Published on (https://www.bnm.md)

Expand Hide

31.12.2013

Recommendations on monitoring by banks of transactions and clients' activities to prevent and combat money laundering and terrorism financing, approved by the DCA of the NBM no. 256 of December 19, 2013

Published in the Official Monitor of the Republic of Moldova no.315-319/1938 of 31.12.2013

Approved by Decision of the
Council of Administration
of the National Bank of Moldova
no. 256 of 19 December 2013

RECOMMENDATIONS
on monitoring by banks of transactions and clients' activities to prevent and combat money laundering and terrorism financing

I. General provisions

1.The Recommendations on monitoring by banks of transactions and clients' activities to prevent and combat money laundering and terrorism financing (hereinafter the Recommendations) are aimed to provide methodological guidance to banks in the creation of effective internal mechanisms as to monitor the transactions and business relations, determine the scope and nature of the business relation, interpret the ordinary nature of clients' activities and to monitor complex transactions to prevent and combat money laundering and terrorism financing.

2.The Recommendations cover:
a) description of the main components of the monitoring of transactions and business relations;
b) procedures for determining the scope and nature of the business relation;
c) interpretation of the ordinary nature of activities;
d) determination of complex transactions.

3. The Recommendations are developed taking into account the Forty Recommendations of the Financial Action Task Force (FATF-GAFI), Wolfsberg Group documents related to monitoring of transactions and other related international documents in the field.
Terms and expressions used in these Recommendations have the meanings set out in the regulations related to the field. For the purpose of these Recommendations, the following terms and phrases shall be used:
real-time payment verification - the process of analyzing and determining the nature of payments before their execution to prevent their conduct in violation of penalties, prohibitions or other restrictions applied in the context of the law on preventing and combating money laundering and terrorism financing;
client screening - the verification of the presence of the name and surname/name and other data related to the client in the lists published in the Official Monitor or provided by the competent authorities with regard to the persons or entities involved in terrorism, extremism or their financing activities or other unlawful activities on which sanctions, prohibitions or other restrictions are applied in the context of the legislation on preventing and combating money laundering and terrorism financing.

transaction monitoring - automatic, manual or mixed verification process of the executed transactions in order to determine the ordinary or unusual nature thereof. The process is applied to both a single transaction as well as a chain of transactions, and if the transaction is suspected to be unusual, this shall be reported to the OfficeforPreventionandFightagainstMoney Laundering (hereinafter SPCSB), as provided by the legislation in force.
ordinary nature of activities - reasoning applied by the bank to determine whether the transactions made by clients are in accordance with the planned activities and operations, and / or information mentioned in the articles of incorporation;

5. The bank's system for transaction monitoring and determination of complex, unusual and suspicious transactions shall ensure the identification, evaluation and minimization of risks and vulnerabilities related to the bank's activity in preventing and combating money laundering and terrorism financing.

II. Monitoring of transactions and business relations

6. Banks shall implement appropriate processes to allow identification of transactions, unusual patterns of transactions and activities. As these will not be suspicious in all cases, banks shall analyze the transaction, their patterns and activities to determine the ordinary or suspicious nature thereof. Transactions and suspicious activities shall be reported to the SPCSB as required by the legislation in force. Therefore, the monitoring of activities and transactions by the bank is a measure to ensure the fulfillment of these requirements.

7. The purpose of transaction monitoring is to alert banks on activities that are unusual or potentially suspicious and require further examination. Therefore, the application of real-time payment verification methods and transaction monitoring will support the bank's efforts to provide services and products to individuals and legal entities in an adequate manner and will protect the bank from its use in money laundering and terrorism financing activities.

8. For an effective transaction monitoring system, the scope and complexity of monitoring process shall be determined in accordance with the associated risk. This means that the bank shall develop and implement different levels of monitoring, depending on the risk factors involved, such as the activities and operations of the bank subdivisions, clients' database and the place where it operates.

9. The risk profile of the bank may be different, depending on the proposed activities, products, or services. Application of transaction monitoring based on the risk profile shall reflect the risks involved in specific areas and lead to their reduction.

10. The main components in an efficient transaction monitoring system are:
a) client screening and real-time payment verification;
b) ongoing analysis of performed transactions to identify unusual activities and transactions.

11. Client screening and real-time payment verification involves examining the payment orders before their execution, with the purpose of identifying persons involved in terrorism activities or on which sanctions, prohibitions or other restrictions are applied in the context of the legislation on preventing and combating money laundering and terrorism financing. This activity shall be implemented including during the course of the business relationship.

