural persons:
a) to confirm the identity of a customer or a beneficial owner by using a legal valid document, containing a photograph of the holder, such as an identity card, passport, residence permit, etc.
b) to confirm the date and place of birth by using any legal documents, such as the birth certificate, ID card, passport, residence permit, etc.;
c) to confirm the validity of the presented identity documents by requesting an expert advice of competent persons, such as notaries, embassies, etc.;
d) to confirm the residence address by requesting the invoices for public utility services, tax payment documents, information provided by public authorities or other persons;
e) to confirm the information submitted after the account has been opened - by contacting the customer by telephone, fax, e-mail (if any) or by sending a letter by post;
f) to verify the reference provided by another bank / financial institution;
g) to verify information by using public or private databases, or any other safe and independent sources (for example, references provided by credit history offices / agencies).
2) when dealing with customers who are legal persons and individual entrepreneurs - by any appropriate method depending on the degree of associated risk, so that the Bank can assure the veracity of the information, such as:
a) to verify a legal existence of the legal person, the individual entrepreneur or the individual performing other type of activity by checking the records made in the State Register of legal persons or, as the case may be, in another public or private register or other independent safe source, such as legal firms, accountants, etc.;
b) to obtain a copy of the articles of incorporation or the memorandum of association, a partnership

contract;
c) to verify in public or private databases information on the customer’s existing business relationships;
d) to examine the latest financial reports (except for cases when the bank account is opened by the newly created legal person, the individual entrepreneur or an individual performing other type of activity) and the accounts, which are subject to an external audit, if applicable;
e) to conduct a research / investigation, either individually or through another person, aiming to determine whether there is any evidence that the person is insolvent, filed for liquidation, intends to sell the entity or there are other potential financial problems which have to be taken care of;
f) to obtain the reference of a bank with which the customer previously had business relations, if any;
g) to contact the customer by telephone or fax, by post or email, to check the information placed on the customer's website, if any, or to make a field visit to the headquarters or other business address indicated by the legal entity, the individual entrepreneur or an individual performing other type of activity;
h) to verify the company's unique identifier and the related data, which can be accessed through a public database;
3) when dealing with entities providing fiduciary asset management services (trust, investment fund, etc.), the Bank shall obtain at least a copy of the document confirming the legal nature and legal existence of the account holder (for example: the fiduciary act, the trust statement, the register of charities, etc.). Other verification procedures may include:
a) to apply to an independent recognized and reputable source, such as a law firm or an accountants company, to attest the veracity of submitted documents;
b) to obtain a bank reference prior to entering into business relationship;
c) to access information or search for it in private and public databases or other independent and secure sources;
d) to verify the identity of the authorized representative and beneficial owner;
4) to verify the identity of the beneficial owner the Bank shall apply the measures referred to in sub-item 1) hereto.
5) if there is a person who is authorized to open an account or to conduct transactions on behalf of the customer, the Bank shall check the identity of this person, the legality of the powers of attorney as well as the identity of the person on whose behalf he acts, by using the same procedures as laid down in this Regulation.
[Item 35 amended by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]

36. The Bank shall pay special attention to high-risk customers. Additional verification measures may include:
1) to confirm the customer's permanent address by using official documents, an extract from the register or a reference from a credit agency, or by making a home visit;
2) to obtain a personal reference (for example, from an existing bank customer);
3) to obtain a bank’s or a banking group’s reference by contacting the bank directly prior to establishing a business relationship with the customer;
4) to verify the sources of identified income, available funds and wealth;
5) to verify the customer’s employment status or the public position held.

37. Documents submitted in order to identify the customer and the beneficial owner as well as to verify their identity must be valid on the date of their presentation and their copies shall be stored / archived by the bank in accordance with the established internal procedures. The documents shall be

submitted individually by each targeted person (the customer, the administrator, the beneficial owner, etc.) or by their authorized representative.

38. Documents shall be submitted by the customer in original or in copy (photocopy), certified in accordance with the law, unless otherwise provided by the law. In the case the documents' copies (photocopies) are not properly certified, the Bank shall request the customer to present the original documents to confirm the information and data submitted. Where the customer fails to submit personally the identification documents, the Bank shall obtain the information and documents required in accordance with the provisions of item 58 of this Regulation.

39. Throughout its business relationship, the Bank shall review and update the information on the identification of customers and actual beneficiaries depending on associated risk. The Bank shall update the information as necessary, considering relevant factors, but at least, for high-risk clients - annually, for medium-risk clients - every 2 years, and for low-risk clients - once every 3 years. Relevant factors that may determine the need to update the information include the previous non-application of the identification measures, the period of their application, the adequacy of the data obtained, new regulatory requirements on due diligence measures and / or the change of relevant customer circumstances.

[Item 39 in the wording of NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]

Section III

Measures to monitor activities and transactions

40. The Bank shall continuously monitor the customer's activities, transactions (bank operations), or its business relationship with the customer. The ongoing monitoring process shall include:
1) determining the customer's ordinary (specific) transactions;
2) an extensive examination of transactions conducted during its business relationship with the customer, to ensure that they are in line with the information held by the Bank, the customer's declared activity and the risk level associated with the customer. The examination of transactions requires, at least, the Bank to have in those mechanisms / IT solutions, including the automated ones, which would enable the Bank to detect suspicious activities, transactions or people. Detecting suspicious activities, transactions, and people can be achieved by setting transaction value limits for a particular group or class of transactions or bank accounts. A particular attention should be paid to transactions that exceed the established value limits and transactions that have no clear economic purpose (for example, those that appear to have no economic purpose or involve large amounts of money that do not correspond to the customer's profile created by the Bank or to the customer's ordinary transaction values);
3) verifying whether documents and information gathered during the customer / transaction monitoring are up-to-date and relevant, including for high-risk customers or business relationships;
4) drawing up a transaction monitoring protocol that will reflect all transactions (type, volume, currency, destination of funds, etc.) and all supporting documents submitted or related to those transactions, whenever deemed necessary depending on the associated level of risk. The monitoring protocol shall be kept in the customer's file and upon request, shall be submitted to ne National Bank of Moldova and/ or the Office for Prevention and Fight against Money Laundering.
5) identification of suspicious activities or transactions, including potential ones, as well as of sources of funds used in these activities and transactions;
6) reporting to the responsible person of the information on risks identified with respect to the customers' accounts and transactions, including for high-risk customers;
7) a real-time monitoring of all transactions conducted by customers or potential customers, to

