# Regulation on requirements for prevention and combating money laundering and terrorism financing in the activity of non-bank payment services provider No 202 of 09 August, 2018

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

**Decision**
**of the Executive Board of the National Bank of Moldova No 202 of 9 August 2018**
**on the approval of the Regulation on requirements for prevention and combating money laundering and terrorism financing in the activity of non-bank payment services provider**
(*in force as of 24.08.2018*)
Published in the Official Monitor of the Republic of Moldova No 321-332 of 24.08.2018, Article 1313

REGISTERED:
Ministry of Justice of the
Republic of Moldova
No 1355 of 21.08.2018

Pursuant to Article 5 paragraph (1) m), Article 11 paragraph (1) and Article 27 paragraph (1) c) of 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, Article 544), Article 5 paragraph (2), Article 93 paragraph (2) letter b) and Article 94 of Law on payment services and electronic money, No 114 of 18 May 2012 and Article 13 paragrpah (3) and (14), Artocle 15 paragraph (2) of Law No 308 of 22 December 2017 on the prevention and combating money laundering and terrorist financing (Official Monitor of the Republic of Moldova, 2018, No 58-66, Article 133), Executive Board of the National Bank of Moldova

**DECIDES**:
1. To approve the Regulation on requirements related to prevention and combating money laundering and terrorism financing in the activity of non-bank payment services providers, (see attached).

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**

Annex

Approved by the
Decision of the Executive Board
of the National Bank of Moldova
No. 202 of 9 august 2018

# REGULATION
## on requirements related to prevention and combating money laundering and terrorism financing in the activity of non-bank payment services providers

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

## Chapter I
## GENERAL PROVISIONS

1. The Regulation on requirements related to prevention and combating money laundering and terrorism financing in the activity of non-bank payment services providers (hereinafter – Regulation) establishes rules for: identification and assessment by non-bank payment services providers of money laundering and terrorist financing risks, development of internal policies and programs, application of customer due diligence requirements, including customer enhanced due diligence measures; data storage; reporting the suspicious activities and transactions; application of financial sanctions related to terrorist activities and proliferation of weapons of mass destruction; putting in place and implementation of the elements of the internal control system, as well as other requirements in order to minimize the risks related to money laundering and terrorist financing.

2. The non-bank payment service provider (hereinafter – Provider) shall apply the provisions of this Regulation in business relations with their customers or when conducting transactions (payments) both directly and through agents.

3. The terms and expressions used in this Regulation shall have the meanings stipulated in Law No 308 of 22 December 2017 on the Prevention and combating money laundering and terrorist financing, Law No 114 of 18 May 2012 on the Payment services and electronic money, Law No 548 of 21 July 1995 on the National Bank of Moldova, as well as other regulatory acts of the National Bank of Moldova and of the Office for Prevention and Fight against Money Laundering, related to the field of prevention and combating money laundering and terrorism financing. In addition, for the purposes of this Regulation, the following terms and expressions shall be used:

*legal entity identifier (LEI)* shall mean a 20-character unique alphanumeric code based on the ISO standard 17442 assigned to a legal entity.

*[Item 3 amended by NBM Decision No. 8 of 13.01.2025, in force 16.01.2025]*

## Chapter II
## RESPONSIBILITIES

4. The Provider shall have in place and implement an internal program on prevention and combating money laundering and terrorist financing.

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

6. The Provider is responsible for developing, approving and ensuring the implementation of the internal program on prevention and combating money laundering and terrorism financing and for compliance of the activity to the provisions of legislation in the field of prevention and combating money laundering and terrorism financing.

7. The Internal Audit subdivision of the Provider or an audit firm/external auditor shall perform, at least annually, an independent assessment of the adequacy and compliance of the Provider's activity with the Program on prevention of money laundering and terrorism financing. The results of the assessment shall be communicated to the responsible manager of the Provider and, on request, to the National Bank of Moldova.

## Chapter III
## REQUIREMENTS REGARDING THE INTERNAL PROGRAM ON PREVENTION AND COMBATING MONEY LAUNDERING AND TERRORIST FINANCING

8. The internal program on prevention and combating money laundering and terrorism financing represents a series of policies, methods, practices, procedures and other rules, including the customer due diligence procedures, promoting ethical and professional standards on the market for payment services, that aim to prevent organized criminal groups or their associates from using the Providers for money laundering or terrorist financing purposes. This program must ensure that payment operations are carried out in a safe and prudent way.

9. The Provider shall draw up the internal program on prevention and combating money laundering and terrorism financing in accordance with the provisions of Law No.308 of 22 December, 2017 on Prevention and combating money laundering and terrorism financing, the present Regulation, other regulatory acts of the Office for the Prevention and Fight against Money Laundering, issued for the purpose of application of this law, taking into account the industry-accepted practices, including the documents issued by the international Financial Action Task Force (FATF). The internal program shall be approved by the manager of the provider, who is responsible for ensuring that the provider’s policies and procedures comply with legal requirements to prevent and combat money laundering and terrorist financing.

10. When developing the internal program, it shall be taken into account the size, complexity, nature and amount of the activities carried out by the Provider, the types (categories) of customers, the degree (level) of risk associated with different customers or customer categories as well as the customers’ transactions, agencies and affiliates through which they operate.

11. Internal program on prevention and combating money laundering and terrorist financing shall include, without being limited to, the following:
1) the responsibilities of the responsible manager of the Provider, which shall include at least:
a) knowing the criteria (indices) of increased risk clients;
b) approving significant operations of the increased risk clients;
c) determining the Provider's areas of activity exposed to the risk of money laundering and terrorist financing. Areas of activity exposed to the risk of money laundering and terrorist financing may be those related to: products and services provided, transactions made both directly and through payment agents, open payment accounts, etc.
d) remediation of deficiencies identified in the field of prevention and combating money laundering

and terrorism financing, including reporting suspicious transactions to the Office for Prevention and Fight against Money Laundering;
e) the implementation of the internal program on preventing and combating money laundering and terrorist financing, determining the responsibilities of personnel at different hierarchical levels, including those in senior management positions;
e[1]) determining the mechanism to protect compliance officers and employees who report violations of legislation on preventing and combating money laundering and terrorist financing;
f) implementation of internal procedures concerning the reasonable time access of the responsible staff to the information required for performance of work obligations;
2) the customer acceptance procedures that describe at least the categories of customers whom the Provider intends to attract as well as the staff levels that shall 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;
3) the measures 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;
4) the CDD measures, including simplified and enhanced CDD measures for each category of customers, products, services or transactions subject to these measures and risk management measures in case of establishing the business relationship until the verification of the identity of the client and the beneficial owner;
5) the procedures to be applied to monitor customer transactions for detecting significant, complex and unusual transactions without a clear legal or economic purpose, suspicious activities and transactions;
5[1]) the procedures and requirements for the application of enhanced due diligence measures when carrying out transactions of resident customers with virtual asset service providers authorised in other states.
6) measures to identify and monitor customers and customer operations with countries / jurisdictions lacking effective anti-money laundering and terrorism financing systems, or posing an increased risk due to high levels of crime and corruption, and/or involved in terrorist activities;
7) the procedures describing the collection and storage of information as well as the conditions of granting access to them;
8) the procedures for reporting internally and to the competent authorities on suspicious money laundering or terrorist financing activities and transactions, or non-compliance with applicable laws or internal procedures;
9) the procedures and measures aiming to ascertain compliance with relevant standards and to assess their effectiveness;
10) standards developed for the personnel's recruitment, employment and training programs in the field of prevention and combating money laundering and terrorism financing;
11) procedures for identifying and analyzing the risks of money laundering and terrorism financing, including the measures to minimize them, by using information technologies, including the modern ones, which are to be procured or developed as one of the Provider's products or services.
*[Paragraph 11 amended by NBM Decision No 38 of 11.03.2021, in force 02.07.2021]*

