Annex

Decision No. 1/347A of the Chairman
of the Central bank of the Republic of Armenia
Dated Septermber 24, 2025

GUIDELINE

ON THE CRITERIA OF HIGH RISK AND THE INDICATORS OF SUSPICIOUS ACTIVITY IN RELATION TO MONEY LAUNDERING AND TERRORIST FINANCING

Contents

Abbreviations 3
Introduction 4
Criteria of high risk 6
Indicators of suspicious activity 7
1. Criteria of high risk 8
1.1 Country risk 8
1.1.1. Criteria relating to preventive system 8
1.1.2. Criteria relating to other contextual factors 9
1.2. Customer, transaction or business relationship risk 9
1.2.1 Criteria relating to customer identity and status 9
1.2.2 Criteria relating to customer business profile and reputation 10
1.2.3 Other substantial and situational criteria 10
1.3 Product, service or delivery channel risk 11
1.3.1 Criteria relating to product or service type 11
1.3.2 Criteria relating to product or service delivery channel 12
2. Indicators of suspicious activity 12
2.1 Suspicions with regard to customer This section presents indicators of suspicious activity that are identified through substantial or situational descriptions specific for the customers' identity and status, their conduct and behavior. 12
2.1.1 Indicators relating to customer identity and status 12
2.1.2 Indicators relating to customer conduct and behavior 14
2.2 Suspicions with regard to transaction or business relationship characteristics 18
2.2.1 Indicators relating to nature of transaction or business relationship 18
2.2.2. Indicators relating to type of transaction or business relationship 19
2.2.3. Indicators relating to use of product or pattern of transaction 22
2.3. Suspicions specific for DNFBP operations 24
2.3.1. Realtors and notaries 24
2.3.2. Accountants and auditors 25
2.3.3. Casinos and games of chance 26
2.3.4. Suspicions with regard to NPOs 27

Abbreviations

CDD	Customer due diligence
DNFBP	Designated Non-Financial Businesses and Professions
Law	Republic of Armenia Law on Combating Money Laundering and Terrorism Financing
ML	Money laundering
NPO	Non-profit organization
Regulation	Regulation on Minimum Requirements to Reporting Entities in the Field of Preventing Money Laundering and Terrorism Financing
STR	Suspicious transaction report
TF	Terrorism financing

Introduction

This guideline on the criteria of high risk and the indicators of suspicious activity in relation to money laundering and terrorist financing (hereinafter referred to as the Guideline) has been developed on the basis of the Law and applies to all types of reporting entities as defined in Part 1(4) of Article 3 thereof.

According to Part 1(21) of Article 3 of the Law, the criterion of high risk as defined by the Law, the legal statutes of the Authorized Body, as well as the internal legal statutes of the reporting entity is a circumstance indicating a high likelihood of ML/TF. According to Part 1(31) of the same article, the indicator of a suspicious transaction or business relationship (hereinafter also referred to as the indicator of suspicious activity) as defined by the legal statutes of the Authorized Body, as well as the internal legal statutes of the reporting entity is a situation or signal alerting to the possibility of ML/TF.

With regard to the interrelation, within the ML/TF context, between the **criteria of high risk** and the **indicators of suspicious activity** in relation to customers, business relationships and transactions, it should be noted that:

- The criteria of high risk, i.e. the circumstances indicating the high likelihood of ML/TF do not necessarily comprise indicators of suspicious activity, i.e. situations or signals alerting to the possibility of ML/TF. For example, if the customer is a politically exposed person [1], this does not mean that all of his transactions by default should be considered as signals alerting to the possibility of ML/TF[2];
- The indicators of suspicious activity, i.e. the situations or signals alerting to the possibility of ML/TF often comprise also criteria of high risk, i.e. circumstances indicating the high likelihood of ML/TF. For example, if a customer does not disclose his being a politically exposed person[3], this already comprises criteria of high risk and indicators of suspicious activity[4].

It should be noted that the Law provides for a specific set of measures in the presence of both the criteria of high risk and the indicators of suspicious activity.

In particular, reporting entities are required:

- In the presence of the criteria of high risk – to conduct enhanced due diligence in accordance with Part 2 of Article 18 of the Law; that is to apply an advanced procedure of customer due diligence process[5], which enables to achieve a more comprehensive understanding of the customer's identity and business profile;

---

[1] Here being a family member of a politically exposed person comprises a criterion of high risk relating to customer status.
[2] Given that conducting a transaction does not necessarily comprise an indicator of suspicious activity relating to customer behavior.
[3] Given that being a politically exposed person comprises a criterion of high risk related to customer status.
[4] Here non-disclosure comprises an indicator of suspicious activity related to customer conduct.
[5] The minimum requirements with regard to applying the advanced procedure of customer due diligence process are set out in Clause 33 of the Regulation.

- In the presence of the indicators of suspicious activity – to consider recognizing the transaction or business relationship as suspicious and filing with the Authorized Body a report in accordance with Part 2 of Article 7 of the Law; that is to perform comprehensive analysis[6], which enables to prove or disprove ML/TF suspicions with regard to the transaction or business relationship.

Moreover, where the **enhanced customer due diligence** conducted in the presence of high risk criteria leads to the application of a more rigorous approach to the business relationship with the customer by means of, *inter alia*, obtaining senior management approval to commence the relationship, establishing the source of funds and wealth of the customer, and applying other measures, the **comprehensive analysis** performed in the presence of suspicious activity indicators leads to: a) forming substantiated ML/TF suspicions, to be followed by recognizing the transaction or business relationship as suspicious and filing a report with the Authorized Body[7]; or b) dispelling ML/TF suspicions, to be followed by documenting and maintaining the grounds for non-recognition of the transaction or business relationship as suspicious, the respective conclusions, the process of performed analysis and its findings[8]. At the same time, in the presence of criteria of both high risk and suspicious activity there is still a possibility of a transaction being rejected or a business relationship being terminated[9].

[6] The minimum requirements with regard to performing the comprehensive analysis for identification of suspicious transactions and business relationships are set out in Chapter 7 of the Regulation.
[7] As provided for in Parts 1 and 2 of Article 7 of the Law.
[8] As provided for in Part 3 of Article 7 of the Law.
[9] As provided for in Part 2 of Article 27 of the Law.

