BANKING AGENCY OF REPUBLIKA SRPSKA

GUIDELINES FOR RISK ANALYSIS AND ASSESSMENT
in the implementation of the Decision on managing anti-money laundering and counter-terrorism financing risk

Banja Luka, March 2024

Pursuant to Article 22, Paragraph 1, Item f) of the Law on the Banking Agency of Republika Srpska ("Official Gazette of Republika Srpska" No. 59/13 and 4/17), Article 22, Paragraph 4, Item m) of the Statute of the Banking Agency of Republika Srpska ("Official Gazette of Republika Srpska" No. 63/17), pursuant to Article 101 of the Law on anti-money laundering and counter-terrorism financing ("Official Gazette of BiH", No. 13/24) and pursuant to Article 47 of the Decision on managing anti-money laundering and counter-terrorism financing risk ("Official Gazette of Republika Srpska", No. 22/24), the Director of the Banking Agency of Republika Srpska issued the

GUIDELINES FOR RISK ANALYSIS AND ASSESSMENT in the implementation of the Decision on managing anti-money laundering and counter-terrorism financing risk

1. General provisions

1.1. Regulated entities shall be obliged to prepare and regularly update a money laundering and terrorist financing risk analysis (hereinafter: Risk analysis) in accordance with the Law on anti-money laundering and counter-terrorism financing, by-laws and in accordance with the Risk Assessment of money laundering and terrorist financing and proliferation of weapons of mass destruction in Bosnia and Herzegovina.

1.2. The Risk analysis for each group or type of client, business relation, transaction, product/service and distribution channel that the regulated entity provides within the scope of its activities, including the method of establishing a business relation with the client, aims to determine the criteria on the basis of which the regulated entity shall classify a particular client, business relation, product/service or transaction into one of the risk categories stipulated by the Law on anti-money laundering and counter-terrorism financing.

1.3. When identifying and assessing the risk of money laundering and terrorist financing, the regulated entity shall be obliged to timely include the risk of money laundering and terrorist financing arising from the introduction of new products and services or significant changes to existing products. The regulated entity shall be obliged, prior to introducing a new product, to analyze:

1) the risk of money laundering and terrorist financing that may arise as a result of such introduction;
2) the impact of such introduction on the regulated entity's exposure to the risk of money laundering and terrorist financing and
3) the impact of such introduction on the possibility of adequately managing the risk of money laundering and terrorist financing.

2. Risk analysis

2.1. The Risk analysis must be proportionate to the nature and scope of the business operations, as well as the size of the regulated entity, and take into account at least the following **factors**:

2.1.1. Client risk:

1) the business operations or professional activity of the client and the client's beneficial owner;
2) the reputation of the client and the client's beneficial owner;
3) the nature and conduct of the client and the client's beneficial owner;

2.1.2. Product, service or transaction risk:

1) the purpose of the account or business relation;
2) the regularity or duration of the business relation;
3) the amount of assets deposited by the client or the volume of transactions executed;
4) the level of transparency or non-transparency of the product, service or transaction. When considering the level of transparency of a product, service or transaction, the regulated entity should in particular assess:

- the extent to which the product or service or transaction enables or facilitates the anonymity of the client, the client's beneficial owner or the client's ownership structure, and
- the extent to which there is a possibility for a third party who is not part of the business relation to give instructions regarding that relation.

5) the complexity of the product, service or transaction. When analysing the complexity of a product, service or transaction, the regulated entity should in particular assess:
   - the extent to which the transaction is complex and whether the relation involves multiple clients or multiple legal systems;
   - whether the transactions are direct and regular;
   - the extent to which third parties are allowed to pay for products or services or that overpayment is allowed when this is not customary, if payment by a third party is expected and whether the regulated entity knows the identity of that party and
   - the level of awareness of the risks associated with the regulated entity's new or innovative product or service, in particular where it involves the use of new technologies or payment methods.
6) the value or volume of the product, service or transaction. When analyzing the value of products, services or transactions, the regulated entity should in particular assess:
   - the extent to which the products or services are primarily cash-based,
   - the extent to which the products or services facilitate or encourage high-value transactions,
   - whether there are limits on the value of the transaction in order to reduce the possibility of misuse of the product or service for the purpose of money laundering or terrorist financing, and
   - whether the transactions involve oil, weapons, precious metals, tobacco products, cultural artifacts and other objects of archaeological, historical, cultural and religious significance or of exceptional scientific value, as well as protected species.