12. Whenever required, but at least annually, the Provider shall review (update) its internal program on the prevention and combating of money laundering and terrorism financing, taking into account relevant legal provisions.

## Chapter IV
## THE ASSESSMENT OF RISK EXPOSURE TO MONEY LAUNDERING AND TERRORIST FINANCING. THE RISK-BASED APPROACH

13. The Provider commits to identify and evaluate the existing risk exposure to money laundering and terrorism financing, taking into account the national risk assessment of money laundering and terrorism financing, as well as the criteria and factors established by the National Bank of Moldova and the Office for the Prevention and Fight against Money Laundering. The results of the assessment shall be documented in an assessemnt report, which shall be approved and periodically updated, responsible for this process being the Provider's responsible manager, and on request shall be submitted to the Office for Prevention and Fight against Money Laundering and/or the National Bank of Moldova.

14. The provider, based on the results of the money laundering and terrorism financing risk assessment, shall ensure the implementation of the risk-based approach to prevent and mitigate money laundering and terrorism financing in proportion to the identified money laundering and terrorism financing risks in the field of activity.

15. For the purpose of implementing item 13 the Provider shall carry out and update the risk assessemnt in its area of activity, at least once a year and after each money laundering and terrorist financing risk assessment at national level, as well as where appropriate, when additional criteria and risk factors are identified by the National Bank of Moldova and the Office for Prevention and Fight againt Money Laundering. This process shall include at least:
1) the preparation of a written report describing the countries or geographical areas, products, customers and transactions presenting a high degree of risk, their share and impact on the Provider's activity;
2) the drawing up of an action plan aiming to minimize the identified risks of money laundering and terrorism financing;

16. The Provider shall identify and assess existing risks of money laundering and terrorism financing before:
1) it launched and developed new products and services;
2) it started using new or developing technologies for both new and existing products and services.

17. While assessing its risk exposure to money laundering and terrorism financing, the Provider shall use different sources of information to identify, manage and mitigate the risks associated with its field of activity. This includes considering typologies, risk indicators, guidelines and / or recommendations issued by national and international competent authorities. In identifying and assessing the risks of money laundering and terrorism financing to which it may be exposed, the Provider must consider at least the following factors:
1) nature, scale, diversity and complexity of the business;
2) the proportion of customers already identified as having an increased risk;
3) jurisdictions with which the provider operates, in particular, jurisdictions with increased vulnerability due to risk factors such as high crime, corruption, terrorism financing, regulation and limited supervision of the area of prevention and combating money laundering and terrorism financing;
4) distribution channels, including the extent to which the Provider performs operations directly with the customer or through agents and subsidiaries and the extent to which it relies on information provided by third parties to carry out client identification measures, the complexity of the payment chain and the settlement systems used between operators in the payment chain, the use of

technology and the extent to which agent networks are used;
5) internal audit and internal regulations;
6) the volume and size of the Provider's transactions, taking into account his usual business and the profile of his clients.

## Chapter IV
## CUSTOMER DUE DILIGENCE MEASURES

*Section 1*

*Customer acceptance procedures*

18. The customer acceptance procedures will contain identifying and verifying the customer and, the customer's beneficial owner, on the basis of reliable, independent information, data or documents. It also includes understanding the purpose and nature of the business relationship and, in high-risk situations, obtaining additional information.

19. 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 Provider's manager responsible for the implementation and compliance with the requirements for the prevention and combating of money laundering and terrorist financing.

20. The Provider shall not enter into business relations with persons, groups or entities involved in terrorist activities and the proliferation of weapons of mass destruction, specified in art. 34 par. (11) of the Law No 308 of 22 December 2017 on the Prevention and combating of money laundering and terrorism financing. The Provider 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 pertaining to the case.

21. The customer acceptance procedures will take into account the risks of money laundering and terrorist financing identified by the provider.

*Section 2*

*Customer due diligence measures*

22. The Provider shall, depending on the risk, apply customer due diligence measures:
1) when establishing business relationship with the customer;
2) in the case of all occasional transactions exceeding 20000 MDL, including those carried out by means of electronic equipment, 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 200000 MDL;
3) when there is a suspicion of money laundering or terrorism 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;

$22^1$. Depending on the level of risk involved, taking into account the type of customer, country (jurisdiction), business relationship, product/service offered or transaction carried out, distribution network, etc., the provider shall apply standard, simplified or enhanced due diligence.

23. By way of derogation from item 22, based on a proper risk assessment demonstrating a low-level risk of money laundering and terrorism financing, the Provider, 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:
1) the maximum amount of electronic deposit does not exceed 5000 MDL;
2) 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;
3) the payment instrument is used exclusively for the acquisition of goods or services;
4) the payment instrument cannot be funded with anonymous electronic money (which cannot be attributed to an identified person);
5) the issuer regularly monitors the transactions or the business relationship to enable the detection of suspicious transactions.

24. When applying the standard due diligence relating to customers in the cases referred to in item 22, the provider shall obtain at least the following information:
1) for customers - natural persons:
a) name and surname;
b) date and place of birth;
c) citizenship and ID card data (IDNP, series and number, date of issue, code of the issuing organ (if any) or other unique indents of an identity document containing the holder's photograph);
d) permanent and/or residence address;
e) telephone number, faximile, e-mail address (if available);
f) resident/non-resident status.
g) the occupation, the position held and/or the name of the employer;
h) the source of the income;
i) identification of the beneficial owner;
j) purpose and nature of the business relationship or occasional transaction (purpose of entering into the business relationship or occasional transaction, type of product and service requested, type of transactions, volume of assets expected to be deposited, volume and frequency of expected transactions, potential duration of the business relationship;.
2) for customers – legal persons, individual entrepreneurs and trusts or similar legal arrangements:
a) the name, the legal form of organization, the act of incorporation, the fiduciary act and the act on the state registration;
b) headquarters/business address;
c) the state identification number (IDNO), 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 the registered office (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) rights and obligations of the management body of the company arising from the primary registration documents or the constitutive act;
$g^1$) for trusts and similar legal arrangements, the identity of the founder, administrator, protector (if any), beneficiaries or classes of beneficiaries and any other persons who ultimately exercise

effective control (in the case of other types of legal constructions similar to trusts - the identity of persons holding equivalent positions;
h) the nature and purpose of the activity, their legitimacy;
i) the purpose and nature of the business relationship or occasional transaction (purpose of entering into the business relationship or carrying out the occasional transaction, type of product and service requested, type of transactions, volume of assets expected to be deposited, volume and frequency of transactions expected, potential duration of the business relationship).;
*[Item 24 amended by NBM Decision No 38 of 11.03.2021, in force on 02.07.2021]*