Criteria of high risk

According to Part 1(20) of Article 3 of the Law, risk is a circumstance indicating the threat and likelihood of ML/TF, which may be defined in terms of countries or geographic locations, types of customers, transactions or business relationships, services, or in terms of other parameters.

Each type of ML/TF risk is characterized by a set of unique criteria, and assessing the potential impact thereof enables arriving at conclusions on the presence of the given type of risk and on its level being either high, medium or low.

It should be noted that the criteria of high risk are set out both in Part 1(21) of Article 3 of the Law and in Clause 27 of the Regulation. They include[10]:

Criteria of high risk defined by the Law

- Politically exposed persons;
- Persons (including financial institutions), which are domiciled or reside in or are from non-compliant countries[11];
- All complex or unusual large transactions;
- Unusual patterns of transactions or business relationships, which have no apparent economic or other lawful purpose.

Criteria of high risk defined by the Regulation

- Legal persons or arrangements that are personal asset-holding vehicles;
- Companies that have nominee shareholders or shares in bearer form;
- Businesses and business relationships that are cash-intensive;
- Companies that have unusual or excessively complex ownership structure;
- Private banking activities;
- Non-face-to-face business transactions or relationships.

The criteria of high risk as set forth in the above legal acts are attributable to any of the three internationally recognized types of ML/TF risk. They include:

- Country risk;
- Customer, transaction or business relationship risk;
- Product, service or delivery channel risk.

Within the framework of the above-specified categorization, the section of the Guideline regarding the criteria of high risk aims to provide descriptive details of recommendatory nature on the criteria of high risk as established by the Law and the Regulation[12], to assist reporting

---

[10] Since the Law and the Regulation stipulate that the risk is determined by combination of the established criteria, a situation will be recognized as a high risk in the presence of even one criterion of high risk except for the case provided under Clause 24(3) of the Regulation.

[11] Part 1(26) of Article 3 of the Law defines a non-compliant country or territory as the foreign country or territory that, according to the lists published by the Authorized Body, is in non-compliance or inadequate compliance with the international requirements on combating money laundering and terrorism financing.

[12] For the sake of integrity, this section also lists the criteria of high risk established by the Law and Regulation.

entities in conducting enhanced customer due diligence required in the presence of such criteria.

Indicators of suspicious activity

According to Part 2 of Article 7 of the Law, reporting entities should consider recognizing a transaction or business relationship as suspicious and filing with the Authorized Body a report on suspicious transaction or business relationship provided for by Law, if the circumstances of the case under consideration fully or partially match the criteria of suspicious transactions or business relationships.

Part 1(30) of Article 3 of the Law defines as suspicious the transactions or business relationships whereby it is suspected or there are reasonable grounds to suspect that the property involved is the proceeds of a criminal activity or is related to terrorists and terrorist activity. Part 1(31) of the same article defines the indicator of a suspicious transaction or business as a situation or signal alerting to the possibility of ML or TF, as defined by the legal statutes of the Authorized Body, as well as the internal legal statutes of the reporting entity.

The indicators set out in the below section of this Guideline are not a comprehensive and exhaustive description of possible ML/TF suspicions in relation to transactions or business relationships; hence, they should not be understood in literal meaning. Moreover, in practice it is possible that suspicions arise in relation to any other situation which does not match with or derive from the indicators established in this Guideline, in which case reporting entities must also consider recognizing the transaction or business relationship as suspicious and filing an STR. In addition, the indicators of suspicious activity that are more typical of certain ML/TF schemes are defined by the typologies that describe the relevant schemes. The analytical materials published by the Financial Monitoring Center of the Central Bank of the Republic of Armenia also include indicators of suspicious activity.

In particular, according to Part 2 of Article 7 of the Law, reporting entities may, as a result of the relevant analysis, recognize a transaction as suspicious if the logic, pattern (dynamics) of or other characteristics of its implementation provide the grounds to assume that it might be carried out for the purpose of money laundering or terrorism financing. Hence, the indicators established in this Guideline by no means predetermine or restrict the reporting entities' discretion or opportunity to conduct analysis and to recognize a transaction or business relationship as suspicious based on their expert judgment and own decision.

The process for determining whether a transaction or business relationship is suspicious can be initiated not only with regard to established business relationships and completed transactions, but also to attempted ones. At that, *completed transactions and established business relationships* are characterized by the full accomplishment of the chain of actions taken by the customers towards achieving their purposes and provide for the relevant legal consequences to come into effect. *In case of attempted transactions or business relationships*, the customers again take certain actions towards achieving their purposes; however, the relevant

legal consequences do not come into effect, which may occur on the customers' initiative or regardless of their intentions[13].

In practice, it is possible that the analysis performed in the presence of any single indicator of suspicious activity does not lead to the formation of reasonable ML/TF suspicions. Accordingly, there is a higher possibility of ML/TF, if a combination of more than one indicator is present in the transaction or business relationship under consideration.

The sections of the Guideline regarding the indicators of suspicious activity presents indicators of suspicious activity in the transaction or business relationships by means of a conventional grouping that firstly reflects on the characteristics of the customers, in particular their identity and status, as well as conduct and behavior, then on the characteristics of the transactions and business relationships, in particular their nature, type and pattern of implementation. These indicators are applicable for both financial institutions and non-financial institutions defined by Law. Additionally, as regards disclosure of ML/TF suspicious transactions and business relationships, indicators of suspicious activity specific for the operations of DNFBPs such as advocates and lawyers, accountants and auditors, organizers of casinos and games of chance, as well as indicators of suspicious activity specific for the relationships with non-profit organizations are presented in this Guideline.

1. Criteria of high risk

1.1 Country[14] [15]risk

To distinguish this type of ML/TF risk, reporting entities should answer the following questions – what geographic locations do we operate in, and what are the countries of location and/ or operation of our customers' counterparties? To determine the presence and level of this type of risk, the following criteria are to be considered as a priority:

1.1.1. Criteria relating to preventive system

1.1.1.1 Countries identified by credible sources[16]as not having adequate AML/CTF systems, or having strategic gaps in their AML/CTF systems, or being a higher ML/TF risk for any other reasons;

1.1.1.2 Countries subject to embargos, sanctions or similar measures issued by the United Nations;

---

[13] For example: a) the customer takes certain actions aimed at establishing a business relationship; however, before signing of the agreement for opening an account he gives up establishment of such relationship on his own initiative, realizing that he cannot meet all requirements of the bank for customer due diligence; or b) the customer approaches to originate a transfer, but fails to present a valid identification document or correctly fill in the payment order, resulting in the bank's rejection of the transaction and the failure of the attempted transaction regardless of the customer's intentions.