identify persons, groups or entities involved in terrorist activities and the proliferation of weapons of mass destruction, including to identify and prevent any payments made by them in violation of the sanctions, prohibitions or other restrictions imposed.

41. The Bank shall pay particular attention to all significant, complex and unusual transactions that do not appear to have a clear economic or legal purpose. The Bank shall examine the nature and the purpose of such transactions, document the findings and take enhanced CDD measures in accordance with the requirements of this Regulation. In such situations, the Bank shall obtain supporting documents for such transactions and determine the source of the funds (contracts, tax invoices / invoices, shipping documents, customs declarations, salary certificates, tax reports, activity reports, other documents).

42. The Bank shall refrain from executing any operations and transactions in goods, including in financial assets, for up to 5 business days, once it gained pertinent suspicions of money laundering or related offenses, terrorist financing, or the proliferation of weapons of mass destruction, whether these are at the stage of preparation, attempt, are in process or have been already completed.

43. The Bank shall apply the provisions specified under item 42 at the request of the Office for the Prevention and Fight against Money Laundering or on its own initiative. When applying the provisions of item 42 on its own initiative. The Bank shall inform immediately, but not later than within 24 hours, the Office for the Prevention and Fight against Money Laundering of the decision taken.

44. When applying the provisions of item 42, the Bank, where applicable, shall ask the customer to provide additional data and information, including any confirmatory documents for the transactions conducted, in order to apply proper CDD measures and, in particular, to understand the purpose and the nature of the business relationship, as well as the source of the transacted assets.

45. The measures applied according to the provisions of item 42 shall cease ex officio based on the written permission and confirmation of the Office for the Prevention and Fight against Money Laundering. The provisions of this item do not exonerate the bank from the obligations laid down in art. 5 sec. (3) of Law No 308 of 22 December 2017 on the prevention and combating of money laundering and terrorist financing and the internal program, elaborated in accordance with item 12.

46. The Bank shall commit:
1) not to carry out any bank operation or transaction, including through a payment account, or to enter into business relationship if the Bank cannot ensure compliance with the provisions of item 25-29, 34 and 35;
2) in the case of an existing business relationship, to terminate the business relationship if the Bank cannot ensure compliance with the provisions of items 25-29, 34 and 35;
3) in conditions specified in sub-item 1) and (2) hereto, to submit to the Office for the Prevention and Fight against Money Laundering, in accordance with the art. 11 of the Law no.308 of December 22, 2017 on the Prevention and combating of money laundering and terrorist financing, special forms developed for the reporting of suspicious activities or transactions. In this case, the Bank shall be relieved from the obligation to provide explanation to the customer on the reasons for its refusal to do business with the customer.
47. The Bank shall not open or maintain anonymous accounts or accounts in fictitious names, establish or continue a business relationship with a fictitious bank or a bank known to allow a fictitious bank to use its accounts or to provide anonymous bank accounts for the use of its customers.

Section 4

Information obtained from third parties

48. The Bank may use the information belonging to third parties to carry out the measures provided for in points 25, 26, 27, 29, 34 and 35, under the following conditions:
1) third parties represent the reporting entities provided in art. 4 para. (1) of Law no. 308/2017 on preventing and combating money laundering and terrorist financing, residents or similar located in another country (jurisdiction), which are adequately supervised and meet requirements similar to those provided by Law no. 308/2017, and;
2) third parties are not residents in high-risk jurisdictions determined according to the criteria established by the Office for Prevention and Fight against Money Laundering.
[Item 48 in wording of NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]

48^{1}. Banks that use third parties have effective procedures in place to ensure that they immediately obtain from them:
1) all the necessary information related to the measures provided in points 25, 26, 27, 29, 34 and 35;
2) upon request, copies of identification data and other documents related to the measures provided in points 25, 26, 27, 29, 34 and 35.
[Item 48^{1} introduced by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]

49. The Bank shall bear ultimate responsibility for the implementation of the measures set out in items 25-27, 29, 34 and 35, in case of recourse to third parties.
[Item 49 amended by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]

Chapter VI
SIMPLIFIED CUSTOMER DUE DILIGENCE MEASURES

50. The Bank shall apply simplified CDD measures when, by their very nature, they present a lower degree of risk of money laundering or terrorist financing.