25. The Provider 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 Provider shall apply the measures described in item 24 sub-item 1).
*[Item 25 amended by NBM Decision No 38 of 11.03.2021, in force 02.07.2021]*

26. 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 Provider shall determine the beneficial owner on the basis of the appropriate registration documents. If there are no grounds for suspicion regarding the concealment of information on the beneficial owner and if after exhausting all possible means established according to item 25, it is found that no person meets the legal conditions to be identified as the beneficial owner (no natural person is not a majority shareholder or does not exercise direct or indirect control in other ways), as an exception, the natural person holding the position of client administrator is considered the beneficial owner. The provider keeps all the information and documents accumulated in the process of determining the beneficial owner of the customer – legal person, including those proving the exhaustion of all possible means of identification, and presents them, upon request, to the National Bank of Moldova and Office for the Prevention and Fight against Money Laundering.When identifying the beneficial owner of for-profit (commercial) legal entities, non-commercial institutions, trusts or similar legal arrangements or other types of legal entities (including those managing and distributing funds), the provider shall take into account the identification criteria set out in Article $5^2$ of Law No 308/2017 on Prevention and Combating Money Laundering and Terrorist Financing and the Guidelines of the Office for Prevention and Fight against Money Laundering on the identification of the beneficial owner.
*[Item 26 amended by NBM Decision No 38 of 11.03.2021, in force 02.07.2021]*

27. When the client or holder of the controlling interests 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 transparencyto 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 Provider obtains relevant identification data from public registers, from the customer or from other reliable sources..
*[Item 27 in the wording of NBM Decision No 38 of 11.03.2021, in force 02.07.2021]*

28. The Provider shall determine whether the person who opens the payment account or initiates a business relationship acts on his behalf (the person's statement of the beneficial owner) and if the opening of the payment account or the initiation of the business relationship is carried out by the empowered person, the provider shall request the Power of Attorney, certified in the manner

prescribed by the law. The Provider shall apply CDD measures to establish the identity of the authorized representative, as well as assesses the necessity of applying enhanced precautionary measures in accordance with the provisions of this Regulation.

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

30. The Provider shall verify the identity of a customer and his beneficial owner prior to establishing a business relationship with the customer or or conducting a transaction set out in item 22 sub-item 2).

31. In order to verify the identification information provided for the customer and the beneficial owner, the Provider shall use documents, data and information obtained from reliable and independent sources. The applied measures shall be proportionate to the risk associated with the customer and the types of submitted documents. For this purpose, the Provider 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 provider/bank;
2) when dealing with customers who are legal persons and trust or similar legal arrangements - by any appropriate method depending on the degree of associated risk, so that the Provider can assure the veracity of the information, such as:
a) to verify a legal existence of the legal person 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, a fiduciary act;
c) to verify in public or private databases information on the customer's existing business relationships;
d) to examine the latest financial reports, 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 provider/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 or the individual entrepreneur;
3) for the beneficial owner – the measures provided in sub-item 1).
4) where a person is empowered on behalf of the customer to open an account or to carry out

transactions, the Provider shall verify the identity of the customer and the identity of the person in whose name it operates by using the same procedures described in this Regulation.
*[Item 31 amended by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]*

32. 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 Provider in accordance with the established internal procedures. The documents shall be submitted by the client in original or in copy (photocopy) legalized according to the applicable legislation. In the case of presentation of copy documents (photocopies) that are not properly authenticated, the provider shall solicit the submission of the original documents to corroborate the information and data presented. In the case of remote identification and verification of the Customer's identity, the Provider shall request and obtain the necessary information and documents in accordance with the Regulation of the National Bank of Moldova on the requirements for identification and verification of the Customer's identity by electronic means.

33. Throughout its business relationship, the Provider shall review and update the information on the identification of customers and beneficial owners according to the associated risk. It updates the information as necessary, considering relevant factors, but at least for high-risk customers - annually, for medium-risk customers - every 2 years, and for low-risk customers - 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 normative requirements regarding the precautionary measures and / or the change of the relevant circumstances regarding the client..
*[Item 33 in the wording of NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]*

## *Section III*
## *Monitoring of the customer's activity and transactions*

34. The Provider should adjust the scale of the client's activities and operations monitoring measures in accordance with the institutional risk assessment and individual risk profile of the clients. Increased monitoring is applied to high-risk situations. Monitoring systems need to be reviewed periodically, but not less than once a year.

35. Operations initiated/performed by the Provider's agent must be monitored periodically under the same conditions as the Provider's operations. Monitoring must be performed by the Provider individually or in collaboration with that agent, on the basis of a concluded agreement and under the control of the provider.

36. The Provider who provides services through paying agents should include them in the internal program for preventing and combating money laundering and terrorism financing and monitor their compliance with the Provider's program.

37. The Provider shall continuously monitor the customer's activities, transactions 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 Provider, the customer's declared activity and the risk level associated with the customer. The examination of transactions requires the Provider to have in place at least those mechanisms / IT solutions, including the automated ones, for detecting 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. A particular attention should be paid to transactions that exceed the established value limits and transactions that have no clear economic purpose ;
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) identification of suspicious activities or transactions, including potential ones, as well as of sources of funds used in these activities and transactions;
5) reporting to the responsible person of the information on risks identified with respect to the customers' accounts and transactions, including for high-risk customers;
6) a real-time monitoring of all transactions (payments) 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.

38. The responsible manager of the Provider is responsible for documenting, storage and communicating with the relevant staff the results of the monitoring, as well as any problems that arise and their resolution.

39. The Provider shall refrain from executing any operations and transactions in financial means, 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.

40. The Provider shall apply the provisions specified under item 39 at the solicitation of the Office for Prevention and Fight against Money Laundering or on its own initiative. When acting on its own initiative while applying the requirements of item 39, the Provider shall inform immediately, but not later than within 24 hours, the Office for the Prevention and Fight against Money Laundering of the decision taken.

41. When applying the provisions of item 39, the Provider, may 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 implied assets.

42. The measures applied according to the provisions of item 39 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 exempt the provider from the obligations laid down in art. 5 par. (3) of Law No 308 of 22 December 2017 on prevention and combating money laundering and terrorism financing and in the internal program, elaborated in accordance with item 11.