[14] For the purposes of this Guideline, all references to the term "country" equally refer to territories or jurisdictions.

[15] Whose resident the customer is, or with which the customer has business, financial or legal connections, or where funds are generated, or where funds are sent to, or which is related to the transaction.

[16] For example, the FATF, the International Monetary Fund, the World Bank, the Egmont Group.

1.1.1.3 Countries designated under ML/TF-related lists published by relevant international organizations[17]or national bodies[18];

1.1.1.4 The country is identified by credible sources[19] as exposed to potential risks and/or having ascertained record of terrorism, financing of terrorism and supporting thereof.

1.1.2. Criteria relating to other contextual factors

1.1.2.1 Countries identified by credible sources[20] as having significant levels and/or ascertained record of corruption and other criminal activity;

1.1.2.2 Countries where drug production and marketing, human trafficking and/or other serious criminality, including financial crimes, are prevalent;

1.1.2.3 Countries considered to be a "tax heaven"[21] or a ”tax shelter”;

1.1.2.4 Countries known for strict laws on banking, trade and other secrecy[22].

1.2. Customer, transaction or business relationship risk

To distinguish this type of ML/TF risk, reporting entities should answer the following questions – who are our customers, and what kind of business relations do we have with them? To determine the presence and level of this type of risk, the following criteria are to be considered as a priority:

1.2.1 Criteria relating to customer identity and status

1.2.1.1 Non-resident natural and legal persons that lack an apparent economic or other legitimate rationale for using the Armenian financial or non-financial systems;

1.2.1.2 Financial institutions[23] that are not subject to effective supervision;

1.2.1.3 Organizations operating in various countries that do not have centralized control or mind and management in any country;

1.2.1.4 Individuals and organizations providing mediation services that have no apparent business purpose;

---

[17] For example, the European Union.
[18] For example, the Office of Foreign Assets Control (OFAC) of the U.S. Treasury.
[19] For example, security services of VARIOUS countries, media publications.
[20] For example, Transparency International, GRECO, Doing Business, etc.
[21] Lists of "tax heavens" or "tax shelters" are published by the Organization for Economic Cooperation and Development, the European Union and the Tax Justice Network.
[22] Reports on comparative assessments and analyses of secrecy norms are published by the Tax Justice Network, in the form of financial secrecy indexes.
[23] In particular, foreign banks and financial service providers, including money transfer services, currency exchange offices, etc.

1.2.1.5 Legal persons that are personal asset-holding vehicles[24];

1.2.1.6 Customers that own large property or extensive wealth;

1.2.1.7 Customers that utilize high-value services[25];

1.2.1.8 Cash and crypto-asset intensive businesses, including:

- Money services businesses[26],
- Crypto-asset service providers;
- Casinos, games of chance, lotteries;
- Convenience stores, gas stations and other fast consumption sales outlets;

1.2.1.9 Providers of intermediation and representation services that are not monitored or controlled for compliance with ML/TF requirements[27].

1.2.2 Criteria relating to customer business profile and reputation

1.2.2.1 Customers that have been subjected to criminal liability for corruption crimes[28], as well as for grave or particularly grave crimes committed deliberately[29];

1.2.2.2 Customers that have been subjected to liability for economic infringements ;

1.2.2.3 Natural and legal persons associated[30] with persons having deliberately committed grave or particularly grave, as well as corruption crimes;

1.2.2.4 Persons that have been refused by other financial institutions/DNFBPs to carry out a transaction or establish a business relationship;

1.2.2.5 Fictitious companies[31] and persons operating through them.

1.2.3 Other substantial and situational criteria

1.2.3.1 The company's legal status and ownership structure[32] do not allow identification of the beneficial owners;

---

[24] In particular, legal persons or arrangements established by an individual for the management of investment assets.
[25] For example, the so-called personal secretary (the international term is "concierge banking") or personalized banking (the international term is "private banking") services.
[26] For example, money transfer service providers, their agents, currency exchange offices, merchants of banknotes, funds transfer or similar courier service providers.
[27] For example, mortgage and deposit agents, brokers.
[28] The list of corruption crimes is established in Annex 1 to the Criminal Code of the Republic of Armenia.
[29] Detailed data on criminal, administrative or civil liability measures applied by the judiciary are available at the Judicial Information System. Reporting entities may also use other available sources, as well as obtain relevant information from the customer within the framework of CDD measures.
[30] For the purposes of the Guideline, more comprehensive definition of “associated person” is provided in Article 8 of the Law on Banks and Banking.
[31] Fictitious companies are those that, while officially registered in a jurisdiction, have no actual domicile, real assets, recorded activity or other features of meaningful existence.
[32] Including the existence of nominee shareholders and directors.

1.2.3.2 The customer is a corporate entity with: a) unreasonably complex structure of the governance bodies; b) unreasonably frequent changes in the composition or membership of the governing bodies; c) persons in the governance bodies with crime or offense record;

1.2.3.3 The business relationship with the customer is established or the transactions are carried out in unusual circumstances with no reasonable explanation[33];

1.2.3.4 The customer conducts transactions or establishes business relationships on unusual terms without any apparent economic or other legitimate rationale;

1.2.3.5 The customer purchases securities that are not consistent with their securities portfolio or the transaction history conducted in the course of the business relationship, without presenting any economic or other legitimate rationale;

1.2.3.6 The funds involved in the transactions have been obtained from decentralized crypto-asset wallets or decentralized trading platforms.

1.3 Product, service or delivery channel risk

To distinguish this type of ML/TF risk, reporting entities should answer the following questions – what products and services do we offer, and what are their delivery channels? To determine the presence and level of this type of risk, the following characteristics are to be considered as a priority:

1.3.1 Criteria relating to product or service type

1.3.1.1 Bearer shares;

1.3.1.2 Bearer payment instruments, including bearer checkbooks;

1.3.1.3 Products that permit receipt of payments from unknown third parties or those unconnected with any party[34];

1.3.1.4 E-wallets, prepaid cards and similar products[35], except for cases where the risk is effectively mitigated in the manner prescribed by the law[36];

1.3.1.5 Products that enable the use of correspondent banking relations by customers of third parties[37];

---

[33] For example, the customer's geographical distance from the financial institution/ DNFBP.