51. Simplified CDD measures represent CDD measures referred to in item 25 applied under a simplified procedure corresponding to the low degree of risk of money laundering and terrorist financing, which include:
1) verifying the identity of the customer and the beneficial owner after establishing a business relationship with the customer, when it is necessary not to interrupt normal business practices;
2) a less frequent updating of the identification data;
3) a reduced degree of ongoing monitoring of transactions or the business relationship;
4) obtaining of a limited amount of information on the purpose and nature of a business relationship.
If the identity of the client and the beneficial owner has not been verified until the establishment of the business relationship, the Bank shall ensure that this measure is carried out as soon as possible after the initial contact, but not later than one month. Until the completion of the verification measures, the Bank does not allow transactions to be carried out through the account or establishes specific conditions for its use (value limits, types of services, etc.), in accordance with internal policies and procedures.
[Item 51 completed by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]

52. Based on its own assessment and in accordance with the results of the national risk assessment, the Bank shall set out the factors that generate lower risk of money laundering and terrorist financing and which determine the application of simplified CDD measures, including whether:
1) the customer is a public authority or a state-owned enterprise;
2) the customer is a company the securities of which are traded on a regulated market / multilateral

trading system, that imposes transparency requirements, either by stock exchange rules or by the applicable law to ensure a proper transparency of the beneficial owner;
3) the customer is a resident of the jurisdictions referred to in sub-items 4) and (5), which meet the requirements of international standards for the prevention and combating of money laundering and terrorist financing;
4) the country of destination (jurisdiction) has in place an effective system of preventing and combating of money laundering and terrorist financing in line with international standards, the efficiency of which is regularly assessed by relevant international organizations;
5) the country of destination (jurisdiction) has a low level of corruption and crime according to official assessments;
6) the range of financial products and services is limited and specifically tailored for a circle of customers, to increase financial inclusion;
On the basis of risk-assessment of the money laundering and terrorist financing at national level and on the basis of the criteria and factors established by the authorities with supervisory functions, the Bank shall accumulate sufficient information to determine whether the customer, transactions or business relationships meet the conditions mentioned above.
[Item 52 amended by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]

53. The Bank will not apply simplified CDD measures if there is a suspicion of money laundering or terrorist financing.

Chapter VII
ENHANCED CUSTOMER DUE DILIGENCE MEASURES

54. In order to enforce the legislation on the prevention and combating of money laundering and terrorist financing, the Bank shall set out the categories of customers, activities and transactions that present a high degree of risk based on the indicators reflecting the volume of assets or incomes, the type of services requested, the type of business run, economic circumstances, the reputation of the country of origin, the plausibility of the customer's explanations, the pre-established value limits by transaction type.

55. Based on its own assessment, the Bank shall set out the factors that generate an increased degree of risk of money laundering or terrorist financing and which determine the application of enhanced CDD measures. The factors that generate increased risk are:
1) the business relationship is conducted in unusual circumstances (e.g. a significant geographical distance between the bank and the customer;
2) customers who reside in jurisdictions with a high risk of money laundering and terrorist financing;
3) customers who cannot come in person to the Bank and present their identification documents;
4) legal persons acting as personal property management entities;
5) companies that have mandated shareholders or whose shares are in custody;
6) business activities involving frequent cash transactions of considerable proportions;
7) situations where the ownership structure and control structure of the legal entity are unusual or excessively complex, having regard to the nature of the activity carried out;
8) banking services provided to a natural person based on a customer-tailored portfolio;
9) transactions are conducted in/from countries (jurisdictions) which, according to credible sources (FATF public statements, mutual evaluations, detailed assessment reports or published monitoring reports) do not have in place effective systems for the prevention and combating of money laundering and terrorist financing;

10) transactions are conducted in/from countries (jurisdictions), which are subject to sanctions, embargoes or similar restrictive measures established by international organizations in accordance with the commitments made by the Republic of Moldova;
11) transactions are conducted in/from countries (jurisdictions) which, according to credible sources, have a high level of corruption or other criminal activity;
12) transactions are conducted in/from countries (jurisdictions) which provide funding or support for terrorist activities or allow designated terrorist organizations to operate on their territory;
13) products or transactions that allow for anonymity;
14) remote business relationships or transactions, carried out without being taken any security protection measures, such as electronic signature;
15) payments received from unknown or unrelated parties;
16) cross-border banking (correspondence banking), including when conducting transactions through payable-through accounts;
17) transactions or business relationships with politically exposed persons;
18) new products and new business practices, including new mechanisms for the distribution and use of new or emerging technologies for both new and existing products;
19) other factors identified in the risk assessment and by the supervisory organs.
[Item 55 amended by the NBM Decision no.38 of 11.03.2021, in force 02.07.2021]

56. In assessing the risk of money laundering and terrorist financing associated with customers, countries / jurisdictions, products / services offered, transactions and the associated distribution channel, the Bank shall also take into account the existing risk variables. These variables shall include at least:
1) the purpose of opening a payment account or initiating a business relationship;
2) the amount of assets / funds deposited by a customer or the volume of transactions conducted;
3) the frequency or duration of a business relationship;
57. The enhanced CDD measures applied by the Bank shall include:
1) obtaining additional customer information (type of activity, volume of assets, turnover, other information available in public sources and internet) as well as frequently updating the identification data of the customer and the beneficial owner;
2) obtaining additional information on the nature and purpose of the intended business relationship;
3) obtaining additional information on the source of the customer's goods and the source of wealth;
4) obtaining information on the reasons of the activity or transaction whether intended, currently carried out or completed;
5) obtaining the approval of the responsible person and / or the head of the branch for the establishment or continuation of the business relationship;
6) enhanced monitoring of the business relationship ensured through an increased number and extension of checks performed, and by selecting activities and transactions that require additional examination;
7) the requirement that the first transaction payment to be carried out through an account opened on behalf of the customer at a bank applying similar CDD measures;
8) the implementation of specialized IT systems in order to ensure the efficiency of information management for proper identification, analysis and monitoring of customers and their transactions, as well as the reporting to the Office for the Prevention and Fight against Money Laundering on transactions, which present suspicions of being part of money laundering and terrorist financing schemes;
9) to alert customers whose activities or transactions are exposed to a higher risk of money laundering and terrorist financing on the need to increase their business partner due diligence

measures;
10) in the case of cross-border relationships, to restrict or terminate the business relationship or the execution of transactions in the event of inappropriate application and non-compliance with the requirements for the prevention and combating of money laundering and terrorist financing by the partner / correspondent bank;
(11) additional measures specified in items 58 to 62.
[Item 57 amended by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]

