Expand Hide

07.03.2014

Recommendations on cross-border relationships in the context of legislation on preventing and combating money laundering and terrorist financing, approved by the DCA of the NBM No. 42 of February 27,2014

Published in the Official Monitor of the Republic of Moldova no.53-59/326 of 07.03.2014

Approved by Decision of the
Council of Administration
Of the National Bank of Moldova
no.42 of 27 February 2014

Recommendations
on cross-border relationships in the context of legislation on preventing
and combating money laundering and terrorist financing

I. General provisions

1.Recommendations on cross-border relationships in the context of legislation on preventing and combating money laundering and terrorist financing (hereinafter - Recommendations) are intended to provide some methodological guidance to banks and other payment service providers in applying the legislation on preventing and combating money laundering and terrorist financing in the process of termination of a business relationship with a foreign correspondent institution.

2.The Recommendations cover:
a) description of risks in cross-border relationships;
b) description of the measures on Know Your Customer (KYC) - correspondent institution;
c) establishment of enhanced due diligence measures to be applied in the cross-border relationships;
d) description of the procedures for determining the shell banks and other fictitious legal entities providing payment services;

3.The Recommendations are developed taking into account the 40 Recommendations of the Financial Acion Task Force (FATF-FATF), Wolfsberg Group documents related to correspondent banking relationships, BASEL documents on KYC and other related international documents.

4.These recommendations do not apply in relation to central banks, central treasuries and monetary authorities of FATF member countries, regional or international development banks, such as the EBRD, IMF, World Bank, etc., at least as far as the relationship with these institutions, banks, authorities involves providing services and products that are in compliance with their statutory duties and activities.

5.Terms and expressions used in these Recommendations have the meanings set out in the Law no.190-XVI of 26.07.2007 on preventing and combating money laundering and terrorist financing, Law no.550-XIII of 21.07.1995 on financial institutions, the Regulation on banking activity on preventing and combating money laundering and terrorist financing, approved by the Decision of the Council of Administration no.172 of 04.08.2011, as well as recommendations and guidelines related to the field. The following terms and phrases shall be also used for the purpose of these Recommendations:

correspondent institution – a bank abroad or other foreign legal entity providing payment services;
cross-border relationships (correspondent) - provision by the bank or other payment service provider of its services and products to the correspondent institution by opening a bank account/payment account or in its absence and the provision of other related services in order to manage liquidity, grant loans, if needed, or make other investments, deliver cash in foreign currency, by recording the equivalent in correspondent accounts opened in other correspondent institutions, as well as in order to make payments on behalf of customers;
payment service providers – legal entities, which according to the Law no. 114 of 18 May 2012 on payment services and electronic money have the right to provide payment services.

6.Compliance with recommendations for the establishment of cross-border relationships will facilitate the identification, evaluation and minimization of risks and vulnerabilities related to the activity of banks and other payment service providers in relation to the correspondent institutions.

II. Risks in cross-border relationships

7.Cross-border relationships between banks and/or other payment services providers and correspondent institutions, over a long period of time, create a mechanism for high efficiency, which is of fundamental importance for the global economy. This mechanism facilitates the movement of money from one person or entity to another and from one country to another, as well as ensures foreign exchange operations. For this international payment infrastructure to continue to operate efficiently and at the same time to ensure the efficiency of money laundering combat and terrorist financing processes, each bank or payment service provider involved shall be responsible for applying customers due diligence measures and monitoring the transactions in accordance with applicable regulations, taking into account relevant international standards.

8.Correspondent relationships are a large business, sensitive in time, involving substantial money flows through a series of banks and legal entities that provide payment services, which have no connection between them and usually are located in different countries. In many cases, a single party involved does not have a complete picture of the entire transactional flow. An institution processes the transactions initiated by its correspondent in favor of a party that is unknown, with no direct relationship, not its customers, and over which the institution has not applied KYC measures. These features may make the correspondent accounts vulnerable to potential abuse of money laundering and terrorist financing and may hinder the detection and prevention of illegal activities.

9.Each correspondent relationship shall be reviewed on the basis of performance and the institutions involved shall properly implement the laws of the country in order to prevent and combat money laundering and terrorist financing. The review of cross-border relationships means paying attention to factors that may pose a higher risk of money laundering or terrorist financing, either individually or in combination. Such factors have been identified in international standards and the main focus was on two types of risks:
a) country risk;
b) customer's risk.