2.1.3. Country and geographical area risk:

1) countries/geographical areas in which the client and the client's beneficial owner are seated;
2) countries/geographical areas that are the main places of business operations of the client and the client's beneficial owner;
3) countries/geographical areas with which the client and the client's beneficial owner have relevant personal or business links or financial or legal interests;
4) the effectiveness of the regime for the anti-money laundering and terrorist financing in a given country;
5) the level of transparency and tax discipline in a given country.

2.1.4. Distribution channel risk:

1) the extent to which the business relation is conducted without the client being physically present. When considering the method in which the requested product/service is delivered to the client, the following should be considered as a minimum:
   - the client is not present at identification;
   - online distribution of the product/service;
   - service segmentation, i.e. the provision of electronic money services by several operationally independent service providers without appropriate supervision and coordination;
   - the possibility of identity fraud and misuse;
   - who are the third parties carrying out the identification and analysis of the client, do they belong to the same group, can the regulated entity rely on the quality of the measures undertaken by the third party, and whether adequate supervision is carried out over the third parties;

- whether the business relation is carried out through a representative, i.e. whether the regulated entity has direct contact with the client or whether the client was brought by a representative who does not have direct contact with the regulated entity.

2) the presence of persons who introduce the client or are intermediaries and the nature of their relation with the client. In cases where the client uses an intermediary, it should be considered whether the intermediary is:
   - a regulated entity subject to implementing anti-money laundering and terrorist financing measures;
   - under effective supervision of anti-money laundering and terrorist financing and
   - seated in a country associated with a higher risk of money laundering and terrorist financing.

2.2. Regulated entities shall be obliged to take into account, by means of the Risk analysis, other risk factors identified by the regulated entity due to the specific nature of its business operations.

2.3. Based on the Risk analysis conducted and the measures they undertake to mitigate the risk of money laundering and terrorist financing, the regulated entities shall be required to assess the overall exposure to the risk of money laundering and terrorist financing as follows:
- low risk,
- medium risk and
- high risk.

3. Risk factors

3.1. Client risk

3.1.1. In order to identify the client risk, including the beneficial owner of the client, regulated entities should consider the risks associated with the business model and type of professional activity, reputation, ownership and organizational structure, as well as the client's conduct regarding the business relation or transaction with the regulated entity.

3.1.2. General factors

3.1.2.1. In relation to the client's activity, or the client's profession, or the client's beneficial owner, the following circumstances may indicate a higher risk of money laundering and terrorist financing:

1) the client or the client's beneficial owner carries out activities in the field of construction, arms trade and its production, trade in goods of high value (such as precious metals, gemstones, cars, art, etc.);
2) the client or the client's beneficial owner carries out activities characterized by a large turnover of cash payments (such as casinos, gas stations, car dealerships, tourist organizations, restaurants, exchange offices, shops, car washes, florists, transporters of goods and passengers, etc.);
3) the client is a foreign bank or other similar financial institution of a country that does not apply standards in the field of anti-money laundering and terrorist financing;
4) the client, the beneficial owner of the client, a person related to the client or the controlling company of the client is a person that provides financial services, i.e. services related to digital assets, and whose establishment, i.e. the provision of such services, in accordance with the regulations of the country in which it is established, does not require the license of the relevant supervisory body, i.e. which is not subject to supervision over the implementation of actions and measures in the field of anti-money laundering and terrorist financing;
5) the client, i.e. the beneficial owner of the client, a person related to the client or the controlling company of the client is established by issuing bearer securities or by issuing digital assets that directly or indirectly enable the concealment of the identity of buyers/investors;
6) the client is a private investment fund.

3.1.2.2. In relation to the reputation of the client, or the client's beneficial owner, the following circumstances may indicate a higher risk of money laundering and terrorist financing:

1) information from reliable and relevant sources about the client's or the client's beneficial owner's connection to criminal offences of money laundering and terrorist financing and predicate offences of money laundering or terrorist financing;
2) the client, the client's beneficial owner, the client's representative or proxy in the course of business relation is identified on the list of persons against whom restrictive measures are in force or the client or the client's beneficial owner is closely connected by personal or business relations with these persons;
3) the client or the client's beneficial owner has been reported for suspicious transactions to the State Investigation and Protection Agency - Financial Intelligence Unit (hereinafter: FIU);
4) in the last three years, the FIU has requested the regulated entity to provide information about the regulated entity's client or the beneficial owner of the client, and about transactions carried out by the regulated entity, for which there are grounds for suspicion that they involve money laundering or terrorist financing;
5) in the last three years, the FIU has issued a written order to the regulated entity, regarding the client, to temporarily suspend the execution of a transaction or to temporarily suspend access to a safe deposit box;
6) in the last three years, the FIU has issued a written order to the regulated entity, regarding the client, to monitor the operations of that client (transactions or operations of that client carried out with the regulated entity).