58. In the case referred to in item 55, sub-item 14), the Bank shall apply enhanced CDD measures to the customer who cannot personally present identification documents (e.g. in the case the customer can be contacted only by correspondence, telephone, e-mail, internet or other electronic means) by using such procedures as electronic signature, biometric methods, session keys, etc. At his first visit to the Bank, the customer is to present documents and information specified in the provisions of the present Regulation. In addition, the Bank shall apply one or all of the following measures:
1) request the customer's identification documents issued by a competent authority or body, including specimen signature, other documents, as appropriate, for the customer's file;
2) take measures to ensure authenticity of electronic documents transmitted to the Bank;
3) use the information provided by a bank in which the customer holds an account and which applies at least similar customer CDD measures;
4) require the first payment to be made on behalf of the customer through an account from another bank that applies at least similar CDD measures and is subject to an effective supervision, where appropriate;
5) establish and maintain contact with a remote customer through separate dedicated channels, regardless of the channels used for carrying out transactions.

59. In cross-border relationships, the Bank shall accumulate sufficient information about the correspondent bank (institution, organization) to fully understand its field of activity. For this purpose, the Bank shall:
1) obtain information at least on:
a) the Council and the Executive Board of the correspondent institution, its main activities, its business address and the measures it applies to prevent and combat money laundering and terrorist financing;
b) the beneficial owners of the correspondent institution;
c) the purpose of setting up a bank account;
d) the reputation of the correspondent institution and the quality of supervision it exercises, including whether it has been the subject of an investigation or any remedial action relating to money laundering or terrorist financing (from public sources);
2) assess the controls performed by the correspondent institution to prevent and combat money laundering and terrorist financing;
3) initiate correspondence after obtaining the approval of the Bank's responsible person;
4) obtain document(s) listing responsibilities of the correspondent institution in the field of the prevention and combating of money laundering and terrorist financing, as well as documents to confirm the fact that the correspondent institution verifies the identity of its customers and has in place efficient CDD procedures;
5) In the case of transactions carried out through "correspondent payment accounts", the Bank shall make arrangements allowing it to verify the CDD procedures applied by the correspondent institution and to transmit / receive, upon request, documents and information relating to customers, their business activity and transactions.

60. In case of business relationships or transactions with politically exposed persons, their family members or persons associated with politically exposed persons, the Bank shall apply at least the following measures:
1) The Bank shall have in place a risk management system that:
a) allows to determine whether a customer, potential customer and / or his beneficial owner is a politically exposed person;
b) the Bank shall request relevant information from the customer and / or his beneficial owner, uses the reference in public data sources or in commercial electronic databases containing information on politically exposed persons;
2) requires obtaining the approval of the Bank's responsible person for the establishment of a business relationship and, if the Bank's customer or the beneficial owner subsequently becomes a politically exposed person, for the continuation of the business relationship;
3) requires establishing and verifying the source of the customer's funds and wealth involved in the business relationship or transaction;
4) requires requesting information about family members and persons associated with the politically exposed person.
5) requires ensuring an enhanced monitoring of the business relationship and the transactions carried out by the politically exposed person, including a regular update of the information on the customer.
[Item 61 repealed by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]

62. If customers acting on behalf of other persons specified under item 55 sub-items 3) and (4) are not authorized to provide the Bank the information requested on beneficial owners, the Bank shall refuse to open an account or establish new business relationships with such customers in the future.

62^1. In business relations or in case of transactions with customers and banks (institutions, organizations) from high-risk countries (jurisdictions) in regard of which FATF requests to take action, in addition to the enhanced due diligence measures provided for in this Chapter, the Bank shall, in addition, apply in accordance with the requested actions and depending on the risk, one or more of the following measures:
1) limiting the development of the business relationship or the execution of transactions in / from the country (jurisdiction) with high risk or with persons from this country;
2) reviewing, modifying or, as the case may be, terminating the relationship with the corresponding institution in the high-risk country (jurisdiction);
3) when establishing legislation of special value limits related to transactions associated with high-risk jurisdictions, reporting transactions in accordance with regulated value limits.
[Item 62^1 introduced by NBM Decision no. 38 of 11.03.2021, in force on 02.07.2021]

62^2. The measures provided for in item 62^1 shall also be applied if requested by the Office for Prevention and Fight against Money Laundering or by the supervisory authority.
[Item 62^2 introduced by NBM Decision no. 38 of 11.03.2021, in force on 02.07.2021]

Chapter VIII
DATA REQUIREMENTS FOR FUND TRANSFER TRANSACTIONS

63. This chapter refers to transfers of funds, carried out in any currency, which are transmitted or received by a bank or an intermediary bank.

64. The provisions of this chapter shall not apply to transfers of funds carried out by using a payment card, an electronic money instrument or any other prepaid digital data device with similar characteristics, provided the following conditions are met:

1) the payment card, electronic money instrument or data device is used solely for the purchase of goods or services;
2) the number of the payment card, electronic money instrument or data device accompanies all money transfers resulting from the transaction.
However, this chapter shall apply where a payment card, electronic money instrument or any other prepaid digital data device with similar characteristics is used to transfer funds between persons.

65. This chapter does not apply to transfers of funds involving cash withdrawal from the payer's payment account.

Section 1
Obligations of the payer's bank

66. The Bank shall ensure that the transfers of funds are accompanied by the following information regarding the payer:
1) the full name of the payer;
2) the number of the payer's payment account;
3) the payer's address, ID number, fiscal code (IDNO / IDNP) or date and place of birth.