[34] For example, products that permit receipt of payments that lack the originator's forename and surname or company name, as well as the account number (or, in the absence thereof, the unique reference number accompanying the transfer).

[35] For example, products that enable relatively easy and quick deposit, accumulation and withdrawal of cash and cash-equivalent instruments.

[36] In particular, the cases where the risk is effectively mitigated by the internal procedures of the reporting entity established in accordance with Article 23 of the Law.

[37] For example, the "payable-through" accounts stipulated in letter "e" of the first paragraph of FATF Recommendation 13.

1.3.1.6 Postal transfers and similar international payment services;

1.3.1.7 Personalized banking services[38];

1.3.1.8 Services related to the trade in and delivery of banknotes and precious metals[39].

1.3.2 Criteria relating to product or service delivery channel[40]

1.3.2.1 Non-face to face business relationships or transactions;

1.3.2.2 Services provided exclusively through the Internet, telephone, email and other communication means;

1.3.2.3 Online banking services, transactions via wireless communication, mobile banking services.

2. Indicators of suspicious activity2.1 Suspicions with regard to customer This section presents indicators of suspicious activity that are identified through substantial or situational descriptions specific for the customers' identity and status, their conduct and behavior.

2.1.1 Indicators relating to customer identity and status

2.1.1.1 Authenticity or reliability of the identification data presented by the customer when establishing the business relationship or carrying out the transaction are questionable and need additional inquiries;

2.1.1.2 The customer wants to remain anonymous or to possibly reduce the scope and depth of the identification data to be provided41 when establishing the business relationship or carrying out the transaction;

2.1.1.3 The customer pursues to obtain unconditional guarantees to ensure the secrecy of the transaction or business relationship42;

2.1.1.4 The customer presents copies of the identification documents only and refers to different circumstances to explain the absence of the originals;

2.1.1.5 The customer uses identification documents that bear signs of alteration or falsification, or otherwise do not appear to be trustworthy;

---

[38] The international term is "private banking".
[39] For example, gold bullions.
[40] The criteria set out in this subsection apply to cases when the entire process of establishing business relationships and conducting transactions, including execution of payments, takes place in non-face to face mode, using online platforms. That is, the cases where prior to establishing the business relationship or carrying out the transaction specific actions (e.g., customer identification and verification of identity) are taken by means of face to face communication and, as a result, the minimum CDD measures defined by the AML/CTF legislation are undertaken, would not be considered to comprise a criterion of higher ML/TF risk.
[41] For example, does not advice on having more than one passport, having a foreign nationality.
[42] For example, proposes to include a clause into the contract on opening the account that the information on his transactions under no circumstances would be made accessible to third parties, including public authorities.

2.1.1.6 The customer occasionally presents different identification documents43;

2.1.1.7 The customer presents different types of identification documents44 issued by the relevant authorities in various countries;

2.1.1.8 The customer has one or more times changed his forename and/or surname and does not have a reasonable explanation for that[45];

2.1.1.9 The customer's home, work or cell phone does not respond, is disabled, out of reach, or does not exist;

2.1.1.10 The customer uses a personal mailbox, general mailing or other correspondence addresses instead of a home or office address, in places where this is not a common practice;

2.1.1.11 The information available on the customer misses some important details such as the actual place of residence, the active phone number, the email address;

2.1.1.12 Usually available general information on the customer, including data on education and career is too scarce or unavailable[46];

2.1.1.13 The information provided by the customer is certified exclusively by foreign sources, and its reliability cannot be verified for certain reasons;

2.1.1.14 All documents on the customer's identity and status are newly produced or recently issued;

2.1.1.15 Information on the customer's identity and status is unrealistic or not supported by relevant documents[47],

2.1.1.16 The customer's status[48] is inconsistent with the substantiations submitted for establishing the business relationship or carrying out the transaction[49;]

2.1.1.17 The information obtained on the customer confirms or discloses his past or current involvement in criminal activity.

---

[43] For example, a passport, ID card, military card.
[44] For example, a passport of the Armenian citizen; a temporary residence permit in a foreign country; a return certificate issued by an Armenian embassy abroad.
[45] For example, taking the surname of the husband is a reasonable explanation for the change of surname.
[46] Examples of usually available information include the person's forename, surname, patronymic, date of birth, registration address (e.g. available in the Republic of Armenia Voters Registry), data on secondary and higher education (e.g. available through different social networks and websites).
[47] For example, a customer introduces himself as the authorized representative of a foreign wealthy individual or major investment firm, or as a successful business person, but does not present any facts other than unconfirmed statements to support his statements.
[48] For example, a student, unemployed, self-employed, etc.
[49] For example, activities related to the large scale import/export of goods, major transactions in the real estate market, charity, etc.

2.1.2 Indicators relating to customer conduct and behavior

Actions aimed at circumvention of CDD and other preventive measures

2.1.2.1 The customer demonstrates special interest in the reporting entity's internal management and control systems, policies and procedures;

2.1.2.2 The customer asks questions that indicate advanced awareness of the regulations on and thresholds for mandatory and suspicious transaction reporting;

2.1.2.3 The customer carries out fragmented or structured transactions to stay below the reporting thresholds;

2.1.2.4 The customer reduces the originally intended amount of the transaction to avoid CDD measures;

2.1.2.5 The customer carries out two or more transactions with a total sum just below to exceeding the CDD threshold established for linked occasional transactions[50];

2.1.2.6 The customer cooperates with other persons for the purpose staying below the identification and mandatory reporting thresholds[51];

2.1.2.7 The customer is an authorized person acting on behalf of several legal entities at the same time;

2.1.2.8 The customer that is a natural person provides for CDD purposes an address, phone number or other contact information, which coincide with the corresponding data of one or more commercial entities;

2.1.2.9 The customer has changed his residence (registration) address, location or place of business many times;

2.1.2.10 The customer does not advise that there is a beneficial owner in the transaction or business relationship, whereas there are data or suggestions about the existence of the beneficial owner[52];

2.1.2.11 The customer refuses to provide information on the beneficial owner of the transaction or business relationship, or provides misleading or false information[53];

2.1.2.12 The customer attempts to conceal the circumstance that he is a politically exposed person;

---

[50] Linked occasional transactions are defined in Part 1(11) of Article 3 of the Law.