43. The Provider shall commit:
1) not to carry out any operation or transaction, including through a payment account, or to enter into business relationship if the Provider cannot ensure compliance with the provisions of items 24, 25, 30,31, and 37;
2) in the case of an existing business relationship, to terminate the business relationship if the Provider cannot ensure compliance with the provisions of items 24, 25, 30, 31, and 37;
$2^1$) where there is a suspicion of money laundering or terrorist financing and the Provider reasonably considers that compliance with the requirements of items 24, 25, 30, 31, and 37 would result in a breach of the duty of confidentiality, not to complete the process of applying the due diligence measures in relation to the prospective customer.

3) in conditions specified in sub-items (1), (2), and ($2^1$) hereto, to submit to the Office for the Prevention and Fight against Money Laundering, in accordance with the art. 11 of Law No308 of December 22, 2017 on the Prevention and combating of money laundering and terrorism financing, special forms developed for the reporting of suspicious activities or transactions. In this case, the Provider shall be relieved from the obligation to provide explanation to the customer on the reasons for its refusal to do business with the customer.

44. The Provider shall not open or maintain anonymous accounts or accounts in fictitious names, shall not issue or accept payments carried out by using anonymous prepaid cards, shall not establish or continue a business relationship with a fictitious partner (fictitious institution) or a partner (institution) known to allow to another fictitious partner (fictitious institution) to use its accounts or to provide anonymous accounts for the use of its customers.

$44^{1.}$ The Provider shall not open and maintain accounts for/with virtual asset Providers in other countries and non-resident client accounts for the purpose of conducting transactions to/from virtual asset Providers in other countries.

*Section 4*
*Information obtained from third parties*

45. The provider may use the information held by third parties to carry out the measures provided for in points 24, 25, 30 and 31 under the following conditions:
1) third parties represent the reporting entities provided in Article 4 paragraph (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, including customer due diligence and data retention measures and;
2) third parties are not residents in high-risk jurisdictions.
*[Item 45 in the wording of NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]*

$45^1$. Providers who use third parties have effective procedures in place to ensure that they obtain from these third parties immediately:
1) all necessary information related to the measures provided for in points 24, 25, 30 and 31;
2) upon request, copies of identification data and other documents related to the measures provided in points 24, 25, 30 and 31, including data obtained by means of electonic means.
*[Item $45^1$ introduced by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]*

46. The Provider shall bear ultimate responsibility for the implementation of the measures set out in items 24, 25, 30 and 31, in case of recourse to third parties.
*[Item 46 amended by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]*

## Chapter VI
## SIMPLIFIED CUSTOMER DUE DILIGENCE MEASURES

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

48. Simplified CDD measures represent CDD measures referred to in items 22 and 23 applied under a simplified procedure corresponding to the low degree of risk of money laundering and terrorism financing, which include:
1) the limitation of obtaining customer identification data by applying a simplified customer

verification procedure;
2) the limitation of obtaining specific information or taking specific measures regarding the purpose and nature of the business relationship and deducting the purpose and nature of the business relationship from the type of transaction or business relationship established;
3) verification of the identity of the customer and the beneficial owner after the establishment of the business relationship, when this is necessary in order not to interrupt normal business practices;
4) reduction of the frequency of customer identification updates in the case of an established business relationship;
5) a reduced degree and scale of ongoing monitoring and control of transactions, based on a reasonable amount limit.
If the identity of the customer and the beneficial owner has not been verified until the establishment of the business relationship, the Provider 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 Provider 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 48 amended by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]*

49. Based on its own assessment and in accordance with the results of the national risk assessment, the Provider shall set out the factors that generate lower risk of money laundering and terrorism financing and which determine the application of simplified CDD measures, including at least the following factors:
1) business relationships/clients and/or products/services established in the Law no. 308 of 22 December 2017 on the Prevention and combating money laundering and terrorism financing;
2) reduced amounts for payments, deposit or cash withdrawal;
3) number of limited payments, deposit or redemption, including withdrawal of cash over a certain period of time;
4) a payment account that can store only limited amounts of funds;
5) the product or service can only be used nationally;
6) the product or service is accepted by a limited number of agents whose business is familiar to the provider;
7) money means are accepted as a means of payment for limited types of services or low-risk products;
8) the product is only available to certain customer categories, such as social benefits recipients or staff members of a company using the product to cover corporate expenses.
Based on the assessment of money laundering and terrorism financing risks at national level and based on criteria and factors established by the supervising organ, the provider accumulates sufficient information to identify whether the client, transactions or business relationships meet the conditions mentioned above.
*[Item 49 amended by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]*

49[1]. On the basis of an appropriate risk assessment demonstrating a low risk of money laundering and terrorist financing, the provider may apply simplified prudential measures in relation to electronic money for transactions for the purchase of goods or services, except for redemption or cash withdrawal of the monetary value of electronic money and for remote payment transactions exceeding MDL1000 per transaction, provided that the following conditions are met:
a) the maximum value stored electronically does not exceed MDL 3000;
b) the value of monthly transfers does not exceed MDL 3000; and

c) the issuer (Provider) carries out sufficient monitoring of the transactions or business relationship to detect suspicious transactions.

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

## Chapter VII
## ENHANCED CUSTOMER DUE DILIGENCE MEASURES

51. In order to enforce the legislation on prevention and combating money laundering and terrorism financing, the Provider 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 performed operations, 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.

52. Based on its own assessment, the Provider shall set out the factors that generate an increased degree of risk of money laundering or terrorism financing and which determine the application of enhanced CDD measures. The factors that generate increased risk are:
1) business relationships/clients and/or products/services established in the Law no. 308 of 22 December 2017 on Prevention and combating money laundering and terrorism financing;
2) products or services that allow large or unlimited cash operations;
3) the transaction is in cash;

3[1]) customers and transactions to/from virtual asset service providers authorised in other countries;
4) transactions are carried out from one or more payers from different countries to a local beneficiary;
5) the client performs operations for someone else (on behalf of another person);
6) the transactions made have no economic meaning;
7) the customer always performs transactions below the reporting threshold;
8) the use of the service by the client is unusual, for example sending or receiving money to or by itself or sending funds immediately after receiving them;
9) the client seems to know little or is reluctant to provide information about the beneficiary;
10) some of the provider's customers transfer money to the same beneficiary or appear to have the same identification information, such as the address or telephone number;
11) the operation is not accompanied by the necessary information about the payer or the beneficiary;
12) money sent or received is in contradiction with the client's income (if known);
13) business partners in foreign jurisdictions;
14) other factors identified in the risk assessment and by the supervisors.