12. To improve the quality of real-time payment verification, banks shall comply with the followings:
a) banks shall verify in real-time the transactions carried out as to identify the persons involved in terrorism activities, or on which sanctions, prohibitions or other restrictions are applied , according to the list published in the Official Monitor or provided by the competent authorities;
b) if the published or provided list is updated, banks shall apply verification measures when initiating a payment or during the course of the business relation;
c) banks shall rely on the lists published in the Official Monitor or those provided by the competent authorities;

d) the bank as an intermediary of transactions (paying provider) shall ensure real-time verification of information about the payment order issuer (payment issuer);
e) to minimize the large number of "false coincidences" and to maximize the operational effectiveness and efficiency, it is essential for the bank to take from the published or provided list relevant information such as: name of the person, date of birth, other unique identification indices;
f) the bank as payment service provider shall cooperate and rely on information provided by partners, according to the legislation in force, to complete the transaction in time and solve the existing problems related to potential penalties, prohibitions or other restrictions imposed in the context of the legislation on preventing and combating money laundering and terrorism financing, or to refuse to make such payments (transactions).

13. The transaction monitoring process within banks shall be incorporated into the bank's internal regulations on preventing and combating money laundering and terrorism financing. The principles shall be correlated with the risk of the bank business model, products and services provided and the nature of the clients.

14. Banks shall apply the risk-based approach in relation with their clients when monitoring clients' transactions. Thus, this process shall reflect the risk assessment within the bank by spheres of activity, products and services, and increased attention shall be given to the activity, transaction and / or the client involving a high risk.

15. Effective monitoring of transactions and activities requires the existence of:
a) an automated transaction monitoring system;
b) a system for generating alerts in the event of data disparity;
c) procedures describing the monitoring process;
d) procedures for regular review and establishment of limits;
e) procedures for review, determined by specific events, such as the approval of new types and methods of money laundering and terrorism financing, based on information received from the competent authorities.

16. Full or partial automation of the monitoring process is required in order to conduct an effective monitoring of transactions. The degree of automation may vary from one bank to another and will depend on the size, nature and complexity of each bank. Automated monitoring systems based on rules are able to identify unusual activities through appropriate setting of various parameters determined by the bank. These rules can be gradually personalized to the clients, depending on the changes in the bank's activity and methods of money laundering and terrorism financing.

17. Banks may use intelligent IT systems to update the clients profile, depending on the transactions performed. They may identify patterns of transactions by examining the correspondence between accounts, comparing the trading activity with the methods of money laundering and terrorism financing and by determining the transaction rating depending on the level of suspicion.

18. Examination of transactions by means of automated solutions involves detecting unusual or suspicious activities and transactions. These may be detected by establishing limits for the amount of transactions for a particular group or category of transactions and bank accounts. Particular attention shall be given to the transactions which exceed these limits and transactions that have no apparent economic purpose. Banks may use the following limits in transaction monitoring process:
a) cash transactions up to MDL 100 000;
b) cash and wire transfer transactions from MDL 100 000 up to MDL 500 000;
c) cash and wire transfer transactions from MDL 500 000;

19. Banks shall identify the risk exposure for the operations and activities subject to the risk of money laundering and terrorism financing and shall determine the relevance and applicability of their system to minimize the risk involved. The automated transaction monitoring system may supplement but not replace the employees' work and reasoning when detecting the unusual or suspicious activities. Therefore, the bank shall ensure that the implementation of such a system will not lead to fewer responsibilities of employees related to the identification of money laundering and terrorism financing activities.

20. The risk-based automated transaction monitoring system in the bank shall provide at least the followings:
a) comparison of clients' transactions or bank accounts used in a certain period with the previously conducted transactions within the bank that are considered reasonable and adequate;
b) comparison of clients' data or specific transactions with the risk rating establishing models;
c) providing alerts when identifying unusual and / or suspicious transactions;
d) recording appropriate alerts to be properly managed in the bank and ensuring their reporting to the SPCSB, as in accordance with the legislation in force;
e) its adjustment to the recommendations of the internal / external audit and / or supervisory authority;
f) providing aggregate information and statistics.

21. The efficiency of the automated transaction monitoring system is significantly influenced by the availability of information that can be used and the procedure for establishing of rules or operating parameters. Thus, effective monitoring requires regular revision and updating of the parameters or criteria used to generate reports for monitoring or for issuing alerts. For this purpose, banks shall make regular improvements to the transaction monitoring system taking into account changes in operational activity and the developments of money laundering and terrorism financing methods. All improvements to the system shall be properly documented and approved by the bank management.