[51] For example, instead of executing the exchange of 5.3 million Armenian drams in one transaction, he comes to the bank with two relatives and carries out two transactions of 2.6 and 2.7 million Armenian drams.

[52] For example, the driver of a well-known businessman attempts to open an account to be used for carrying out large scale operations.

[53] For example, the driver of a well-known businessman claims that the funds in the large scale operations transacted through his account come from the non-refundable assistance provided by his distant relatives.

2.1.2.13 The customer does not disclose the circumstance that he or she is a trustee or managing person of other similar legal arrangement;

2.1.2.14 The customer attempts to convince the staff to refrain from performing the documentation necessary for establishing the business relationship or carrying out the transaction;

2.1.2.15 The customer conducts transactions with such natural or legal persons, regarding which an alert has previously been received on the hypothesis of illegal trafficking of narcotic drugs, or with persons associated with them;

2.1.2.16 The customer repetitively and with no good reason delays the filing of the corporate documents that ascertain the legal status and financial situation of the organization;

2.1.2.17 The customer submits documents to substantiate its operations, which have the features of feint and fictitious transactions (contracts)[54].

Unusual and suspicious actions

2.1.2.18 The customer is accompanied and watched by other persons when establishing the business relationship or carrying out the transaction[55];

2.1.2.19 The customer is nervous and irritable when communicating with the customer service staff;

2.1.2.20 The customer is obviously reluctant to answer questions about his identity and business profile, about the purpose of the transaction or business relationship;

2.1.2.21 The customer obviously over-performs to give persuasive answers;

2.1.2.22 The customer uses different spellings of his forename and surname in various documents; has more than one signature;

2.1.2.23 The customer provides unreliable data about the circumstances and conditions of the transaction or the business relationship[56];

2.1.2.24 The customer provides confusing details about the transaction or the business relationship [57];

---

[54] The definition of feint and fictitious transactions (contracts) is provided under Article 306 of the Civil Code, and the relevant features are set out in the typology No. 11,"*Money Laundering by Means of Feint and Fictitious Transactions (Contracts)"* published by the Financial Monitoring Center of the Central Bank.

[55] For example, the customer always comes with another person and obviously follows his instructions to carry out transactions.

[56] For example, advises that the funds originate from the sale of an apartment, but presents a three-year old contract for apartment purchase and sale, where he is not the selling party.

[57] For example, advises that the sender of the money transferred to him is his male cousin living abroad, while the actual transfer has been received from a female of another nationality.

2.1.2.25 The customer has a limited understanding of the purpose of the transaction or the business relationship [58];

2.1.2.26 The customer makes contradictory and mutually exclusive statements[59];

2.1.2.27 The customer sets on proving that the funds derive from a legal origin and are no way connected with money laundering;

2.1.2.28 The customer requires the services to be rendered with inexplicable urgency;

2.1.2.29 The customer negotiates specifying in the transaction documents a price that is apparently lower or higher than the real or market value;

2.1.2.30 The customer strives to establish friendly relations with the service staff, or offers money, assistance or other types of rewards for their services;

2.1.2.31 The customer is engaged in an economic activity with unreasonable financial profitability or losses;

2.1.2.32 The customer does not know the other party to the transaction and does not have information about the nature of its activities;

2.1.2.33 The customer has no idea about the source of the transacted funds;

2.1.2.34 The customer is involved in suspicious transactions and has no idea that there are indicia of money laundering in his operations[60];

2.1.2.35 The customer's operations are typical for the victims of mass marketing fraud or financial pyramids[61];

2.1.2.36 The customer's operations are typical for the victims of attractive business proposals' fraud scheme[62];

2.1.2.37 The customer sells their assets or shares at a price lower than the market price or at an obviously non-profitable price;

---

[58] For example, advises that the amount has been sent by his friend living abroad, who would give further instructions on its disposal.
[59] For example, argues that the purpose of the cross-border transfer is to arrange summer holidays, whereas the beneficiary of the transfer is a company involved in the trade of construction materials.
[60] For example, regularly receives funds from accounts in one foreign country and transfers them to another foreign country, while retaining a certain fee for his services.
[61] For example, attempts to transfer 1.000 US dollars to a distant African country as if for the completion of the documents on the "heritage received" from a distant relative.
[62] For example, attempts to transfer 10.000 US dollars to a Latin-American country as if for "profitable investment" in gold mine stocks.

2.1.2.38 The customer who deposited large-scale funds for a long-term investment, requests to cancel the transactions and to withdraw or transfer the funds without proper justification;

2.1.2.39 The customer's operations indicate that securities may be traded in a pre-arranged or otherwise non-competitive manner, including trading of illiquid or below-market-value securities, which may suggest market manipulation[63];

2.1.2.40 The customer buys or sells large volumes of securities or option contracts related to the securities immediately before the release of the significant news or announcement (material fact), which may suggest potential insider trading or market manipulation;

2.1.2.41 The customer that has not had any actual entrepreneurial activity for a long time unexpectedly becomes active;

2.1.2.42 The customers that have come together simultaneously carry out similar transactions or establish business relationships[64];

2.1.2.43 Several customers access online banking systems from the same electronic system, or have identical or similar contact details;

2.1.2.44 The customer concludes at the same branch a series of transactions on the same day apparently trying to use the services of different staff members;

2.1.2.45 The customer is interested in how the financial institution conducts transactions to/from account located in non-compliant countries;

2.1.2.46 The customer uses new financial instruments that can effectively conceal the source or intended purpose of funds (P2P transfers, ATM cash withdrawals, prepaid cards);

2.1.2.47 The customer unexpectedly reactivates the accounts or payment instruments that have not been used for a long period of time;

2.1.2.48 The legal person customer repeatedly provides updated information about participants, beneficial owners, head of the executive body, as well as nature of its activities;

2.1.2.49 The customer or the counterparty operates online websites whose characteristics appear to correspond to the types of fraud, for example offering investment services without holding the appropriate license or authorization;

---

[63] For example, the so-called "wash trading of securities" or cross-trading.
[64] For example, each of them converts 4.9 million Armenian drams into US dollars.

2.2 Suspicions with regard to transaction or business relationship characteristics

This section presents indicators of suspicious activity that are identified through substantial or situational descriptions specific for the nature and type of the transactions or business relationships, the products used and the patterns applied therein.