53. The provider shall apply enhanced customer due diligence, in addition to those set out in item 24, in situations which, by their nature, may present a high risk of money laundering or terrorism financing, at least by:
1) obtaining additional information about the customer and beneficial owner (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 of 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 funds and property;
4) obtaining information on the purpose of the activity or transaction whether intended, currently

carried out or completed;
5) obtaining the approval of the responsible person and/or of the head of the branch for the establishment or continuation of the business relationship;
6) enhanced and permanent monitoring of the business relationship ensured through an increased frequency of checks performed, and by selecting activities and transactions that require additional examination and by requesting additional information confirming the legality of the operations and the adequacy of these types of activity declared;
7) 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 money laundering and terrorism financing;
8) to alert customers whose activities or transactions are exposed to a higher risk of money laundering and terrorism financing on the need to increase their business partner due diligence measures;
9) 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 money laundering and terrorism financing by the partner/correspondent institution;
10) additional measures specified in items $53^1$ to $56^2$.
*[Item 53 amended by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]*

$53^1$. When dealing with resident customers who crarry out transactions with/to virtual asset service providers authorised in other countries, the provider shall:
1) open special accounts for resident clients for the purpose of carrying out these types of transactions;
2) shall not allow the execution of transactions with a cumulative volume exceeding the equivalent of MDL 50 000 per month for each resident client;
3) does not allow the execution of occasional transactions of this type;
4) implement specialised IT solutions for the purpose of enhanced monitoring of this type of transactions, including for determining the origin of the goods involved and ensuring the traceability of transactions.

54. In case the customer cannot personally be present at the identification (e.g. in the relationship by correspondence, telephone, e-mail, internet or other electronic means), the Provider applies enhanced CDD measures by using such procedures as electronic signature, biometric methods, session keys, etc. At his first visit to the Provider, the customer has to present documents and information according to the requirements of the present Regulation. In addition, the Provider shall apply one or all of the following measures:
1) request the customer’s identification documents issued by a competent authority or organ, including specimen signature, other documents, as appropriate, for the customer's file;
2) take measures to ensure authenticity of electronic documents transmitted to the Provider;
3) use the information provided by a partner (provider, agent, bank) in which the customer holds an account and which applies at least similar CDD measures and is subject to effective supervision;
4) require the first payment to be made on behalf of the customer through an account from another provider/bank that applies at least similar CDD measures and is subject to an effective supervision, where appropriate;
5) establish and maintain a method of contacting the client, independent of the way remote client operations are performed.

55. In relationships with correspondent institutions, the Provider shall accumulate sufficient information about its partner to fully understand its field of activity. For this purpose, the Provider shall:
1) obtain information at least on:
a) the governance body of the correspondent institution, its main activities, its business address and the measures it applies to prevent and combat money laundering and terrorism financing;
b) the purpose of setting up a bank account;
c) the reputation of the correspondent institution including whether it has been the subject of an investigation or any remedial action relating to money laundering or terrorist financing from publicly available sources;
2) assess how appropriate and effective the policies of the corresponding institution are in preventing and combating money laundering and terrorism financing;
3) establish the correspondence relationship after obtaining the approval by the responsible administrator of the Provider;
4) obtain document(s) listing responsibilities of the correspondent institution in the field of the prevention and combating 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) makes 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.

56. In case of business relationships or transactions with politically exposed persons, their family members or persons known to be close associates of politically exposed persons, the Provider, in addition to the measures specified in item 24, shall apply the following measures:
1) the development and implementation of appropriate risk management systems, including risk-based procedures to determine whether a client, potential client or beneficial owner of a client is a politically exposed person;
2) obtaining the approval of the Provider's responsible person for the establishment of a business relationship and for the continuation of the business relationship with such clients;
3) adoption of appropriate measures for establishing the source of wealth and of goods involved in the business relationship or transactions with such clients;
4) ensuring an enhanced and continuous monitoring of the business relationship.

*[Item 56 completed by NBM Decision No 38 of 11.03.2021, in force 02.07.2021]*

In business relationships or transactions with politically exposed persons, their family members or persons known to be close associates of politically exposed persons, the Provider shall apply the enhanced due diligence measures set out in items 1) to 4) for a period of 12 months after the termination of their significant national or international public office. At the end of that period, the provider shall, on the basis of a risk assessment determining whether or not the person concerned continues to present risks in relation to politically exposed persons, apply the due diligence measures in accordance with the risk identified.

56[1]. In business relations or in the case of transactions with customers and financial institutions from high-risk countries (jurisdictions) assigned/monitored by the FATF, in addition to the enhanced due diligence measures provided for in this Chapter, the Provider shall apply in addition, in accordance

with the required actions by the FATF 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 (jurisdiction) or, as the case may be, its termiantion;
2) assessing, modifying or, as the case may be, terminating the relationship with the corresponding institution in the high-risk country (jurisdiction);
3) carrying out external audit for the Provider's branches located in the countries concerned.
4) closure of the Provider's branch located in the countries (jurisdictions) concerned.
*[Item 56[1] introduced by NBM Decision No 38 of 11.03.2021, in force 02.07.2021]*

56[2]. The measures provided for in item 56[1] as well as other enhanced due diligence measures shall also be applied if they are requested by the Office for Prevention and Fight against Money Laundering or by the supervisory authority.
*[Item 56[2] introduced by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]*

## Chapter VIII
## PROVIDER'S AGENTS

57. The provider applies due diligence measures to agents in order to know their legal form and property and control structure and will establish business relationships with agents who will implement the law requirements on prevention and combating money laundering and terrorism financing. The requirements described in this chapter will not apply to agents who are licensed reporting entities, regulated and supervised by the National Bank of Moldova, i.e. licensed banks and non-bank payment service providers. The internal procedures of the Provider upon its agents must include aspects such as:
1) when initiating a business relationship, it is necessary to identify the agent and apply due diligence measures regarding its previous activity, such as a recent change from the current relationship with other providers, regardless of whether the agent provides payment services on behalf of one or more providers, the duration of the activity in the field, the property structure, the financial soundness, the registration of the agent in the register of payment companies / postal service providers and the register of companies issuing the electronic money of the agent.
2) obtaining additional appropriate information to understand the agent's activity, such as providing services to other providers, information on prior compliance with the legislation, nature and expected level of operations, number of customers and geographical exposure.
3) when approving a new agent, it is necessary to organize training for the staff of the agent on legal requirements in the field of money laundering and terrorism financing, the program, internal policies and procedures for preventing and conformity for combating money laundering and terrorism financing with the provider's one. Accordingly, these trainings should be organized periodically.
4) provides guidance and assistance to the provider's agent for complying with the provider's program of prevention and combating money laundering and terrorism financing.
5) ensuring compliance with legislation such as reporting suspicious activities, high value operations, monitoring of risks related to the domain, reporting and keeping records through the periodic verification program.
6) ensuring a prompt response and remediation of risk situations by remote check method and on-site at the agent and, where appropriate, organizing additional training, suspension or termination of the business relationship with the agent.