10.Country/territory risk shall be assessed in terms of compliance with the correspondent relationships, in order to determine the potential risk of money laundering or terrorist financing due to certain country/territory related criteria. Among the criteria that determine whether a country/territory pose a high risk of money laundering and/or terrorist financing are:
a) sanctions, bans or other restrictions imposed by international organizations, in the context of legislation on preventing and combating money laundering and terrorist financing;
b) high levels of crime and corruption;
c) the absence or existence of an inadequate legal framework for preventing and combating money laundering and terrorist financing;
d) providing support to terrorist organizations and terrorist activities;
e) the country is in the list of jurisdictions that do not implement the international standards of transparency.

11.Banks and payment service providers shall take into account the headquarters of the correspondent institution, and the country of residence of the beneficiary of the correspondent institution. In certain specific circumstances, country risk may also include an assessment of the main geographic markets covered by the correspondent institution.

12.Customer's risk is related to either the organization and structure of the correspondent institution or the nature and scope of its business. Factors that could constitute a risk of money laundering and terrorist financing occur in the following situations:

a) the correspondent institution is a resident of an offshore area/country and/or conducts its business in an offshore area/country;
b) the correspondent institution is the owner or is controlled by a politically exposed person;
c) the correspondent institution offers its customers services that are characterized by a high degree of risk;
d) the correspondent institution is a non-banking financial institution, such as a foreign exchange entity or the administrator of money remittance system;
e) the correspondent institution carries out transactions with a high degree of risk and fall under the indices and criteria of suspicion.

13.Banks and other payment service providers shall use the above criteria to develop their own risk model related to the identification of the correspondent institution in order to enhance the existing KYC, control and monitoring measures. Banks and other payment service providers shall document the methods used and control taken.

III. Know Your Customer

14.Know Your Customer - correspondent institution means the application by the bank of the risk-based approach process to identify the correspondent institution and the potential risks of that it can generate during the course of the business relationship. Key risk indicators to be taken into consideration both at the beginning of the relationship and during the business relationship, in order to establish standard or increased KYC measures to be taken are:
a) headquarters of the correspondent institution;
b) governance and ownership structure of the correspondent institution;
c) the customers and activity of the correspondent institution.

15.The country in which the correspondent institution operates and the headquarters/residence of its owner may pose a high risk. Some countries are internationally recognized as jurisdictions that implement inadequate measures in the field of preventing and combating money laundering and terrorist financing or have inadequate supervision, or pose a high risk because of crime, corruption, or support for terrorist financing activities or terrorist organizations. However, other developed countries have adequate regulations in this area, which lowers business risk. Thus, banks and other payment service providers shall take measures to review and analyze information relating to countries to make sure that the correspondent institution does not pose a high risk because of this indicator.

16.Another high risk is the location of the owner, organizational and legal form and transparency of its ownership. The location and experience of management may raise additional concerns, in particular in case of involvement of politically exposed persons in the management or ownership of the correspondent institution.

17.The type of activity of the correspondent institution and the type of markets in which it operates is an important indicator that shall not be neglected when determining the risk of correspondent institution. Involvement in certain business segments, internationally recognized as vulnerable to money laundering, corruption and terrorist financing risks presents new concerns. Therefore, a customer - correspondent institution, which income comes mainly from customers with a high degree of risk, may also be at high risk.

18.Customers of banks or other payment service providers - correspondent institutions shall be subject to appropriate KYC measures to ensure that the bank or other payment service provider will operate properly taking into account the risk profile of the customer. When establishing the business relationship, in order to know the correspondent institution, banks or other payment service providers can use at least the “Questionnaire on correspondent institution due diligence” (see Annex no.1 to these Recommendations) and “Information and documents on knowledge of the correspondent institution” (see Annex no.2 to these Recommendations) or other formats of questionnaires at their discretion. If the correspondent institution operates in an environment subject to appropriate regulation and supervision in the field of preventing and combating money laundering and terrorist financing, the bank or other payment service provider may rely on publicly available information necessary to know its partner.

19.In the application of partner due diligence measures, the bank or other payment service provider shall consider the following additional risk factors:
a) services and products offered;
b) history and status of regulatory and supervisory authority and, if necessary, the bank or other payment service provider shall examine the materials and information accessible to the public to determine whether the institution in question was the subject of illegal actions or effects in the past;
c) the nature of control in the filed of preventing and combating money laundering and terrorist financing over the correspondent institution;

d) confirmation that the beneficiaries of correspondent relations will not use the services and products of the institution to engage in business relationships with shell banks or other financial institutions that provide fictitious payment services.