2.2.1 Indicators relating to nature of transaction or business relationship

2.2.1.1 The transaction or business relationship is inconsistent with the business relations/ practices applicable in the given industry[65];

2.2.1.2 The transaction or business relationship obviously is not profitable or economically viable for the customer;

2.2.1.3 The number and volume of the transactions lack rationale based on simple economic analysis;

2.2.1.4 The transactions are inconsistent with the customer's status[66] or business profile[67];

2.2.1.5 The parties to the transaction are natural persons whose bank accounts have been used to circulate large volumes of funds for business purposes;

2.2.1.6 The parties to the transaction are often involved in transactions consisting of receipt/transfer of various amounts of funds, and a contract suggesting a single transaction has been submitted as underlying documentation;

2.2.1.7 The business relationship between the parties to the transaction lacks an apparent economic or other legitimate rationale [68];

2.2.1.8 The subject of the transaction is advisory and similar services in large amounts and with uncertain parameters for measurement/assessment;

2.2.1.9 The transactions are carried out with inexplicable involvement by intermediaries[69];

2.2.1.10 The payment for the transaction is carried out by a person who has no relationship with the customer, and there is no reasonable explanation for this;

2.2.1.11 The transaction price is apparently lower or higher than the real or market value of the transaction subject.

---

[65] For example, an individual entrepreneur engaged in agricultural activity concludes a large contract to obtain consultant services.

[66] For example, a customer with no known source of major income makes large cash deposits, buys expensive property.

[67] For example, an individual entrepreneur engaged in grocery retailers wants to make use of a letter of credit or other trade finance instrument for the import of a large batch of automobile spare parts.

[68] For example, a food importer concludes a deal with an automobile spare parts exporter.

[69] For example, Company A concludes a contract with Company B for the latter to engage Company C for facilitation of market research to sell its products in Country D.

2.2.2. Indicators relating to type of transaction or business relationship

Transactions with use of cash

2.2.2.1 The customer frequently carries out large cash transactions that are inconsistent with his business profile;

2.2.2.2 The customer frequently exchanges large denomination banknotes for small denomination ones;

2.2.2.3 The customer regularly buys significant amounts of gold in cash;

2.2.2.4 The customer performs successive cash transactions in "unrounded" amounts[70];

2.2.2.5 The customer regularly carries out cash transactions at amounts slightly below than the mandatory reporting threshold;

2.2.2.6 The customer carries out large currency conversion transactions in cash that lack an apparent economic or other legitimate rationale;

2.2.2.7 The customer submits uncounted cash to fund a transaction and, after counting the banknotes, reduces the transaction amount as much as is necessary for staying below the mandatory reporting threshold;

2.2.2.8 The customer that is a natural person submits a large amount of cash for depositing on his personal account, with obvious signs of skilled packing or factory marking on the banknote bundles;

2.2.2.9 The customer has deposited a large amount of cash into their personal account, presenting the source of funds as proceeds from the conversion of crypto-assets;

2.2.2.10 The corporate customer regularly performs cash (cashbox) transactions;

2.2.2.11 The customer regularly makes cash deposits into personal accounts of other persons, presenting them as “charity”, “humanitarian aid”.

Transaction with use of accounts

2.2.2.12 The pattern of transactions carried out through the customer’s account are inconsistent with his business profile[71];

2.2.2.13 Funds are credited and debited on the customer's account without an apparent economic or other legitimate rationale;

2.2.2.14 The customer’s account is used to credit a large number of small amounts and subsequently to debit a small number of large amounts, or vice versa;

---

[70] For example, 4.915.610 Armenian drams, 8.971 US dollars etc.

[71] For example, a pensioner that has no declared source of income receives large amounts from persons apparently unrelated to him; a person registered as unemployed makes a transfer to buy an expensive car.

2.2.2.15 The customer has a number of accounts opened with different statuses[72] and carries out transactions between them[73];

2.2.2.16 The accounts of a natural person are used to make payments within the framework of the contractual obligations of a legal entity;

2.2.2.17 Unexplained transactions are carried out between accounts opened for personal and business purposes;

2.2.2.18 Funds from a company account are transferred to the account of a natural person who is a shareholder, director or employee of the company, or a person affiliated with them;

2.2.2.19 The company receives transfers from the account of a natural person who is a shareholder, director or employee of the company, or a person affiliated with them;

2.2.2.20 The company account is used to make regular payments, which are not salaries or fees for services, to individuals;

2.2.2.21 The customer's accounts are used for frequent and unexplainable transfers of funds to various financial institutions;

2.2.2.22 A number of deposits are made on a reactivated account with a negligible or zero balance, immediately followed by one or several withdrawals until disbursing the account balance;

2.2.2.23 The customer opens accounts at different financial institutions within the same area without an apparent economic or other legitimate rationale;

2.2.2.24 A small local company on the same day deposits funds on its accounts at different branches without an apparent economic or other legitimate rationale;

2.2.2.25 Transfers from foreign cards to the customer's bank accounts are often canceled by the originator;

2.2.2.26 Transfers to the customer's bank accounts are received from cards reported as lost or stolen.

Wire transfers

2.2.2.27 The customer sends and receives wire transfers to/ from accounts in non-compliant countries, and their economic purposes are unknown;

---

[72] For example, as a natural person, an individual entrepreneur, a legal entity's authorized representative.

[73] For example, deposits funds on the personal account, then transfers them as a loan to the account of the individual entrepreneur, then submits a payment order to transfer the funds to the account of the legal entity, then withdraws the amount in cash.