58. The provider monitors the agent's activity in order to ensure its proper implementation of the requirements for preventing and combating money laundering and terrorism financing. The degree and nature of paying agent's monitoring depends on the volume of agent's operations, the method of monitoring used (manual, automatic or combined), the countries where the money is transferred, the results of the previous monitoring (if applicable) and the type of activity. In applying a risk-based approach, the degree of monitoring will be based on the perceived risks, both external and internal, associated with the agent, such as the products or services provided by the agent, its location and the nature of the activity.

59. The provider monitors the agent's activity under a risk-based approach and identifies specific risk criteria to determine which paying agent activities need to be reviewed. The specific criteria defined for this purpose should be periodically reviewed to determine whether they are appropriate for the established risk levels.

60. For the purpose of redressing and minimizing specific risks deriving from the activity of an agent, the Provider shall implement at least the following measures:
1) creating and maintaining a register of high-risk agents.
2) the need to apply enhanced due diligence measures in appropriate cases.
3) applying limits to cash transactions.
4) providing specific trainings for paying agents specific suspicion indicators in order to improve their knowledge of the field and reporting standards.

## Chapter[1] IX
## REQUIREMENTS ON INFORMATION ACCOMPANYNG TRANSFER OF FUNDS

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

62. The provisions of this chapter shall not apply to transfers of funds carried out by using a payment card, an electronic money instrument, a mobile phone or any other digital or IT prepaid or postpaid device with similar characteristics, provided the following conditions are met:
1) the card, electronic money instrument or device is used exclusively to pay for goods or services;
2) the number of the card, electronic money instrument or device accompanies all money transfers resulting from the transaction.
However, this chapter shall apply where a card, electronic money instrument, a mobile phone or any other digital or IT prepaid or postpaid device with similar characteristics is used to transfer funds between natural persons acting as consumers for purposes other than trade, business or professional activity, including industrial and handicraft.

63. This chapter shall not apply to a transfer of funds when it:
1) involves cash withdrawal from the payer's own payment account;
2) constitutes a transfer of funds to a public authority as payment for taxes, fines or other levies;
3) is carried out between payment service providers, as the payer and the payee of the payment, acting on their own behalf;
4) is carried out through cheque images exchanges, including truncated cheques.

63[1]. This chapter shall not apply to:

[1] *Chapter IX amended by NBM Decision No. 8 of 13.01.2025, in force 16.01.2025*

1) the services listed in art. 2 para. (2) (1)-(13) and (15) of the Law no. 114/2012 on payment services and electronic money;
2) persons that have no activity other than to convert paper documents into electronic data and that do so pursuant to a contract with a payment service provider, or to persons that have no activity other than to provide payment service providers with messaging or other support systems for transmitting funds or with clearing and settlement systems.

*Section 1*
*Obligations of provider of the payer*

64. The payer's provider shall ensure that the transfers of funds are accompanied by the following information regarding the payer:
1) the full name of the payer (name/surname and name):
2) the number of the payer's payment account;
3) the payer's address, including the name of the country, identity document number and customer identification number (ex. IDNP/IDNO) or, alternatively, the payer's date and place of birth; and
4) the current LEI of the payer, subject to the existence of the necessary field in the relevant payments message format and where provided by the payer or, in its absence, any available equivalent official identifier.

65. The payer's provider shall ensure that the transfer of funds is accompanied by the following information regarding the payee:
1) the full name of the payee (name, surname and name);
2) the number of the payee's payment account; and
3) the current LEI of the payee, subject to the existence of the necessary field in the relevant payments message format and where provided by the payer or, in its absence, any available equivalent official identifier.

66. By way of derogation from item 64 sub-item 2) and item 65 sub-item 2), in the case of transfers not effected from or to a payment account, the payer's provider shall ensure that the transfer of funds is accompanied by a unique transaction identification code instead of the payment account number(s).

67. Before transferring funds, the payer's provider shall verify the accuracy of information specified in item 64 and, where applicable, in item 66, based on documents, data or information obtained from a reliable and independent source, taking into account the provisions of this Regulation.

$67^1$. The obligation to verify the accuracy of the information on the payer referred to in item 67 shall be deemed to be fulfilled if the payer's provider applies due diligence measures in order to verify the identity if the payer, updates and retains the information on the payer in accordance with the provisions of Chapters V-VII and XI.

68. By way of derogation from item 64 and, where applicable, without prejudice to the information required in accordance with the Regulation on credit transfer, direct debiting, and the assignment of IBAN codes, approved by the Decision of the Executive Board of the National Bank of Moldova no. 108/2023, where the payment service provider of the payee is established outside the Republic of Moldova, payer's provider shall ensure that the international transfers of funds with a value not exceeding 20000 lei and do not appear to be linked to other transfers of funds which, together with the transfer in question, would exceed 20000 lei, are accompanied by at least the information on the

payer and payee's names and the payment account number of the payer and of the payee or, when item 66 is applicable, the unique transaction identifier.

68[1]. By way of derogation from item 67, in the situation provided by item 68, the payer's provider has the obligation to verify the information on the payer only when it:
1) has received the funds to be transferred in cash or in anonymous electronic money; or
2) has reasonable grounds for suspecting money laundering or terrorist financing.69. In the case of the batch file transfers made by a single payer to several payees whose payment service providers operate outside the Republic of Moldova, the provisions of item 64 shall not apply to the individual transfers bundled together therein, provided that the batch file transfer contains the information referred to in items 64, 65 and 66, that this information has been verified in accordance with items 67 and 67[1], and that the individual transfers are accompanied by the number of the payer's payment account or, where item 66 is applicable, by the unique transaction identifier.

69[1]. By way of derogation from item 64 and 65 and, where applicable, without prejudice to the information required in accordance with the Regulation on credit transfer, direct debiting, and the assignment of IBAN codes, approved by the Decision of the Executive Board of the National Bank of Moldova no. 108/2023, where all payment service providers involved in the payment chain are established in the Republic of Moldova, transfers of funds shall be accompanied by at least the payment account number of the payer and payee, or where item 66 applies, the unique transaction identifier. In this case, within maximum three working days of receiving a request for information from the payment service provider of the payee or from the intermediary payment service provider, the payer's provider shall make available the following information:

1) on the payer or the payee in accordance with items 64-66, for transfers of funds exceeding 20000 lei, whether such transfer is carried out in a single transaction or in several transactions which appear to be linked;

2) the name of the payer and of the payee and the payment account number of the payer and of the payee or, where item 66 applies, the unique transaction identifier. In this case, the obligation to verify the information on the payer corresponds to that provided for in item 68[1].

70. The Provider shall not execute any transfer of funds unless full compliance with the provisions of items 64-69[1] has been ensured.

*Section 2*
*Obligations of the provider of the payee*

71. The payee's provider shall put in place and implement effective procedures, including, where appropriate, controls after or during the transfer, in order to determine whether the fields relating to the information on the payer and payee in the messaging or payment and settlement system used to effect the transfer of funds have been filled in using character or inputs compatible in accordance with the conventions of that system and in accordance with the requirements of items 64 sub items 1)-3), 65 sub items 1)-2), 66, 68, 69 and 69[1]of this Regulation.