22. In case the bank does not implement an automated transaction monitoring system, then it shall ensure the implementation of a system that generates reports, where the activity and performed transactions are analyzed and the level of risk involved. In such cases, the bank may opt for the advantages of sampling techniques of clients or transactions.

23. To achieve the effectiveness of the monitoring under the conditions set out in item 22, regular reports and appropriate control procedures are required as to ensure that clients' transactions are covered by the monitoring process of the bank, according to the degree of risk involved. Regular monitoring reports of transactions shall contain the following types of transactions: cash transactions, money transfers, transactions with financial instruments, credit repayment and reactivation of dormant bank accounts followed by frequent unusual transactions and / or in large amounts.

24. Transaction monitoring system shall include procedures to assess not only current clients' transactions but also to determine the pattern or type of transactions and their flows. Current transactions shall be compared with previous transactions of the same type and risk profile of the client. Additionally, banks shall examine the identified methods and typologies of money laundering and terrorism financing developed by national and international authorities.

25. Revision and updating of transaction monitoring framework, in the context of changing or not the risk involved, involves consulting the following sources of information:
a) publications issued by FATF -GAFI and other competent authorities;
b) recommendations and publications of law enforcement agency;
c) information from supervisory authorities and SPCSB;
d) media publications with regard to the prevention and combating money laundering and terrorism financing;
e) operational experience obtained during the monitoring of the bank.

26. Monitoring of transactions within the bank, depending on the degree of risk, shall ensure the followings:
a) obtaining confirmation documents justifying the economic operations, such as banking and settlement documents (contracts, invoices, shipping documents, deeds of purchase), customs declarations, certificate of salary, tax reports, activity reports, etc.;
b) establishment of the relevance of documents received for the period monitored;
c) application of increased precautionary measures and criteria for assessing the potential suspicious nature of the transactions that do not contain complete information on the payer, the purpose and nature of the transaction;
d) determination of unusual and suspicious transactions and their reporting to the SPCSB, as in accordance with the legislation in force;

27. A prerequisite for the establishment and operation of an effective monitoring of transactions is the support and commitment of the bank's management. Therefore, assigning sufficient resources to maintain and operate the system are essential. The responsible persons in the bank shall receive and analyze the information resulting from the monitoring of transactions and shall take decisions with regard bank's actions to minimize the risk of money laundering and terrorism financing.

28. An important element of the monitoring system of the bank is the monitoring of the business relationship. This involves reviewing all available data and information related to the bank's client in order to update these with the purpose to know the client's business and related transactions expected to be carried out.

29. Banks may take the following measures related to the monitoring of business relations:
a) update the know-your-customer information on presented when establishing the business relation;
b) verify compliance of the client's business, products and services offered with the market segment within which it operates;
c) obtain information on changes in the articles of incorporation, ownership structure and client management structure;
d) seek to achieve the purpose and the objective of the client set upon establishing the business relationship.

III. The nature of the business relationship

30. Determining the nature of the business relationship is a process applied by the bank, upon the initiation of the business relationship, to understand the purpose and objectives to be achieved by the person or entity. To this end, the bank shall take into account the fact that the legal entity is established to provide public goods and services and the individual seeks to obtain benefits by using banking products and services.

31. Banks may determine the nature of the business relationship with its clients by obtaining data about their current or planned activity. Thus, the bank may determine the activity or activities carried out by the client by examining and analyzing the articles of incorporation, information declared by the client and by verifying the authenticity of the information submitted by the client.

32. Circumstances indicating the existence of a business relationship are:
a) opening a bank account in the bank;
b) holding a payment card;
c) purchasing financial instruments;
d) providing certain services for a while;
e) concluding any other agreement facilitating the existence of a business relationship.

33. Depending on the risk involved, the information that is relevant and necessary to determine the nature of the business relationship may include some or all of the items listed below:
a) details regarding the activity of the client or employer;
b) source of funds expected to be used in the business relationship;
c) copies of the last available financial statements;
d) level and nature of the activity planned to be carried out within the business relationship.

IV. Ordinary nature of the activity

34. The nature of the activity of a bank client may be determined by assessing the business taking into account some characteristic factors. For most businesses, it is clear when the activities are ordinary activities. For example, the activity of accepting deposits from the public by banks is an ordinary activity for banks. However, it is difficult to interpret the concept of ordinary activity in other businesses. For

example, it is difficult to determine whether the activity is ordinary or not if the client carries out its activity rarely or only occasionally.