2.2.2.28 The customer makes personal or business wire transfers to areas that are associated with drugs and human trafficking, other types of criminal activity;

2.2.2.29 The company that has no activity in the country of registration uses the Armenian financial institution to transfer funds from one foreign country to another;

2.2.2.30 Payable-through accounts of the financial institution accounts enable the customers of foreign correspondent banks to carry out transactions directly with third parties; including sending and receiving funds;

2.2.2.31 Funds transferred from a foreign country are returned to the country of origin for the benefit of the original sender or of a third party;

2.2.2.32 A number of customers make wire transfers to the same beneficiary;

2.2.2.33 A number of customers with the same beneficial owner receive wire transfers;

2.2.2.34 A large number of small amount wire transfers are regularly made with obvious features of structuring;

2.2.2.35 Wire transfers are made in a structured manner that cannot be reasonably explained[74];

2.2.2.36 The company receives large wire transfers inconsistent with its account usage pattern and sends them to one or several (foreign) accounts;

2.2.2.37 The company's account balances are regularly transferred to the accounts of foreign companies subsequent to receipts of comparable transfers from the same or other foreign companies;

2.2.2.38 The company executives or employees immediately withdraw in cash wire transfers received from abroad, or provide loans to other persons, often in a chain-like manner, making it difficult to identify the source and ultimate purpose of funds ;

2.2.2.39 The number and volume of wire transfers by the customer are inconsistent with his regular activities.

Deposit and loan transactions

2.2.2.40 The customer makes deposits into the bank accounts held with several banks with a large total amount;

2.2.2.41 The customer makes frequent deposits presenting them as proceeds of the sale of assets;

[74] For example, payments within the scope of the same contract are made in several transfers without reasonable explanation.

2.2.2.42 The customer makes deposits with different characteristics[75] on various accounts, then transfers them regularly to an account at the same or another bank;

2.2.2.43 The customer regularly withdraws the deposit amount in cash, and shortly afterward redeposits cash into their accounts and/or makes a deposit, presenting the previously withdrawn deposit as a source of funds;

2.2.2.44 The customer quickly withdraws in cash the funds of the major credit transferred to his account from abroad;

2.2.2.45 The customer makes frequent premature repayments of loan liabilities;

2.2.2.46 The customer makes a large loan repayment from an unknown source that is not consistent with the information available on the customer;

2.2.2.47 The customer makes large repayments of a mortgage loan;

2.2.2.48 The customer repays long-term liabilities; such as the mortgage loan, in a period of time significantly shorter than the one stipulated by the contract;

2.2.2.49 The customer regularly receives funds as a repayment of previously provided loans or as a receipt of new loans;

2.2.2.50 The source of the advance payment for the loan is inconsistent with available data on the customer's activity and income;

2.2.2.51 The advance payment for the loan is received from various financial institutions by means of several transfers;

2.2.2.52 The customer is not interested in loan terms or fees and related expenses;

2.2.2.53 The customer acquires major assets to pledge as collateral for a loan with no apparent economic or other legitimate rationale;

2.2.2.54 The customer makes few or no repayments for the loan secured by collateral of major assets, which uncovers his initial intention of not repaying the loan on one hand, and using the loan as evidence of legality of the funds on the other hand.

2.2.3. Indicators relating to use of product or pattern of transaction

2.2.2.55 A letter of credit or another trade finance instrument is used in the transaction, which is not consistent with the customer's business profile;

2.2.2.56 Payment instruments such as nominee securities, traveler's checks[76] are used in the transaction[77];

---

[75] For example, with different terms of maturity, in different currencies, through different deposit instruments etc.
[76] Including the cases when the documents contain uncompleted fields, unusual marks or symbols.
[77] Including the cases of using them as a collateral.

2.2.2.57 Checks issued on behalf of third parties, credit or debit cards owned by third parties are used in the transaction;

2.2.2.58 Personal or corporate accounts/ cards with large usage limits are used in transactions for divergent purposes[78];

2.2.2.59 Online transactions are carried out with parties whose IP address[79] is in a non-compliant country;

2.2.2.60 Online transactions with obscure and unclear purposes are carried out;

2.2.2.61 Transactions in large numbers or amounts are carried through accounts of internet betting companies;

2.2.2.62 There is a long time gap between the dates of product or service delivery and dates of payments made/ to be made for them, without an appropriate guarantee of payment that is usually applicable to installment payments.

2.2.2.63 Making advance payments to the tax authority's account from foreign or unidentified bank cards, followed by their refund within a relatively short period based on a respective application, without providing reasonable justification.

Indicators of suspicious activity in relation to crypto-assets

2.2.2.64 The customer's funds originate from or are directed to the platform that is not registered in the country of the customer or the crypto-asset service provider;

2.2.2.65 The customer is involved in large-scale crypto-asset transactions that are presented as transactions conducted on their behalf or in their account[80];

2.2.2.66 The customer's funds originate from or are directly or indirectly directed to the account/wallet address that has been recognized as suspicious in relation to terrorist activities or their financing (through public lists, open sources, crypto-asset intelligence companies, etc);

2.2.2.67 The customer sends crypto-assets to platforms that are located in non-compliant countries or territories, or are not subject to effective supervisory mechanisms;

---

[78] For example, a personal card is used for business purposes, or vice versa.
[79] The international term is "Internet Protocol address":
[80] For example, the customer conducts a transaction on a personal account, receiving funds from external addresses that are immediately converted into other currencies or other type of crypto-assets and are transferred to the same external address (or to another address that in some way linked to the original address)

2.2.2.68 The customer engaged in crypto-asset service provision receives large amounts of funds through fast/instant transfer systems[81];

2.2.2.69 Crypto-asset transactions are conducted between accounts/wallets that have been opened by persons connected with each other by common data[82];

2.2.2.70 The customer uses crypto-asset "mixers" [83], "tumblers" [84] and/or receives funds from the sale of privacy coins[85];

2.2.2.71 The customer uses cross-chain bridges[86] to exchange crypto-assets (for example Bitcoin Ethereum), making frequent or high-value deposits or withdrawals;

2.3. Suspicions specific for DNFBP operations

This section presents indicators of suspicious activity that are specific for the situations arising in the course of activities of designated non-financial businesses and professions stipulated by the Law, such as realtors and notaries, accountants and auditors, organizers of casinos and games of chance, when they involve in operations (including financial transactions) for or on behalf of their customers. The indicators are not exhaustive, and all DNFBP should also assess the relevance and availability of the indicators specified in other sections of the Guidance, including in relation to the existence of situations and alerts indicating the likelihood of ML.