71[1]. In case of transfer of funds in the amount exceeding 20000 lei, whether those transfers are carried out in a single transaction or in several transactions which appear to be linked, prior to crediting the payee's account or making funds available to him, the payee's provider shall verify the accuracy of the information on the payee referred to in items 65 sub items 1)-2), 66, 68, 69 and 69[1]

based on documents, data or information obtained from a credible and independent source, taking into account the provisions of this Regulation.

72. In case of transfers of funds which are not exceeding the threshold established in item $71^1$, the payee's provider shall verify the completeness and accuracy of the information on the payee referred to in item $71^1$ only in the following situations:
1) when the payment is made in cash or in anonymous electronic money; or 2) when there are reasonable grounds for suspecting money laundering or terrorist financing.

$72^1$. The obligation to verify the completeness and accuracy of the information on the payee referred to in items $71^1$ and 72 shall be deemed to be fulfilled if the payee's provider applies due diligence measures in order to verify the identity of the payee, updates and retains the information on the payee in accordance with the provisions of Chapters V-VII and XI.

73. The payee's provider shall apply effective risk-based procedures, including procedures referred to in item 11, based on the risk-sensitive basis regarding customer due diligence measures, to determine whether to execute, reject or suspend a transfer of funds where complete information on the payer and the payee is missing and for taking the appropriate follow-up actions.

74. Where upon the receipt of funds the payee's provider finds that the information specified in items 64 sub items 1)-3), 65 sub items 1)-2), 66, 68, 69 and $69^1$ is missing or is incomplete, or has not been filled in using characters or inputs admissible in accordance with the conventions of the messaging or payment and settlement system as referred to in item 71, the provider shall reject the transfer or request the required provision information on the payer and the payee before or after crediting the payee's account or making the funds available to them, depending on the associated risk.

75. Where a payment service provider making the transfer repeatedly fails to provide the required information on the payer or payee, the payee's provider shall take steps which may first include issuing warnings and setting deadlines, before proceeding to either rejecting any transfer of funds executed by this payment partner, or deciding, where appropriate, to restrict or terminate the business relationship with it. The provider of the payee shall inform the National Bank of Moldova about those omissions, as well as on the taken measures.

$75^1$. The Provider, when acting as the provider of the payee or, where applicable, when is acting as both the payer's and payee's provider, shall take into account all the missing information on 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.

*Section 3*
*Obligations of intermediary provider*

76. The intermediary provider shall put in place and implement effective procedures, including, where appropriate, controls after or during the transfers, to determine whether the fields relating to the information on the payer and payee in the messaging or payment and settlement system used for the transfer of funds have been filled in using characters or inputs compatible in accordance with the conventions of that system and in accordance with the provisions of items 64 sub items 1)-3), 65 sub items 1)-2), 66, 68, 69 and $69^1$ 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 77 repealed by NBM Decision No. 8 of 13.01.2025, in force 16.01.2025]*

78. The intermediary provider shall establish effective risk-based procedures for determining whether to execute, reject or suspend a transfer of funds where the required information on the payer and the payee is missing and for taking appropriate follow-up actions.

79. Where upon the receipt of funds the Provider finds that the information specified in items 64 sub items 1)-3), 65 sub items 1)-2), 66, 68, 69 and $69^1$ is missing or is incomplete, or has not been filled in using characters or inputs compatible in accordance with the conventions of the messaging or payment and settlement system, as referred to in item 71 and 76, the Provider shall reject the transfer or request the required information on the payer and the payee before or after the transmission of the funds, depending on the associated risk.

80. Where the payment service provider making the transfer fails to provide repeatedly the required information on the payer or payee, the payee's provider shall take steps which may first include issuing warnings and setting deadlines, before proceeding to either rejecting any transfer of funds executed by them, or deciding, where appropriate, to restrict or terminate the business relationship with this provider. The intermediary provider informs the National Bank of Moldova about these omissions, as well as about the measures taken.

$80^1$. The intermediary provider shall take into account missing information on the payer or the payee when assessing whether a transfer of funds or any related transaction is suspicious and whether it should be reported to the Office for Preventing and Combating Money Laundering in accordance with art. 11 of the Law no. 308/2017 on the prevention and combating money laundering and financing of terrorism.

## Chapter X
## ACTIVITY AND TRANSACTION REPORTING

81. The Provider commits to report the Office for the Prevention and Fight against Money Laundering, in accordance with Article 11 of Law No 308/2017, of:
1) any suspicious goods, activities or transactions suspicious to be related to money laundering, to predicate 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 Provider has identified any action or circumstances that raise suspicions;
2) any cash transactions or operations, with a value exceeding MDL 200 000 (or its equivalent), carried out through one or more related transactions during a month, starting on the first day and ending on the last day of the month – up to the 5th day of the month following the month in which the operations or transactions were carried out
3) any transactions conducted through an operation with a value of at least MDL 200 000 (or its equivalent) – and which does not fall under the provisions of subitem 2) – by the 10th of the month following the month in which the transactions were carried out.

4) transactions made through money remittance systems with a value of at least MDL 40 000 (or its equivalent) - within 5 days from the moment of the transaction.

*[Item 81 amended by the Decisions of the NBM No 324 of 20.12.2018, in force as of 04.02.2019]*

82. The Provider 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 terrorism financing, which were made known to the entire staff and which provide for the reporting by personnel of all suspicious activities and transactions;
2) systems for detecting suspicious activities and transactions according to the established criteria and indices, including by competent authorities;
3) procedures for informing the responsible administrator on issues related to the prevention and combating of money laundering and terrorism financing.

83. The Provider shall, as appropriate, inform the National Bank in accordance with Law No. 308 of 22 December 2017 on the prevention and combating money laundering and terrorism financing, suspicious activities and transactions, fraud cases that essentially affect the provider's security, stability or reputation.

## Chapter X
## DATA STORAGE

84. The provider shall keep all documents, data and information obtained under this Regulation, including those obtained under due diligence measures concerning customers and beneficial owners, information obtained by electronic means as part of the romote customer identification and identity verification process such as copies of identification documents, archives of primary accounts and documents, business correspondence, results of analyzes and research carried out, during the active period of the business relationship and for a period of 5 years from its termination or from the date of carrying out the occasional operations. The retained data must be sufficient to permit the reconstitution of each activity or transaction in the manner in which it is necessary to serve as evidence in criminal proceedings, contraventions and other legal proceedings.
*[Item 84 amended by NBM Decision No 38 of 11.03.2021, in force 02.07.2021]*

85. 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; files containing records of the monitored customer transaction and the transaction supporting documents;
4) keeping records of all conducted transactions "(type, volume, currency, destination, etc.), including complex and unusual transactions;
$4^1$) keeping records and information 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 85 completed by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]*

86. The Provider 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 relating to domestic and international transactions, are accessible and available, in an opeartional manner, 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 paragraph (2) of Law No 308 of 22 December 2017 on the Prevention and combating of money laundering and terrorism 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 XII
## INTERNAL CONTROL SYSTEM REQUIREMENTS

87. The Provider shall have in place internal control systems that will ensure the continuous compliance with the applicable regulatory acts and the existing internal program in the field of prevention and combating money laundering and terrorism financing, that will contribute to reducing the related risks.