35. If the bank is not convinced that the activities of the client is ordinary or not, the bank shall examine:
a) whether the activity normal and can not be confused with another business and it is characteristic for the system, processes, promotion and competitiveness in the market segment where it operates;
b) frequency of the activity;
c) periodicity of the activity;
d) whether the activity is involved in transactions with a large amount of money;
e) whether the activity is a source of income for the business and its owners;
f) whether the activity is resource consuming;
g) whether the activity is able to provide clients with a service or product.

36. When determining the nature of the activity, banks shall take into account the extent to which each factor describes the business activity. Therefore, all factors shall be considered, each one being separately being indefinite. Only taken all together these factors will indicate whether or not the activity is ordinary.

37. Various aspects of the business or operations may help to perform the necessary analysis and the described factors may improve the quality of the assessment. A key aspect in the analysis is the financial size of the business. To assess this factor, it is important to examine the funds involved in the economic activity over a period of time. Thus, the exact nature of business activity may be identified by calculating the average indicators characterizing the amount of the transaction and the income received thereafter.

38. Resources allocated for the activity shall be proportionate to the volume of products and services. Resources can mean time of the employees, equipment used, raw material and equipment, buildings, land and other capital expenditures and / or any other expenses. Their assessment over a period of time will allow estimating the degree of development of the business and its continuity and the ordinary nature of the activity.

V. Complex transactions

39. Banks shall understand the structure and purpose of the planned transactions and shall determine whether the intended purpose of the transactions is consistent with their structure and related economic sense. In case banks can not determine the consistency of transactions, these shall obtain additional information to confirm their legality. If the client refuses to submit the supporting documents, banks shall not conduct the transactions and shall report such circumstances to the SPCSB, as in accordance with the legislation in force.

40. Depending on the size, complexity and structure of their business, banks shall define the characteristics of financial transactions with complex structures that imply high risks and do not guarantee the veracity of the purpose of transactions with related economic sense. A number of transactions may have complex characteristics but to be totally transparent. Lack of transparency may lead to misunderstanding of the structure of transactions and therefore may lead to high risks in bank's activity.

41. Generally, complex transactions presents a series of transactions involving different types of transactions or a flow of transactions with a structure and high degree of difficulty without a clear economic purpose. Transactions that the bank may consider in determining their complex nature are as follows, but not limited to:
a) transactions with financial instruments - checks, bills, certificates of deposit, shares and bonds, including those interest-bearing, forward contracts, swaps, interest rate instruments, futures, etc.;
b) lending transactions with related collateral - ordinary loans, credit lines, factoring, mortgages, issuance of guarantees and sureties, lease, letter of credit, etc.;
c) transactions related to investment and fiduciary management of assets - pension funds, insurance

companies, investment funds, investment counseling and support, etc.;
d) transactions carried out in self-employment activities - real estate agents, notaries, accountants, auditors, etc.;
e) transactions of professional participants of the securities market - in the meaning of the Law no.199 of 11.18.98 on the securities market and Law no.171 of 11.07.2012 on the capital market;
f) transactions related to the purchase - sale of precious metals and stones and gambling.

42. In order to minimize the risks and to manage them appropriately, the bank shall apply the followings, but not limited to, when carrying out complex transactions:
a) continuous training of employees for the complex transactions;
b) appropriate systems and models for tracking the performance and risk management;
c) management procedures and internal control;

VI. Final provisions

43. Banks shall organize their transaction monitoring system so that to determine the suspicious, complex and unusual transactions and to minimize the risks related to bank's activity in preventing and combating money laundering and terrorism financing.

44. Implementation of an adequate transaction monitoring system shall also ensure an efficient use of bank's resources as to manage rationally the processes applied when identifying client's activity and transactions.

See also

Tags
complex transactions [1]
business relationship [2]
transaction monitoring [3]
client screening [4]
real-time payment verification [5]
money laundering [6]
terrorism financing [7]
256 [8]

Source URL:
https://www.bnm.md/en/content/recommendations-monitoring-banks-transactions-and-clients-activities-prevent-and-combat

Related links:

[1] https://www.bnm.md/en/search?hashtags[0]=complex transactions [2] https://www.bnm.md/en/search?hashtags[0]=business relationship [3] https://www.bnm.md/en/search?hashtags[0]=transaction monitoring [4] https://www.bnm.md/en/search?hashtags[0]=client screening [5] https://www.bnm.md/en/search?hashtags[0]=real-time payment verification [6] https://www.bnm.md/en/search?hashtags[0]=money laundering [7] https://www.bnm.md/en/search?hashtags[0]=terrorism financing [8] https://www.bnm.md/en/search?hashtags[0]=256