IV. Due diligence measures

20.Correspondent relationships have a high degree of risk for each bank or other payment service provider and therefore additional measures on knowing the partners are required. Given the types of risk indicators, the bank or other payment service provider shall establish at the initiation of the relationship and during that relationship reasonable measures to be taken in order to know the correspondent institutions and to control the risk to which they are exposed.

21.Specialized international institutions, such as FATF, Wolfsberg Group, Basel Committee on Banking Supervision, etc., by approving documents and related recommendations, have listed a number of measures that can be applied by banks that establish cross-border relationships. The measures listed below are important and shall be applied over the correspondents that present a high risk of money laundering and terrorist financing:
a) due diligence measures - the accumulation of sufficient information about the correspondent institution to understand the nature of its activity and determining the reputation and quality of supervision, from publicly available information. This requires analyzing publicly available information and documents, including information published by the media, to determine whether the institution in question was subject to investigations of money laundering or terrorist financing or whether sanctions were applied to it. The information collected should allow the bank or other payment service provider to periodically verify the identity of the owner of the correspondent institution and its governing bodies, including new and previously unknown links with politically exposed persons or individuals or legal entities to which sanctions were applied;
b) to request and review the policies and practices of the correspondent institution - analysis of program to prevent and combat money laundering and terrorist financing, including requirements relating to KYC. Obtaining sufficient information about the program of the correspondent institution for the field to assess whether the practices to prevent and combat money laundering used are appropriate and adequate and in line with the international standards. A useful tool in this regard is the “Questionnaire on know your customer - correspondent institution”, the template of which is shown in Annex no.1 to the Recommendations;
c) to visit and conduct discussions with beneficial owners and/or senior management of the correspondent institution, as appropriate;
d) risk-based involvement of independent control bodies, such as internal audit, in the analysis of information related to the correspondent institution, both when approving or establishing cross-border relationships and when reviewing periodically the existing relationships;
e) enhanced monitoring of transactions conducted through the correspondent institution.

22.Banks or other payment service providers shall monitor their transactions to help identify unusual or suspicious activities and transactions for reporting them as required by law. Since the unusual transactions or unusual patterns of activity are not always suspicious, banks or other payment service providers shall implement appropriate processes and systems to identify real suspicious activities and transactions, using known typologies in this regard.

23.In the correspondent relationships, the volume and speed of transactions and in some cases the lack of specific or complete information about the correspondent customers and beneficial owners of the transaction make the monitoring of transactions of the institution more difficult than for other business involving direct relationships with customers. Thus, to improve continuous monitoring of transactions through correspondent accounts, the rule setting transaction value limits is widely used and exceeding of such limits will lead to a thorough examination of the purpose and nature of the transactions, which allows identifying potential unusual and suspicious transactions.

24.The results of monitoring of transactions is observed when the bank or other payment service provider applies its system so that the institution presenting an increased risk to be subject to monitoring in the first place.

25.Primary responsibility for customer due diligence measures and ongoing monitoring of the correspondent relationships shall be under the control of a subdivision or a person clearly identified. This gives the possibility to define certain parameters and rules for transactions and to establish restrictions on various types of transactions and/or the amounts or volumes and/or involvement in transactions with certain countries for a fixed/unfixed period, in order to comply with the business and related legislation.

26.Monitoring of transactions is a difficult process, and the use of indices of suspicion facilitates the knowledge of possible suspicious transactions. In this regard, the following indices for the transfers in very large amounts and/or very

large volumes/frequencies and/or bursts of activities occurring in short periods of time may be:
a) transactions involving countries with high-risk, vulnerable to money laundering and terrorist financing;
b) transactions involving shell banks or fictitious legal entities that provide payment services;
c) transactions involving fictitious entities (bogus legal entities);
d) transactions frequently including amounts that are less than own internal monitoring limits or limits set by the relevant legislation;
e) transactions involving accounts that operate significantly beyond the limits, based either on information collected on due diligence measures or based on previous behavior related to the activity planned;
f) transactions are carried out through several different countries or more financial institutions before or after the involvement of the bank or payment service provider, without any apparent purpose, other than that to conceal the nature, source, ownership or control of funds;
g) transactions have the following features or combined features, such as repeated transfers from an originator to a particular beneficiary, and/or individual electronic transfers carried out in a short period of time, such as transfers carried out daily, twice the day or every other day.