3.1.2.3. In relation to the ownership or organizational structure of the client or the client's beneficial owner, the following circumstances may indicate a higher risk of money laundering and terrorist financing:

1) due to the organizational structure, legal form or complex and unclear ownership relations, it is difficult to determine the identity of the client's beneficial owners or the persons managing them;
2) there are no reasonable grounds for changing the client's ownership structure;
3) the client or the client's beneficial owner is a non-profit organization that can be used for the purpose of financing terrorist activities;
4) the client or the client's beneficial owner is a person with a disproportionately small number of employees in relation to the volume of business/declared turnover and/or a person who does not have its own infrastructure, business premises, etc.;
5) the client or the client's beneficial owner is an offshore legal entity or a person under foreign law.

3.1.2.4. In relation to the conduct of the client, or the client's beneficial owner, in connection with a business relation or transaction, the following circumstances may indicate a higher risk of money laundering and terrorist financing:

1) the client avoids providing all necessary evidence of identity, and there are no objective reasons for this, or there is doubt regarding the identity of the client or the client's beneficial owner;
2) the client's business activity or transactions are carried out under unusual circumstances. Unusual circumstances include, in particular:
   - a significant and unexpected distance between the client's location and the organizational unit of the regulated entity in which the client opens an account, establishes a business relation or carries out a transaction;
   - frequent and unexpected establishment, without economic justification, of business relations of a similar type with multiple regulated entities,

e.g. opening accounts in multiple banks, concluding multiple financial leasing agreements with multiple financial leasing providers, concluding multiple loan agreements with multiple banks/microcredit organizations, etc.;

3) the client uses products or services in a manner that was not identified in the procedure when the business relation was established;
4) the client is a non-resident and the services requested from the regulated entity would be more adequately provided in another country or there is no economic logic for the type of service requested by the client;
5) there is a suspicion that the client is not acting on its own behalf, i.e. there is a suspicion that the client is carrying out the instructions of a third party;

Regulated entities should take into account that certain circumstances that describe a client's behavior will not be apparent at the very beginning of establishing a business relation with the client.

3.1.2.5. In relation to risk factors associated with the client, i.e. the client's beneficial owner, the following may indicate a potentially higher risk:

1) the client who can be used as a means of safeguarding personal assets or a means of gaining access to financial services;
2) companies that do not or may not carry out trade, production or other activities in the country in which they are registered and
3) a company with its registered office in Bosnia and Herzegovina that is 25% or more owned by a foreign legal entity that does not or may not carry out trade, production or other activities in the country in which it is registered.

3.1.2.6. When assessing the client risk, regulated entities shall be obliged to use the results of the Risk Assessment of money laundering and terrorist financing and proliferation of weapons of mass destruction in Bosnia and Herzegovina in the part that relates to the activity, i.e. profession of the client or forms of organization of the client's companies involved in money laundering.

3.1.2.7. Likewise, when analyzing and assessing the risk of money laundering and terrorist financing of the regulated entity, including the analysis and assessment of the client risk, regulated entities should specifically consider the types of their clients, depending on whether the client is:

1) a regulated entity defined by the Law on anti-money laundering and counter-terrorism financing;
2) a state body (regardless of the level: state, entity, district, local);
3) public agency, public fund - public institute (PIO/MIO, FZO RS, etc.), chamber (regardless of level);
4) joint-stock company listed and whose shares are traded on the stock exchange, i.e. whose financial reports are publicly disclosed;
5) joint-stock company not listed, i.e. whose shares are not traded on the stock exchange;
6) limited liability company, i.e. a company organized in some other form;
7) entrepreneur, with special attention to special business operations (precious stones, precious metals, and other high-value goods, car dealers, real estate dealers, etc.);
8) private individual - citizen;
9) politically exposed person;
10) person who is not present when establishing a business relation;
11) person who is on the lists of persons against whom restrictive measures are in force;
12) a company with intensive cash operations, including:

- money transfer companies, authorized money exchange offices, money transfer intermediaries and other companies offering money transfer services,
- casinos, betting shops and other activities related to games of chance and
- companies that do not have intensive cash operations, but use larger amounts of cash to carry out certain transactions;

13) humanitarian or other non-profit organizations;
14) an accountant, lawyer, notary, tax consultant and others who have accounts in a certain credit institution and act on behalf of their clients;

3.1.3. Specific factors related to client risk

3.1.3.1. **Banks and other payment service providers**

The following factors may contribute to an increase in risk with these regulated entities in relation to the client risk factor:

1) there are indications that the client avoids establishing a permanent business relation with these regulated entities (e.g., requests one or more transactions even though establishing a permanent business relation would be economically more logical);
2) frequent and unexpected transfers, without a clear economic reason, of funds from an account with one regulated entity to accounts with another regulated entity, especially if the banks are located in different locations, except in the case of multinational companies operating through multiple accounts, frequent transfers of digital assets from one address of those assets to another;
3) the client's needs could be met in a faster and simpler manner with another bank;
4) the client gives the impression that it is acting on someone else's behalf, for example when it is visible that other persons are supervising the client inside or outside the premises where the transaction is being carried out or the client acts by reading notes with instructions;
5) the client's conduct has no economic justification, e.g. the client accepts an unfavorable exchange rate or a high fee without objection,
6) the client requests a transaction in a currency that is not the official means of payment or is unusual in the legal system of the country where the client or the payee is located or requests or gives significant amounts of currency in large or small denominations;
7) the client's payment transactions are always slightly below the appropriate limits;
8) the client uses the service in an unusual way, e.g. sends money to itself or receives money that it has sent to itself or sends money immediately upon receipt;
9) the client gives the impression that it does not know much about the payee or is cautious in providing information about it;
10) several clients transfer funds to the same payee or give the impression that they have the same identification data, e.g. address or telephone number.

3.1.3.2. **Leasing providers**

The following factors may contribute to the increase in the risk of a financial leasing provider in relation to the client risk factor:

1) the client concludes multiple leasing contracts in a short period of time without a clear economic justification;
2) the client who is a private individual and does not have the status of an entrepreneur, seeks to conclude a leasing contract for the purpose of purchasing machinery and other equipment used in the production process;

3) the client who has the status of an entrepreneur or a company seeks to conclude a leasing contract for the purpose of purchasing items that are not related to the performance of the client's main activity;
4) the client who terminates the leasing contract relatively soon after concluding it, and then soon comes forward with the intention of concluding a new leasing contract relating to the same or a similar item that was the subject of the lease in the terminated contract;
5) insisting on paying a higher percentage of participation in the purchase of the leased asset than that stipulated and which, in accordance with the general terms and conditions of its operations, the financial leasing provider requires when concluding the financial leasing contract.

3.1.3.3. **Electronic money institutions**

The following factors may contribute to a higher risk for an electronic money institution in relation to a client:

1) the client purchases electronic money under several products from the same electronic money institution, makes frequent product top-ups or redeems (withdraws cash) at short intervals without economic justification, and if the distributors themselves (or agents acting as distributors) are also regulated entities, this also applies to electronic money products from different institutions purchased from the same distributor;
2) the values of transactions carried out by the client are always slightly lower than any value restrictions (limits);
3) there are circumstances indicating that the product is used by multiple persons whose identities are unknown to the institution (e.g. the product is used simultaneously with several Internet Protocol addresses - (hereinafter: IP addresses);
4) there are frequent changes to the client's identification data, such as residential address or IP address or linked bank accounts;
5) the product is not used for its intended purpose (e.g. it is used globally, and is intended for use as a gift card only at certain points of sale).

The fact that the product is available only to certain categories of clients, e.g. socially vulnerable persons or employees of the legal entity issuing them for the purpose of covering expenses, may indicate low risk.

3.2. Product, service or transaction risk

3.2.1. General factors

3.2.1.1. When analyzing and assessing the risk of money laundering and terrorist financing, regulated entities shall be required, during the analysis and assessment of product, service or transaction risk, to specifically consider the features of the products they offer to their clients, depending on whether these products (the manner and extent of their use) are suitable for money laundering and/or terrorist financing.