88. The provider's internal control system depends on several factors including the nature, scale and complexity of the payment service provider's business, the diversity of its operations, including geographic diversity, customer base, product and activity profile, the degree of risk associated with each jurisdiction of its operations and distribution channels, that is, the extent to which the provider interacts directly with the customer or through the paying agents.

89. When establishing subsidiaries and branches in the territory of other states as well as during their activity, the Provider shall apply measures developed for the prevention and combating of money laundering and terrorism 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 terrorism financing, the Provider 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 Provider shall apply appropriate additional measures to mitigate the risk of money laundering and terrorism 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 Provider'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 Provider'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 Provider if the rules of law of another country (jurisdictions) do not allow the implementation of the measures provided for in this item.

89[1]. In case of the opening of subsidiaries in other countries, at the level of the financial group, the internal control system and the program to prevent and combat money laundering and terrorist financing shall include, in addition to the elements set out in items 91-94, 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 terrorism 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 terrorism financing;
3) adequate requirements regarding the confidentiality of information subject to the exchange of professional secrecy and personal data, as well as the use and processing of such information.
*[Item 89[1] introduced by NBM Decision no. 38 of 11.03.2021, in force 02.07.2021]*

90. The provider who performs operations through agents should include them in their internal control systems for preventing and combating money laundering and terrorism financing and monitor them to comply with their provisions.

91. The internal control system shall include at least the following elements:
1) an independent audit conducted by the provider's staff or an audit firm/external auditor to verify the provider's compliance with the provisions regarding the prevention and combating of money laundering and terrorism financing. In this context, the audit shall include:
a) independent assessment of the program on prevention and combating of money laundering and terrorism financing and of the compliance with law requirements;
b) monitoring staff performance by compliance testing;
c) operations testing in case of necessity;
d) informing the responsible administrator on the assessment's results and recommending measures to be taken to minimize identified risks and shortcomings;
2) the appointment of person, who is administrator, as responsible for ensuring compliance with the applicable legislation on the prevention and combating of money laundering and terrorism financing (hereinafter referred to as "responsible person"). For this purpose, the responsible person shall have the following tasks:
a) to provide advice to the provider's employees on issues arising during the implementation of the program on the prevention and combating of money laundering and terrorism financing, including on the identification and examination of provider's customers and the assessment of the risk of money laundering and terrorism financing;
b) to take decisions based on the information received;
c) to take measures for reporting to the Office for the Prevention and Fight against Money Laundering in accordance with the law;
d) to organize trainings for the provider's employees in the field of the prevention and combating of money laundering and terrorism financing;
e) to collaborate with the audit entity/officers in view of verifying compliance of the provider's activity with the legislation in the field of the prevention and combating of money laundering and terrorism financing;
g) to perform other functions in accordance with this Regulation and the internal documents of the provider;
3) internal provisions on the liability and sanctioning of employees who deliberately do not inform / report about any suspicious activities or transactions to the responsible person or directly to the competent authority and / or personally facilitate carrying out of transactions, which are part of the money laundering and terrorism financing schemes.

92. The person conducting the provider's audit analyzes the implementation of the program for preventing and combating money laundering and terrorism financing by the provider and submits a report in writing on the results of the analysis performed to the responsible person of the provider.

93. The Provider shall have in place programs for recruiting and ongoing training of the staff in the field of prevention and combating money laundering and terrorism financing. The Provider shall

ensure that its personnel has appropriate knowledge, skills, including reputational ones, and abilities to effectively fulfil their responsibilities in the field of prevention and combating money laundering and terrorism financing.

94. The recruiting and training programs referred to under item 93 shall cover various aspects of the process of preventing and combating money laundering and terrorism 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 programs;
2) training of the frontline staff (employees who work directly with customers) in checking the identity of new clients, 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 terrorism financing;
5) the level of staff involvement in the prevention and combating of money laundering and terrorist financing process.
The curriculum of staff trainings must be adapted to the individual needs of each provider.

95. The Provider 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 XIII
## REQUIREMENTS FOR APPLICATION OF INTERNATIONAL RESTRICTIVE MEASURES

96. The Provider shall immediately apply restrictive measures related to terrorist activities and proliferation of weapons of mass destruction to assets, including those obtained from or generated by assets owned, held or controlled, directly or indirectly, in full or in common, 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 96 amended by NBM Decision No 38 of 11.03.2021, in force 02.07.2021]*

97. For the application of restrictive measures under item 96, the Provider 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 money laundering and terrorism financing and the Law no.25 of 4 March 2016 on the application of international restrictive measures, using in this purpose the Order of the Director of the Security and Intelligence Service on the lists of persons, groups and entities involved in terrorist activities;
2) procedures for screening / detection of designated persons or entities and of transactions /payments 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.

98. Upon identification of assets owned, including assets derived from or generated by such assets 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, the Provider shall undertake the following steps:
1) based on the decision of the Provider's responsible person, shall put on hold, for an indefinite period of time, the execution of operations and transactions, which are being prepared, attempted, implemented or already carried out direct or indirect for the benefit, in whole or in part, of any persons, groups and entities involved in terrorist activities and the proliferation of weapons of mass destruction subject to restrictive measures, legal persons/entities owned or controlled, directly or indirectly, by such persons, groups or entities, as well as persons, groups and entities acting on behalf of, or at the direction of, such persons, groups and entities;
2) immediately inform, but not later than within 24 hours after the application of the restrictive measures, the Office for the Prevention and Fight against Money Laundering, about its putting on hold, for an indefinite period of time, the execution of operations and transactions. 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 Provider's responsible person to put on hold, for an indefinite period of time, the execution of operations and transactions relating to identified assets;
3) where applicable, the Provider 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 98 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 98 sub-items 2) a) and b);
4) inform the National Bank of Moldova of the restrictive measures applied in compliance with the provisions of item 98 sub-item 2) a) and b).

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

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

## Chapter XIII
## OTHER DISPOSITIONS

101. Where a Provider 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 terrorism financing, the National Bank of Moldova imposes sanctions to the Provider in accordance with the legislation in force.

102. When applying the present Regulation, the Provider shall inform the National Bank of Moldova of any suspicious activities and fraud incidents posing risks for the bank's safety, stability or reputation.

[*Item 102 amended by the Decision of the NBM No 324 of 20.12.2018, in force as of 04.02.2019*]

*Annex is repealed*