67. The Bank shall ensure that the transfer of funds is accompanied by the following information regarding the payee:
1) the full name of the payee;
2) the number of the payee's payment account.

68. By way of derogation from item 66 sub-item 2) and item 67 sub-item 2), in the case of transfers not effected from or to a (bank's) payment account, the payer's bank shall ensure that the transfer of funds is accompanied by a unique transaction identification code instead of the (bank) payment account number(s).

69. Prior to transferring the funds, the Bank shall verify the completeness and accuracy of data specified in item 66 based on documents, data or information obtained from a credible and independent source, taking into account the provisions of this Regulation.

70. The Bank shall ensure that all cross-border fund transfers are accompanied by complete information on the payer and payee's names, the account number or a unique transaction / payment identification code, and that the "destination of payment / transfer" field has been properly completed.

71. In the case of the batch file transfers of loans made by a single payer to several payees whose payment service providers operate outside the Republic of Moldova, the provisions of item 66 shall not apply, provided that 1) a batch file transfer is accompanied by data referred to in item 66, 67 and 68, 2) these data were verified in accordance with item 69, and 3) individual transfers are accompanied by the number of the payer's payment account or by the unique transaction identification code (according to item 68), whichever applicable.

72. The Bank shall not execute / carry out any transfer of funds unless compliance with the provisions of item 66-71 has been ensured.

Section 2
Obligations of the payee's bank

73. The Bank shall put in place effective procedures, including, where appropriate, post-transaction or real-time checks, to determine whether the transaction data fields reflecting information on the

payer and payee in the payment and settlement system used for the transfer of funds were completed in accordance with the provisions of item 66 and 67 of this Regulation.

74. Prior to crediting the payee's account or making funds available to him, the Bank shall verify the completeness and accuracy of the information referred to in item 67 based on documents, data or information obtained from a credible and independent source, taking into account the provisions of this Regulation.

75. The Bank shall verify the completeness and accuracy of information available on the payee, based on documents, data or information obtained from a credible and independent source, taking into account the provisions of this Regulation, in the case of transfers of funds, the amount of which does not exceed the threshold set out in item 25, sub-item 2), in the following situations:
1) when the payment is made in cash or in anonymous electronic money in the case of transactions that appear to be linked;
2) when there are good reasons to suspect that the transaction is part of the money laundering or terrorist financing scheme.

76. The Bank shall apply effective risk-based procedures to determine whether to execute, reject or suspend a transfer of funds where complete information on the payer and the payee is missing. The Bank shall consider applying these procedures also in the case when the "destination of payment / transfer" field has not been filled in.

77. Where upon the receipt of funds the Bank finds that the information specified in item 66 and 67 is missing or is incomplete, the Bank shall reject executing the transfer or request the provision of relevant information on the payer and the payee prior to crediting the payee's account or making money available to the payee, depending on the associated risk.

78. Where a credit institution / bank systematically fails to provide relevant information on the payer or payee, the payee’s bank shall take steps which may first include issuing warnings and setting deadlines, either for rejecting any transfer of funds executed by this credit institution / bank, or for deciding, where appropriate, to restrict or terminate the business relationship with it. The Bank shall report such incidents to the Office for the Prevention and Fight against Money Laundering in compliance with the applicable regulatory acts.

78^{1}. The Bank, when acting as the payer's and payee's bank, shall take into account all information regarding the payer and the payee to assess whether the transfer of funds or any related transaction is suspicious and whether it should be reported to the Office for the Prevention and Fight against Money Laundering according to the legislation.
[Item 78^{1} introduced by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]

Section 3
Obligations of an intermediary bank

79. The Bank shall put in place effective procedures, including, where appropriate, post-transaction or real-time checks, to determine whether the transaction data fields reflecting information on the payer and payee in the payment and settlement system used for the transfer of funds were completed in accordance with the provisions of item 66 and 67 of this Regulation and shall ensure that all information received on the payer and payee accompanying a transfer of funds is kept together with that transfer;
[Item 79 amended by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]

80. The Bank shall ensure that the batch file transfers contain information on the number of the payer's payment account or a unique transaction / payment identification code, and that the batch file provides fully traceable information on the payer and payee of the transaction.

81. The Bank shall apply effective risk-based procedures to determine whether to execute, reject or suspend a transfer of funds where complete information on the payer and the payee is missing. The Bank shall consider applying these procedures also in the case when the "destination of payment / transfer" field has not been filled in.

82. Where upon the receipt of funds the Bank finds that the information specified in item 66 and 67 is missing or is incomplete, the Bank shall reject executing the transfer or request the provision of relevant information on the payer and the payee prior to crediting the payee's account or making money available to the payee, depending on the associated risk.

83. Where a credit institution / bank systematically fails to provide relevant information on the payer or payee, the payee's bank shall take steps which may first include issuing warnings and setting deadlines, either for rejecting any transfer of funds executed by this credit institution / bank, or for deciding, where appropriate, to restrict or terminate the business relationship with the respective institution/bank.

84. The Bank shall report such incidents to the Office for the Prevention and Fight against Money Laundering in compliance with the applicable regulatory acts.