3.2.1.2. Regulated entities shall be required to specifically consider whether, in what manner and to what extent, clients will use any of the products and services they offer to their clients, which carry a different level of risk. Depending on the use, each individual product may carry a different level of risk.

3.2.1.3. Products and services that may pose a higher risk are:

1) products or transactions that may favor anonymity;
2) services that are new to the market, i.e. not previously offered in the financial sector, must be specifically monitored to determine the actual level of risk;
3) new products and new business practices, including new delivery mechanisms and the use of new or emerging technologies for new and existing products;

4) provision of services outside the business premises of the regulated entity (e.g. granting consumer loans or concluding a leasing agreement in a merchant's sales facility) and
5) new products and new business practices, including new ways of establishing a business relation, as well as the use of new or emerging technologies, for both existing and new products;

3.2.1.4. Products and services that may indicate a potentially lower risk:
- products where the lower risk is affected by spending restrictions or ownership transparency and
- the previous conduct of the client who is a long-term client of the regulated entity does not raise suspicion or indicate the existence of a risk of money laundering and terrorist financing.

3.2.1.5. Transactions that may carry a higher risk are:
- transactions that significantly deviate from the standard conduct of the client;
- transactions that do not have economic justification (e.g. unexpected repayment of a loan before the due date or in a short period from the date of approval of the loan; unexpected repayment of the leasing item before the due date or in a short period from the date of conclusion of the financial leasing contract);
- a transaction of payment to the account, i.e. repayment of a loan or leasing item was carried out by payment from one or more payers from different countries;
- transactions in which a disproportionately high deposit amount (e.g. 100%) is placed as security for obtaining a loan or borrowing or leasing item;
- unusually large volume or amount of transactions.

3.2.1.6. Likewise, the regulated entity shall be obliged to, when assessing the risk of a transaction, take into account the analysis and review of the method of money laundering for which the Law on anti-money laundering and counter-terrorism financing or the Risk Assessment of money laundering and terrorism financing and proliferation of weapons of mass destruction in Bosnia and Herzegovina has determined a high risk of money laundering or terrorism financing.

3.2.2. Specific factors related to the risk of a product, service or transaction

3.2.2.1. **Banks and other payment service providers**

3.2.2.1.1. Factors that may contribute to an increase in risk for these regulated entities in relation to the product and service risk factor are:
1) private banking, i.e. the provision of private banking services and the management of funds of foreign citizens, which may be particularly risky because a client with a significant amount of money is in charge of one employee or a small group of employees who may be instructed by their superiors to accept anything the client requests, which the client may misuse;
2) electronic banking in cases provided for by the regulated entity in its procedure;
3) electronic issuance of orders for trading in securities in cases provided for by the regulated entity in its procedure;
4) providing clients with whom no business relation has been previously established with those types of services that the employee of the regulated entity, based on its experience, has assessed as carrying a high level of risk (one-off transactions, e.g. money transfers);
5) providing services for opening so-called joint accounts to which funds are transferred from different sources and from different

clients, and which are deposited in one account opened in one name;

6) approving a loan secured by a mortgage if the real estate is located in another country, and especially if it is difficult to determine whether the client has the right of ownership over the subject of the mortgage or it is difficult to determine the identity of the beneficial owner of that real estate;
7) the payment service enables payment transactions in large or unlimited amounts;
8) the payment service has a global scope;
9) the payment transaction is cash-based or financed with anonymous electronic money;
10) the transfer was made by payments from one or more payers from different countries to an account with a bank and
11) activation of an inactive account (the regulated entity is obliged to be particularly careful when activating inactive accounts, especially if the activation of the account involves transactions in significant amounts or shows some of the indicators of suspicious activity. In such cases, among other things, it is necessary for the regulated entity to re-verify the identity of the clients).

3.2.2.1.2. Products and services that may indicate a potentially lower risk are:

1) financial products or services that are provided to a certain type of client with the purpose of increasing financial inclusion;
2) life insurance policies concluded through a payer with a low premium of up to 10,000 KM per year;