27.Banks or other payment service providers shall promote a general policy in correspondent relationships to support international payment system and international trade without prejudice to the commercial interest of customers and the correspondent institution. However, banks or other payment service providers shall avoid establishing correspondent relationships that pose a high risk, such as relations with:
a) shell banks or fictitious legal entities providing payment services;
b) unauthorized or unregulated financial institutions;
c) correspondent institutions that produce significant uncertainties when applying due diligence measures;
d) correspondent institutions that do not have in place measures to prevent money laundering and terrorist financing or such measures are deemed inadequate and/or insufficient, which therefore does not allow to comply adequately with the national legislation in the field of preventing and combating money laundering and terrorist financing.

V. Determination of shell banks or fictitious legal entities providing payment services

28.A bank or legal entity providing payment services is deemed fictitious if it has no physical presence in the country where it is registered and licensed, does not perform real leadership and management and is not affiliated with a regulated financial group.

29. Administration of such shell banks or fictitious legal entities providing payment services is in a different country than where they operate, often with offices in an associated company or private residences. Usually, a bank or a legal person providing payment services keeps in touch only with a private agent for registration of the legal entity, which knows nothing about its business and daily operations and provides, upon request, only information on the registered address of the bank or legal entity proving payment services. Structures with the above-listed peculiarities are usually in off-shore areas/countries. However, some off-shore areas comply with the requirements of preventing and combating money laundering and terrorist financing.

30.As shell banks or fictitious legal entities providing payment services are not affiliated with a supervised financial group, the licensing authority is the only entity responsible for its supervision. However, once the administration of the institution is located in another country, the supervisory authority is not able to effectively supervise the institution, by conducting on-site inspections or discussions with bank management, in accordance with international standards. Thus, the supervisory authority does not know about the existence of such an institution and that it operates in the country. Shell banks or fictitious legal entities providing payment services, which are assigned to the description often mentioned, were involved in illegal or suspicious financial transactions. In this context, shell banks or fictitious legal entities providing payment services impose significant barriers to conducting adequate supervision and there are no special conditions that could be implemented to obtain effective legal supervision.

31.For an adequate knowledge of the correspondent institutions and determining shell banks or fictitious legal entities providing payment services, in order to avoid establishing business relationship or conducting transactions, shell banks or other fictitious legal entities providing payment services shall pay attention to the following basic features characteristic for such institutions:
a) lack of activity at a fixed address;
b) the activity/transactions are carried out in a country other than that in which it was licensed;
c) lack of employees;

d) lack of full / partial bookkeeping;
e) lack of supervision by banking supervisors authority.

VI. Final provisions

32.Banks and other payment service providers shall organize the activity in the cross-border relationships so that to ensure proper implementation of the legislation in the field of preventing and combating money laundering and terrorist financing. At the same time, these shall use a transaction monitoring system to ensure the effective management of resources of banks and other payment service providers to manage rational processes for business relationships with correspondent institutions.

Annex no.1
to the Recommendations on cross-border relationships in the context
of legislation on preventing and combating money laundering and terrorist financing

Questionnaire on correspondent institution due diligence

I. Policies, procedures and practices regarding the prevention and combating money laundering and terrorist financing		
Is the correspondent institution's program on preventing and combating money laundering and terrorist financing institution approved by the Board or other governing body?	Yes	No
Does the program, approved in the form of an internal regulation, contain requirements on the existence in the correspondent institution of a responsible person in this field, and his/her responsibilities for the supervision and coordination of measures to ensure the implementation of such program?	Yes	No
Does the program, approved in the form of an internal regulation, contain requirements documenting the processes needed for the prevention, detection and reporting of suspicious transactions?	Yes	No
In addition to the control performed by the regulatory and supervisory authorities, has the institution established an internal audit function or an independent third party to evaluate systematically the policies, procedures and practices regarding the prevention and combating money laundering and terrorist financing?	Yes	No
Do the policies of the correspondent institution contain requirements regarding the prohibition to have accounts or business relationship with a bank or other financial institution that provides fictitious payment services?	Yes	No
Does the correspondent institution have in place policies governing the relationships with politically exposed persons in accordance with the best practices?	Yes	No
Does the correspondent institution have in place adequate procedures for keeping records and information in accordance with the relevant regulations?	Yes	No
Are the policies, procedures and practices of the correspondent institution in the field of prevention and combating money laundering and terrorist financing applied to all its branches and subdivisions both at home and abroad?	Yes	No
II. Risk assessment		
Does the institution apply risk-based approach to its clients and transactions of these?	Yes	No
Does the correspondent institution have in place and apply increased due diligence requirements to categories of customers and transactions with high-risk made via the institution or that are deemed to present increased risks due to illegal activities?	Yes	No
III. Know your customer rules, general and enhanced due diligence measures		
Does the correspondent institution have implemented a KYC system, including information about transactions or opening of accounts, etc. (such as name/name and surname, headquarters/residence, address, phone number, type of activity/occupation, registration date/year of birth, tax code/ID number of a valid ID and name of the country/state that issued the ID)?	Yes	No
Does the correspondent institution have the obligation to collect information on the nature of its customer’s activity?	Yes	No
Does the correspondent institution apply increased due diligence measures to its customers and transactions classified as of high risk?	Yes	No