Chapter IX
ACTIVITY AND TRANSACTION REPORTING

85. The Bank commits to inform the Office for the Prevention and Fight against Money Laundering of:
1) any suspicious goods, activities or transactions suspicious to be related to money laundering, to associated offences and to terrorism financing that are in course of preparation, attempting, accomplishment, or are already performed – immediately or, latest, within 24 hours after the Bank has identified the action or circumstances that raise suspicions;
2) any cash transactions or bank operations, whether they are carried out in a single transaction with value exceeding 200 000 MDL (or its equivalent) or through a series of cash transactions that appear to be linked - within 10 calendar days;
3) any transactions conducted through bank transfer with a value exceeding 500000 MDL (or equivalent) - not later than the 15th of the month following the reporting month;

86. The Bank shall have in place:
1) clear procedures, developed in compliance with the provisions of the Law no. 308 of 22 December 2017 on the Prevention and combating of money laundering and terrorist financing, which were made known to the entire staff and which provide for the reporting by personnel of all suspicious assets, any activities or transactions that raise suspicions of money laundering, any related offence or terrorist financing;
2) systems for detecting suspicious activities and transactions according to the established criteria and indices, including by competent authorities;
3) procedures for informing the Bank's responsible person and, if required, the internal security service on issues related to the prevention and combating of money laundering and terrorist financing.

Chapter X
DATA STORAGE

87. The Bank shall retain all documents, records and information obtained under this Regulation, including those obtained under due diligence measures concerning customers and beneficial owners, such as copies of identification documents, archive of primary accounts and documents, business correspondence, analysis results and research carried out, during the active period of the business relationship and for a period of 5 years after its termination or after the date of occasional transactions and transfers of funds, and subsequently up to 5 years in electronic format.

[Item 87 in the wording of NBM Decision no.38 of 11.03.2021, in force 02.07.2021]

88. The procedures of records and information storage shall include at least the following, as appropriate:
1) keeping a register of all customers and identified beneficial owners, which shall contain at least: the full name of the customer; IDNO / IDNP, as appropriate; the account number; the account opening and closing date;
2) keeping all primary documents, including business correspondence;
3) keeping files containing records regarding the identification and verification conducted on customers and beneficial owners on monitoring customers' transaction and maintaining the transactions' supporting documents;
4) keeping records of all conducted transactions (type, the volume of transactions, currency, destination, etc.) and related monitoring protocols, including for complex and unusual transactions;
4^1) keeping records on transfers of funds, including in cases where the technical limitations of the payment system do not allow the transmission of all information by the intermediary institution;
5) archiving information on conducted transactions and related business correspondence in IT systems and ensuring that the archived data are safe and quickly accessible for operational purposes.
[Item 88 amended by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]

89. The Bank shall ensure that any document and information obtained as a result of the customer (beneficial owner) identification and verification procedures, any data related to transaction monitoring, including transaction supporting documents, are available to the National Bank of Moldova and the Office for the Prevention and Fight against Money Laundering, upon request. Based on the request of the competent authorities, in accordance with item 9 sec. (2) of the Law no. 308 of 22 December 2017 on the Prevention and combating of money laundering and terrorist financing, the record storage period established for the information related to customers and their transactions may be extended for a period specified in the request but not more than 5 years.

Chapter XI
INTERNAL CONTROL SYSTEM REQUIREMENTS

90. The Bank shall have in place internal control systems that will ensure that the Bank complies with the applicable regulatory acts and the existing internal programme in the field of money laundering, that will contribute to reducing the related risks.

91. When establishing subsidiaries and branches in the territory of other states as well as during their activity, the Bank shall apply measures developed for the prevention and combating of money laundering and terrorist financing in accordance with its own internal control system, internal policies and procedures and regulatory acts of the Republic of Moldova insofar as the legislation of

the host country permits. Where the host country (jurisdiction) promotes less rigorous requirements for the prevention and combating of money laundering and terrorist financing, the Bank shall ensure the implementation of the requirements set forth in Moldovan regulatory acts insofar as the law of the host country (jurisdiction) permits. Where the host country (jurisdiction) does not allow proper application of the requirements set forth in Moldovan regulatory acts, the Bank shall apply appropriate additional measures to mitigate the risk of money laundering and terrorist financing and inform about this fact the National Bank of Moldova within two months' period. The National Bank may exercise its supervision in accordance with the legal framework to ensure compliance of the Bank's subsidiaries and branches established in the territory of other states with the relevant applicable regulatory acts; in the case of failure to comply with relevant regulatory acts, the National Bank of Moldova may restrict the activity of a respective subsidiary or branch, or withdraw its approval through which it authorized the establishment of the Bank's subsidiary or branch in the territory of another state. In applying this item, the National Bank of Moldova issues technical standards on the type of additional measures and minimum steps to be taken by the bank if the rules of law of another country (jurisdictions) do not allow the implementation of the measures provided for in this item.

92. The Bank shall communicate and implement the provisions of its internal programme for the prevention and combating of money laundering and terrorist financing within its branches, subsidiaries and other subdivisions owned by the Bank, including those located in other countries. In order to prevent and combat money laundering and terrorist financing, the Bank shall exchange data with branches, subsidiaries and other subdivisions owned by the Bank in compliance with the provisions of the applicable regulatory acts.

92^1. In case of opening of subsidiaries and branches on the territory of other States, at the level of the financial group, the internal control system and the program on preventing and combating money laundering and terrorist financing shall include, in addition to the elements set out in items 93-95, the following additional elements:
1) policies and procedures for the exchange of information for the purpose of enforcing customer precautions and managing the risks of money laundering and terrorist financing;
2) requirements for the provision of information within the group on customers, accounts and transactions, where this is necessary for the application of measures to prevent and combat money laundering and terrorist financing;
3) adequate requirements for maintaining the confidentiality of the information subject to the exchange which constitutes banking secrecy and personal data, as well as the use and processing of this information.
[Item 92^1 introduced by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]