2.3.1. Realtors and notaries

2.3.1.1 The customer acquires real estate that was alienated recently, or alienates the real estate that was acquired recently;

2.3.1.2 The same real estate is regularly alienated to certain associated persons;

2.3.1.3 Transactions related to the same property are conducted within a short period of time, including through different notaries;

2.3.1.4 The customer alienates or acquires real estate, which is inconsistent with his business profile;

2.3.1.5 The customer sells the real estate shortly after buying it for a significantly different price, when there are no substantial price changes in the market;

---

[81] For example, card-to-card transfer, transfer from an electronic wallet, etc.
[82] For example, citizenship, IP address.
[83] Mixers are service providers that split the crypto-assets of their customers and conduct large-scale transactions between own crypto-accounts to conceal the traceability of transactions (for example, Coinjoin, Wasabi Wallet, Samurai Wallet).
[84] Tumblers are service providers that split the crypto-assets of their customers and make multi-level transfers between newly-created and reserve crypto-asset accounts managed by them to conceal the traceability of the transactions (for example, Tornado Cash, Join Market).
[85] "Privary coins" crypto-assets allow persons to remain untraceable or make anonymous private transfers (for example, Monero, Dashcoin, Zcash, Grin, etc.)
[86] Cross-chain bridge is a tool that allows transferring crypto-assets between various blockchains.

2.3.1.6 The customer seeks to buy high-value real estate within the shortest possible time, without specifying any particular requirements, preferences, desired location, or without entering into negotiations on the price of the property

2.3.1.7 The customer demonstrates unusually advanced awareness with regard to the AML/CTF legislative requirements in relation to real estate transactions;

2.3.1.8 The customer decides not to proceed with the transaction after being asked questions about the source of funds or the method of payment;

2.3.1.9 The customer avoids performing real estate acquisition transactions on his own behalf, or register the acquisition of the real estate in the name of another person without any reasonable rationale;

2.3.1.10 The customer presents unreasonable explanations as to the last-minute changes in the contract regarding the buyer's name, the transaction amount or other substantial details;

2.3.1.11 The customer seeks to sell the real estate acquired previously within a short period of time, at a price significantly different from the acquisition price;

2.3.1.12 The customer negotiates specifying in the real estate sales contract a price that is lower or higher than the real or market value.

2.3.2. Accountants and auditors

2.3.2.1 The customer makes payments to foreign companies for consulting or similar services, which is inconsistent with its business profile;

2.3.2.2 The customer reports revenues that are significantly less than the costs of running the company; however, the company continues its non-profitable activity without a reasonable explanation;

2.3.2.3 The customer purchases a number of assets used for personal or consumption purposes[87], where this is inconsistent with the business practice of the industry or the particular type of business activity;

2.3.2.4 The customer has no employees; which is not typical for the particular type of business activity;

2.3.2.5 The customer's invoices or expenditure documents contain obvious technical or substantive discrepancies;

2.3.2.6 The amounts specified in sales bills do not match with the actual value of sold goods;

2.3.2.7 The customer frequently changes the accounting service providers;

---

[87] For example, expensive yachts, cars, houses.

2.3.2.8 The customer is not aware of the whereabouts of its financial statements and supporting documents;

2.3.2.9 The customer reports liabilities in its financial statements, which in fact do not exist or have been repaid;

2.3.2.10 The customer's liabilities[88] are inconsistent with its entrepreneurial activities;

2.3.2.11 There are significant discrepancies between the customer's factual activities and accounting documents.

2.3.3. Casinos and games of chance

2.3.3.1 Upon opening a gambling account the customer deposits a large amount into the gambling account;

2.3.3.2 After funding the gambling account the customer seeks to withdraw the funds available in the gambling account without placing any bet;

2.3.3.3 The customer regularly carries out transactions in amounts just below the identification or mandatory reporting thresholds;

2.3.3.4 The customer structures transactions of buying and redeeming chips to stay below identification or mandatory reporting thresholds;

2.3.3.5 The customer carries out several transactions of buying and redeeming chips without making any bets;

2.3.3.6 The customer engages in gambling activity with a certain specific periodicity[89];

2.3.3.7 The customer buys a large amount of chips followed by insignificant gambling activity and trying to create the impression of active playing;

2.3.3.8 The customer carries out multiple redemptions of chips, which is not consistent with his limited gambling activity;

2.3.3.9 The customer almost always personally chooses at which table to play;

2.3.3.10 The customer constantly circulates funds between their gambling accounts serviced in the sport and casino sections, without any reasonable rationale;

2.3.3.11 The customer attempts to receive the certificate of winning on behalf of a third person;

---

[88] For example, loans, borrowings, accounts payable.

[89] For example, the customer that has been inactive for a long time, demonstrate significant activity for one day or several consecutive days, and then either stops placing bets or shows passive behavior and so on.

2.3.3.12 The customers acting in conspiracy with each other make contra bets and intentionally lose[90] to each other;

2.3.3.13 The customer exchanges small denomination banknotes to large denomination ones, certificates of winning, or checks;

2.3.3.14 The customer often switches the bank card used to fund/withdraw from the gambling account;

2.3.4. Suspicions with regard to NPOs

This section presents indicators of suspicious activity that are specific for the relationships with non-profit organizations, when they act as customers of financial institutions or DNFBPs.

2.4.1 The NPO is not appropriately monitored and controlled in the country of its registration;

2.4.2 The NPO has no employees or has a very small staff;

2.4.3 The NPO has no seat/offices and contact details[91];

2.4.4 The NPO's factual activities are inconsistent with its declared goals and objectives;

2.4.5 The NPO's financial flows are inconsistent with its factual activities;

2.4.6 The NPO's founders and/or executive management are from another country, and the organization's international operations are mainly associated with that country;

2.4.7 The NPO's founders and/or executive management regularly receive funds from the NPO in the form of payments that are not salaries;

2.4.8 Financial contributions provided to the NPO exceed declared incomes of the contributors or are inconsistent with their known economic activities, financial and social status;

2.4.9 The NPO makes expenditures, including for purchase of assets, that are inconsistent with its declared objectives;

2.4.10 The NPO's activities target beneficiaries or their groups that are in non-compliant countries;

2.4.11 The NPO uses the social networks to raise funds for donation and deactivates the relevant account after completion of the fundraising process;

2.4.12 The NPO has no documents regarding the internal procedures;

2.4.13 The NPO that carries out activities in the conflict zone transfers a large amount of funds to local companies whose activities are by no means related to the humanitarian services;

---

[90] For example, in a baccarat game, they simultaneously make bets on "red", "black" or "zero", or in a poker game, they deliberately lose their funds to the other customer.
[91] Including phone number, e-mail address.

2.4.14 An unusual increase is observed in the frequency and number of transactions made through the NPO's accounts.