3.2.2.1.3. Transactions that may carry a higher risk are:

1) transactions that are carried out in a manner that avoids standard and customary control methods (transactions in amounts slightly lower than the amounts stipulated as limits below which measures stipulated by the Law on anti-money laundering and counter-terrorism financing are not undertaken);
2) complex transactions that include multiple participants without clear economic determination, multiple interconnected transactions that are carried out in a short period or in several consecutive intervals in an amount that is below the limit for reporting to the FIU;
3) loans to legal entities, and in particular loans from founders from abroad to legal entities in the country;
4) transactions whose true basis and reason for implementation is clearly concealed by the client;
5) payments for consulting, management and marketing services, as well as other services for which there is no determinable value or price on the market;
6) transactions for which the client refuses to provide documentation;
7) transactions for which the documentation does not correspond to the method of executing the transaction itself;
8) transactions for which the source of funds is not clear or their connection to the client's business operations cannot be determined;
9) transactions for payment of goods and services to the client's partners that originate from offshore destinations, and the

documentation clearly shows that the goods originate from neighboring countries;

10) transactions based on payment for goods or services in countries that are not usually used to produce the goods being paid for or to perform that type of service;
11) the frequency of transactions based on advance payment for the import of goods or the performance of services where it is not certain that the goods will actually be imported, or the service will be performed;
12) transactions intended for persons against whom international restrictive measures are in force;
13) payment of funds from a client's account, i.e. transfer of funds to a client's account that is different from the account that the client specified during identification, i.e. through which it usually operates or has operated (especially if it is a cross-border transaction);
14) transactions intended for persons with a residence or registered office in a country that is an offshore country;
15) transactions intended for non-profit organizations that have their registered office in an offshore country, i.e. a country that is a tax haven or a country that is not a member of the European Union;
16) the transaction is based on cash or is financed with anonymous electronic money or electronic money products that are exempt from the obligation to perform client due diligence measures,
17) the amount of the transaction sent does not correspond to the income of the client;
18) transactions related to trade in oil, weapons, precious metals, tobacco products, cultural artifacts and other objects of archaeological, historical, cultural and religious significance or of exceptional scientific value, and protected species.

3.2.2.1.4. A less risky transaction may be indicated by the following circumstances:

1) the transfer of funds is made using funds from an account held in the name of the payer with a financial institution of a resident of BiH, or a resident of a country that has the same or stricter standards than those applied in BiH, and the recipient of the funds is a resident of BiH, or a resident of a country that has the same or stricter standards than those applied in BiH;
2) the transaction amount is low (however, regulated entities must bear in mind that small transactions in themselves may not constitute a circumstance indicating a lower risk of money laundering and terrorist financing).

3.2.2.1.5. Regulated entities may apply simplified identification and monitoring measures in relation to an individual business relation or occasional transaction that they assess to pose a low risk of money laundering and terrorist financing, taking into account the results of the Risk Assessment of money laundering and terrorist financing and proliferation of weapons of mass destruction in Bosnia and Herzegovina.

3.2.2.2. **Electronic money institutions**

3.2.2.2.1. The following circumstances relating to the product may indicate the risk assessment of an electronic money institution:

1) limits relating to the issuance and use of electronic money;

2) the method of financing (purchase or top-up) of electronic money; and
3) value in use and transferability.

3.2.2.2.2. The following factors may contribute to a higher risk for an electronic money institution relating to the product:
1) the product enables payments in electronic money, top-up or redemption of that money (e.g. cash withdrawal) in large or unlimited amounts;
2) the product enables large or unlimited amounts of funds to be stored in an electronic money account or on a corresponding instrument;
3) the product can be financed (purchased or topped-up) anonymously or through another electronic money product, especially if that money is anonymous;
4) the product enables person-to-person transfers (P2P);
5) the electronic money associated with the product is accepted as a means of payment by a large number of merchants or at a large number of points of sale;
6) the product is intended to be accepted as a means of payment by merchants selling goods and services associated with a high risk of financial crime;
7) the product can be used for cross-border transactions or for transactions in another country;
8) the product can be used by persons who are not clients of the regulated entity; and
9) the product allows the redemption of electronic money by cash withdrawal.

3.2.2.2.3. The following factors may contribute to a lower risk for electronic money institutions in relation to the product:
1) low-limit payments, top-ups or redemptions of electronic money (including cash withdrawals) are allowed over a certain period (although these regulated entities should be aware that this limitation in itself may not be sufficient to constitute a circumstance that may reduce the risk of money laundering and terrorist financing);
2) the number of payments, top-ups or redemptions of electronic money (including cash withdrawals) is limited over a certain period;
3) the product allows only small amounts to be held in the electronic money account or relevant storage instrument at any one time;
4) the product allows funds for purchase or replenishment, subject to verification, to be transferred from an individual or joint account that the client has opened with a resident financial institution, i.e. a resident of the European Economic Area;
5) the product does not allow or severely restricts cash withdrawals;
6) the product can only be used within one country;
7) the electronic money in connection with that product is accepted as a means of payment by a small number of merchants or points of sale with whose operations the electronic money institution is familiar;
8) the product cannot be used or its use is limited by merchants selling goods and services associated with a high risk of financial crime and

9) the product is accepted as a means of payment only for certain types of low-risk services or products.