93. The internal control system shall include at least the following elements:
1) an independent audit conducted by the internal audit subdivision in order to verify the Bank's compliance with the provisions on prevention and combating money laundering and terrorist financing. In this context, the audit shall include:
a) independent assessment of the adequacy of policies and procedures related to the prevention and combating of money laundering and terrorist financing as well as to the identified risks of money laundering and terrorist financing;
b) independent assessment of the efficiency of implementation by the Bank's staff of the approved policies and procedures in the field of the prevention and combating of money laundering and terrorist financing;
c) independent assessment of the efficiency of the compliance and quality control supervision, including the parameters set for automatic alerts;

d) independent assessment of the efficiency of trainings conducted by the Bank for its relevant personnel;
e) informing the management organs on the assessment's results and recommended measures to be taken to minimize the identified risks and deficiencies;
2) the appointment of persons, including from the member of the Council or from the Executive organ of the Bank to be responsible for ensuring compliance with the applicable legislation on prevention and combating money laundering and terrorist financing (hereinafter referred to as "responsible person"). For this purpose, the responsible person shall have the following tasks:
a) provides advice to the Bank's employees on issues arising during the implementation of the programme on the prevention and combating of money laundering and terrorist financing, including on the identification and examination of bank customers and the assessment of the risk of money laundering and terrorist financing;
b) approves the commencement, continuation or termination of business relations with high-risk customers (or delegates the duty to the branch manager, as the case may be);
c) takes decisions based on the information received;
d) takes measures to report to the Office for the Prevention and Fight against Money Laundering of the information in accordance with the law;
e) organizes trainings for the Bank's employees in the field of the prevention and combating of money laundering and terrorist financing;
f) presents to the Board of the Bank, at least once a year, a written report on the results of the implemented programme on the prevention and combating of money laundering and terrorist financing, including information on the risks of money laundering and terrorist financing identified during the year and on measures taken to minimize them;
g) collaborates with the audit entity/officers in view of verifying compliance of the Bank's activity with the legislation in the field of the prevention and combating of money laundering and terrorist financing;
h) performs other functions in accordance with this Regulation and the internal documents of the Bank;
3) internal provisions on liability and sanctioning of employees who deliberately do not inform / report about any suspicious activities or transactions to the responsible person, the security service or directly to the competent authority and/or personally contribute to carrying out transactions of money laundering and terrorist financing.

94. The Bank shall have in place programmes for recruiting and ongoing training of the staff in the field of the prevention and combating of money laundering and terrorist financing. The Bank shall ensure that its staff and the Bank's responsible person have appropriate knowledge, skills and abilities to effectively fulfil their responsibilities in the field of the prevention and combating of money laundering and terrorist financing.

95. The recruiting and training programmes referred to under item 94 shall cover various aspects of the process of preventing and combating money laundering and terrorist financing as well as of obligations arising under the relevant legislation, including:
1) training of new employees on the importance and basic requirements set by the respective programmes;
2) training of the frontline staff (employees who work directly with customers) in identifying types of customers, checking their identity, performing an ongoing monitoring of accounts / transactions conducted by existing customers, tracking indices and reporting of activities and transactions that raise suspicions or are subject to reporting;
3) regular updating of staff responsibilities;

4) new techniques, methods and schemes of money laundering and terrorist financing;
5) the level of staff involvement in the prevention and combating of money laundering and terrorist financing.
The curriculum of staff trainings must be tailored to the individual needs of each bank.

96. The Bank shall process the customers' personal data collected in compliance with the requirements of this Regulation and ensure their confidentiality, taking into account the requirements of the applicable regulatory acts on the personal data protection.

Chapter XII
REQUIREMENTS FOR APPLICATION OF INTERNATIONAL RESTRICTIVE MEASURES

97. The Bank shall immediately apply restrictive measures to assets, including those obtained from or generated by assets owned, held or controlled, directly or indirectly, wholly or jointly, by persons, groups and entities involved in terrorist activities and the proliferation of weapons of mass destruction subject to restrictive measures, ,persons, groups and entities acting on behalf of, at the indication, who make part of or are controlled, directly or indirectly, by such persons, groups and entities.
[Item 97 amended by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]

98. For the application of restrictive measures under item 97, the Bank shall develop internal rules and procedures that shall include at least the following elements:
1) procedures for collecting, keeping and updating the list of persons, groups and entities involved in terrorist activities and the proliferation of weapons of mass destruction subject to international restrictive measures (including through the use of existing databases), in compliance with the provisions of the Law no. 308 of 22 December 2017 on the Prevention and combating of money laundering and terrorist financing and the Law no. 25 of 4 March 2016 on the Application of international restrictive measures;
2) procedures for screening / detection of designated persons or entities and of transactions (bank operations) involving assets, which could be applied to potential customers, existing customers or customers conducting occasional and money transfer transactions;
3) competences of persons responsible for the implementation of internal rules and procedures for the application of international restrictive measures to block funds;
4) procedures for internal information dissemination / reporting as well as for reporting to the Office for the Prevention and Fight against Money Laundering.

99. Upon identification of assets owned, held, or controlled, directly or indirectly, by persons, groups and entities involved in terrorist activities and the proliferation of weapons of mass destruction subject to restrictive measures, the Bank shall undertake the following steps:
1) based on the decision of the Bank's responsible person, shall put on hold, for an indefinite period of time, the execution of bank operations and transactions that are ordered by or benefit, directly or indirectly, the persons, groups and entities involved in terrorist activities and the proliferation of weapons of mass destruction subject to restrictive measures;
2) immediately inform, but not later than within 24 hours, the Office for the Prevention and Fight against Money Laundering, about putting on hold, for an indefinite period of time, the execution of bank operations and transactions that are ordered by or benefit, directly or indirectly, the persons, groups and entities involved in terrorist activities and the proliferation of weapons of mass destruction subject to restrictive measures. The submitted information shall include at least the following:

a) data and information (name of natural / legal person, IDNO / IDNP, if any, country of origin / residence, the list of the competent authority / organization which is referred to in the restrictive measure applied, etc.) on the person, group or entity identified;
b) data and information (amount, currency, payee, destination, etc.) of identified assets;
c) information on the decision of the Bank's responsible person to put on hold, for an indefinite period of time, the execution of bank operations and transactions relating to identified assets;
3) where applicable, the Bank shall accept additional payments made by a third party, or the increase of the value of identified assets and extend the scope of the restrictive measure to include these assets, taking into account the provisions of item 99 sub-item 1), and shall duly inform on the above the Office for the Prevention and Fight against Money Laundering, in compliance with the provisions of item 99 sub-item 2) (a) and (b);
4) inform the National Bank of Moldova of the restrictive measures applied in compliance with the provisions of item 99 sub-item 2) (a) and (b);