Does the correspondent institution collect information and assess its customers in accordance with the approved policies and practices to prevent and combat money laundering and terrorist financing?	Yes	No
Does the correspondent institution have in place procedures for keeping record of each customer, recording in this respect identification documents and information collected as part of customer due diligence process upon opening of accounts?	Yes	No
Does the correspondent institution take measures to understand the ordinary transactions of its customers based on their risk assessment?	Yes	No
IV. Transaction reporting, prevention and detection of suspicious transactions		
Does the correspondent institution have in place policies and procedures for identifying and reporting of transactions that must be reported to the competent authority?	Yes	No
Does the correspondent institution have in place policies and procedures for identifying structured transactions made to avoid reporting requirements of large amounts of cash?	Yes	No
Does the correspondent institution verify the transactions of its customers that have a high risk for the institution (such as transactions with persons, entities or countries that are classified as of high risk)? Are such procedure also used before carrying out the transaction?	Yes	No
Does the correspondent institution have in place policies to ensure that fictitious banks or legal entities that provide payment services do not use the accounts, products and services for transactions?	Yes	No
Does the correspondent institution have in place policies to ensure correspondent transactions only with institutions in other countries that are properly licensed?	Yes	No
V. Transaction monitoring		
Does the correspondent institution have in place a program for monitoring unusual or suspicious activities?	Yes	No
Does the monitoring program provide for requirements to obtain supporting documents when carrying out a transaction?	Yes	No
VI. Other information		
Does the correspondent institution conduct trainings in preventing and combating money laundering and terrorist financing for relevant staff, which includes information relating to the procedure for the identification and reporting of transactions to the competent authorities, indices and methods of money laundering and terrorist financing through products and services?	Yes	No
Does the correspondent institution keep record of training session that includes information related to the personnel and materials used?	Yes	No
Does the correspondent institution have in place policies to communicate new regulations related to the prevention and combating of money laundering and terrorist financing?	Yes	No
Does the correspondent institution contracted third party services to implement any measures related to the prevention and combating of money laundering and terrorist financing?	Yes	No
If yes, is staff of the third party trained for the given domain?	Yes	No
Have there been applied sanctions by supervisors or other authorities in the last three years to the correspondent institution related to the field of preventing and combating money laundering and terrorist financing?	Yes	No

Annex no.1
to the Recommendations on cross-border relationships in the context
of legislation on preventing and combating money laundering and terrorist financing

Information and documents related to correspondent institution due diligence

1. „Questionnaire on correspondent institution due diligence" (see Annex no.1 to these Recommendations);
2. Obtaining recent copies of policies and procedures for preventing and combating money laundering and terrorist financing, if required;
3. Brief biographies of board members and the executive body of the correspondent institution, and specimens of their

signatures;

4. List of owners that directly hold a voting right of 10 percent or more of the number of securities issued and the list of owners who indirectly own or control a voting right of 25 percent or more of the number of securities issued;
5. The last annual financial report of the correspondent institution;
6. Copy of the license of the correspondent institution and the stamp, if applicable;
7. Copies of articles of corporation, such as the status of the institution, contract and registration certificate;
8. Excerpt from the State Register on the registration of the correspondent institution.

See also

Tags

money laundering [1]

terrorist financing [2]

cross-border relationships [3]

payment service providers [4]

customer [5]

42 [6]

shell banks [7]

questionnaire [8]

Related links:

[1] http://bnm.md/en/search?hashtags[0]=money laundering [2] http://bnm.md/en/search?hashtags[0]=terrorist financing [3] http://bnm.md/en/search?hashtags[0]=cross-border relationships [4] http://bnm.md/en/search?hashtags[0]=payment service providers [5] http://bnm.md/en/search?hashtags[0]=customer [6] http://bnm.md/en/search?hashtags[0]=42 [7] http://bnm.md/en/search?hashtags[0]=shell banks [8] http://bnm.md/en/search?hashtags[0]=questionnaire