3.3. Country/sovereign risk (geographical risk)

3.3.1. General factors

3.3.1.1. When analyzing and assessing the risk of money laundering or terrorist financing associated with countries and geographical areas, the regulated entity shall be obliged to consider the risks in relation to the country and geographical area in which the client and the beneficial owner of the client have their registered office or residence, main place of business operations, or relevant personal and business relations.

3.3.1.2. The significance of geographical risk factors often depends on the nature and purpose of the business relation, and the regulated entity takes into account the following:

1) if the asset used in the business relation was acquired abroad, the regulated entity is obliged to determine what system against money laundering and terrorist financing is established in that country;
2) if the funds are received from a country known to be home to terrorist organisations or are sent to such a country, the regulated entity is required to consider the extent to which this could raise suspicions of money laundering and terrorist financing, based on the regulated entity's knowledge of the purpose and nature of the business relation;
3) if the client is a financial institution of another country or a provider of services related to digital assets headquartered in another country, the regulated entity should pay particular attention to the adequacy and effectiveness of that country's system against money laundering and terrorist financing, in particular in relation to those institutions or service providers;
4) if the client is a trust or a foreign legal entity, the regulated entity is required to, if applicable, take into account the extent to which the country, in which the client or the beneficial owner of the client is located, is in compliance with international tax transparency standards.

3.3.1.3. Risk factors related to the geographical area, which may indicate a potentially higher risk, are particularly considered by regulated entities when clients come from a country:

1) which is subject to sanctions, embargoes and similar measures by relevant international organisations (United Nations, Council of Europe, etc.);
2) for which credible sources (FATF, Council of Europe, IMF, World Bank, etc.) have determined:
   - that it does not have appropriate laws, regulations and other measures to prevent money laundering and the financing of terrorist activities;
   - that it finances or assists terrorist activities and that designated terrorist organisations operate in the country;
   - that there is a significant level of corruption and crime in the country;
3) which is not a member of the European Union or does not apply relevant European Union directives;
4) which, according to the international organization FATF, is classified as a non-cooperative country or territory or if it is an offshore financial center listed on the list created by relevant institutions;
5) which is on the list of high-risk countries created by the Council of Ministers of Bosnia and Herzegovina.

3.3.1.4. Risk factors related to the geographical area, which may indicate a potentially lower risk, include at least the registration, seat or residence of the client in one of the following countries:

1) countries that have an effective system for preventing money laundering and terrorist financing;
2) countries that have been established by credible sources to have a low level of corruption or other criminal offences and
3) countries that, based on credible sources, such as mutual assessments or published reports on further activities, meet the requirements for preventing money laundering and terrorist financing in accordance with the FATF recommendations and effectively implement them.

3.3.1.5. Regarding information on risky countries, i.e. non-cooperative states or territories that do not meet key international standards related to the prevention of money laundering or the financing of terrorist activities, the regulated entity shall monitor the official websites of international authorities.

3.3.2. Specific factors related to the country/sovereign risk (geographical risk)

3.3.2.1. **Banks and other payment service providers**

3.3.2.1.1. Banks and other payment service providers, within the meaning of the law governing payment services, in addition to the application of the general part of these guidelines, shall also apply additional risk factors related to the geographical area:

1) the payer or payee is permanently resident or temporarily residing, i.e. has its registered office or permanently carries out its activities in a country whose legal and institutional framework is such that there is a high level of risk of money laundering and terrorist financing;
2) the payee is permanently resident or temporarily residing, i.e. has its registered office or permanently carries out its activities in a country with a poorly developed regulated banking sector, where money transfer services provided by unregulated entities may be used for payments;
3) the product is financed from a country associated with a high risk of money laundering and terrorist financing;
4) the client or the person for whose benefit the client initiates the execution of a transaction with digital assets has a residence or abode, or is headquartered or carries out business activity in a country whose legal and institutional framework is such that there is a high level of risk of money laundering and terrorist financing;
5) the client is a provider of services related to virtual currencies or other digital assets from a country whose regulations do not regulate digital asset operations and the licensing or registration of digital asset service providers, nor is there supervision over digital asset service providers, or a country whose legal and institutional framework is such that there is a high level of risk of money laundering and terrorist financing, or such a provider of services related to virtual currencies or other digital assets participates in the execution of a transaction with virtual currencies and
6) a provider of services related to virtual currencies or other digital assets from another country participates in the execution of a transaction with virtual currencies, which provides its clients with services related to virtual currencies that directly or indirectly enable the concealment of the client's identity, i.e. which carries out transactions with such virtual currencies.

3.3.2.1.2. The regulated entity shall be obliged to pay special attention to those legal systems that are known for providing funds or providing

support to terrorist activities or that are known to have operational terrorist groups, as well as to legal systems where financial sanctions, embargoes or other punitive measures are in force that have been imposed as a result of links to terrorism, the financing of terrorist activities or the proliferation of weapons of mass destruction.

3.3.2.2. **Microcredit organizations and leasing providers**

3.3.2.2.1. When establishing a business relation with a foreign client, the regulated entity shall be obliged to take into account that the nature and purpose of the business relation can often be a determining factor in the relative importance of individual country and geographical risk factors, in particular:

1) when the funds used in the business relation come from outside Bosnia and Herzegovina,
2) when the client is a credit or financial institution, the regulated entity is obliged to take into account the adequacy of the system for preventing money laundering and terrorist financing of the country and the effectiveness of the supervision of preventing money laundering and terrorist financing in that country,
3) when the funds are received from or sent to countries known to be home to terrorist organizations, these regulated entities are obliged to consider the extent to which this may raise suspicion, based on the regulated entity's knowledge of the purpose and nature of the business relation,
4) when the client is a legal person, these regulated entities are obliged to take into account the extent to which the country, with which the client and, where applicable, the client's beneficial owner are associated, effectively meets international tax transparency standards.

3.4. Distribution channel risk

3.4.1. General factors

3.4.1.1. When analyzing distribution channels, it is necessary to assess how the distribution channels used by the regulated entity to provide its clients with a specific product/service affect the risk of money laundering and terrorist financing.

3.4.2. Specific factors related to distribution risk

3.4.2.1. **Payment service providers and electronic money institutions**

3.4.2.1.1. The following factors may contribute to a higher risk for payment service providers and electronic money institutions in relation to the distribution of electronic money:

1) there are no restrictions on the funding instrument,
2) the distribution channel allows for a certain degree of anonymity,
3) the money transfer service is provided through agents that have unusual turnover compared to other agents in similar locations, e.g.: unusually large or small transactions, unusually large cash transactions, execute a significant number of transactions with payers or payees from countries associated with a higher risk of money laundering and terrorist financing,
4) are not from the financial sector and have another main activity;
5) issuance and distribution of electronic money via the Internet (online) or otherwise without the physical presence of the client, without appropriate identification, such as electronic signatures,

electronic identification documents, as well as other measures aimed at preventing misuse or concealment of the true identity;

6) distribution of electronic money through third parties which are not regulated entities within the meaning of the Law on anti-money laundering and counter-terrorism financing, when the issuer of electronic money relies on the distributor to implement some of the measures that the regulated entity is obliged to implement in order to prevent money laundering and financing of terrorist activities, and has not reliably determined that the distributor has appropriate systems and controls in place to adequately undertake those measures;
7) separation of services, which means the provision of electronic money services by several operationally independent providers of such services without appropriate supervision and coordination.

3.4.2.1.2. When concluding a contract for the distribution of electronic money through third parties, the regulated entity should understand the nature and purpose of the activity carried out by the third party, in order to ensure that the goods and services sold or provided by that person are in compliance with the regulations. The regulated entity should also assess the risks of money laundering and terrorist financing related to the activity carried out by that third party. In the case of a third party operating over the Internet, the regulated entity should also understand the structure of clients that such a person has or will have, as well as determine the expected volume and value of transactions that will be carried out through that third party in order to identify suspicious or unusual transactions.

4. Final provisions

These Guidelines shall enter into force on the date of their issuance and shall be published on the official website of the Banking Agency of Republika Srpska.

Number: D-4/24

Date: 20 March 2024

Director

_____

Srđan Šuput