100. In case of any identity doubts or suspicions that do not allow the Bank to form a firm opinion as to the identity of the person, group or entity included in the list referred to under art. 34 sec. (11) of the Law no. 308 of 22 December 2017 on the Prevention and combating of money laundering and terrorist financing, the Bank shall immediately, but not later than within 24 hours, inform on the above condition the Office for the Prevention and Fight against Money Laundering;

101. The Bank shall ensure a constant monitoring of the official websites of the United Nations Organisation, the European Union and the Intelligence and Security Service in order to ensure the appropriate applicability of restrictive measures to persons, groups and entities involved in terrorist activities and the proliferation of weapons of mass destruction.

Chapter XIII
OTHER DISPOSITIONS

102. Where a Bank is found to be in breach of the provisions of this Regulation or of the obligations arising under the legislation on the prevention and combating of money laundering and terrorist financing, the National Bank of Moldova imposes sanctions to the Bank in accordance with the legislation in force.

103. When applying the present Regulation, the Bank shall inform the National Bank of Moldova of any assets, business operations or transactions that raise suspicions of money laundering, related offenses or terrorist financing, as well as any fraud incidents that essentially affect the Bank's security, stability or reputation.

Attachment to the
Regulation
on requirements related to prevention
and combating money laundering and
terrorist financing in the activity of the banks

Recommendations on the criteria for identifying the beneficial owner

Natural persons who may control the legal person through ownership interests

a) The natural person(s) who directly or indirectly holds a minimum percentage of ownership interest in the legal person (the threshold approach).

The bank shall consider the threshold higher than 25% owned by the natural person (s) as an essential factor in determining the beneficial owner. In the case of indirect control over the legal

entity (legal entities or corporate vehicle chain), the beneficial owner is determined using the actual controlling ownership technique (calculating the share held by each potential beneficial owner in the chain and the natural person holding the highest level of participation is considered to be the beneficial owner).

b) Shareholders who exercise control alone or together with other shareholders, including through any contract, understanding, relationship, intermediary or tiered entity (a majority interest approach).
The Bank shall consider indirect control, which may extend beyond legal (direct) ownership or could be through a chain of corporate vehicles or legal entities and through certain nominations, as a key factor in determining the beneficial owner. In such situations, the indirect control can be identified through various means, such as: agreement between shareholders, the exercise of a dominant influence or the power to appoint senior management. Shareholders can increase the level of control through formal or informal agreements or through the use of nominee shareholders (owner invested or registered, holding shares on behalf of the beneficial owner under a custody agreement). The bank considers the different types of ownership interests and the possibilities that may exist, including voting or economic rights (for example, equity or debt-for-equity securities).

Natural persons who may control the legal person through other means
a) The natural person(s) who exerts control of a legal person through other means
The bank shall consider the personal connections between the individual and the persons referred to in subparagraphs (a) and (b) in identifying the beneficial owner or persons who own the property.

b) The natural person(s) who exerts control without ownership
The Bank considers situations when the individual participates in the financing of the legal entity or obtains benefits or there are close family relationships, historical or contractual associations, or if the legal entity defaults on certain payments (debts). In addition, control may be presumed even if control is never effectively exercised, such as the using, enjoying or benefiting from the assets owned by the legal person.

Natural persons who may exercise control through positions held within a legal entity
a) The natural person(s) responsible for strategic decisions that fundamentally affect the business practices or general direction of the legal entity.
The Bank considers the situation when the position of director / administrator can play an active role in exercising control over the legal person's business. However, information on directors may be of limited value if its country allows the administrator to be a nominal person (the person acting on behalf of unidentified interests).

b) The natural person(s) who exercises executive control over the daily or regular affairs of the legal person through a senior management position.
The Bank shall consider situations where the chief executive officer (CEO), chief financial officer (CFO), managing or executive director, or president may play an active role in exercising control over the business of the legal person, or the individual (s) have significant authority over financial relationships, including financial institutions (banks) and the ongoing financial affairs of the legal person.

Sources for obtaining information about beneficial owners
a) Register of founders or the list of shareholders submitted by the legal person, which is kept and permanently updated, compiled according to the data and information in the legal documents for the incorporation of the legal person and / or the memorandum and articles of association and registered with the state authorities or private registers, as determined by applicable law;

b) The public / private register of the registration data of the legal person, drawn up according to the applicable law, containing at least the following information: name, proof of registration, legal status and form, registration address, basic powers governing the activity, the list of directors and the register of shareholders or founders, including the categories of shares held and the right to vote;

c) Information obtained from other reporting entities under similar conditions regarding the application of customer due diligence measures to clients and their beneficial owner.

d) Information held by other competent authorities on the basis of legal obligations (e.g. tax authorities, financial or regulatory authorities and other companies holding similar registers);

e) Available information on listed companies on a regulated market / multilateral trading system, which requires information disclosure requirements, either by stock exchange rules or by law or by enforceable means, in order to ensure the proper transparency of the beneficial owner.