

GUIDANCE

On criteria for the high risk and suspicion of terrorist financing and financing of the proliferation of weapons of mass destruction

Introduction

1. The criteria outlined in the Guidance on criteria for the high risk and suspicion of terrorist financing and financing of the proliferation of weapons of mass destruction (hereinafter referred to as the Guidance) should not be considered as separate from the "Guidance of Criteria of higher risk and indicators of suspiciousness in relation to Money Laundering and Terrorist Financing" (hereinafter referred to as the Guidance) in no way exclude each other and they serve as a supplementary indicative criteria.
2. For the purpose of assisting reporting entities in fulfilling their obligations in combating terrorist financing and the financing of the proliferation of weapons of mass destruction, the Financial Monitoring Center of the Central Bank of the Republic of Armenia, based on point 16 of part 1 of Article 10 of the Law "On combating money laundering and terrorism financing", has developed Criteria of higher risk and indicators of suspiciousness relation to terrorist financing and proliferation of weapons of mass destruction. The Guidance was developed on the basis of the FATF publications, and study of the international practice.

Part A: Criteria of higher risk and indicators of suspiciousness in relation to terrorism financing

1. Criteria of higher risk in relation to terrorism financing

1.1. Criteria related to jurisdiction^{1 2}

- 1.1.1. There is information from law enforcement agencies or credible media outlets suggesting that groups/ organizations committing terrorist offences are operating in the country;
- 1.1.2. There is information from law enforcement agencies or credible media outlets suggesting that funding or support is provided in the country for terrorist activities through government sources, organized groups or organizations;

¹ The term "country" is used equally and identically with the terms "territory" or "jurisdiction".

² In which the customer is resident, or with which the customer has business, financial or legal links, or from which funds are generated, or to which funds are sent to, or which is related to the transaction.

- 1.1.3 Mutual assessment reports or other credible sources identify strategic gaps in the implementation of FATF standards and relevant UN Security Council Resolutions, weak control of military goods in the country;
- 1.1.4 The country is an area of military or other armed conflicts, or is adjacent to such areas;
- 1.1.5 The country is subject to financial sanctions, embargoes or similar measures related to terrorism or its financing imposed by the UN or other international organizations.

1.2 Criteria related to customer³

- 1.2.1 The customer is a person included in the lists of individuals, groups and entities involved in terrorist acts and subject to restrictive measures for terrorism or its financing;
- 1.2.2 The customer has been convicted for terrorist activity or participation in terrorist groups/ organizations;
- 1.2.3 The customer is identified by law enforcement agencies or credible media outlets as being linked to terrorist activities or terrorist groups/ organizations;
- 1.2.4 The customer's online presence⁴ supports ideology related to terrorism, violent extremism or radicalization, which indicates the engagement or the intent to engage in terrorist, violent extremist activity;
- 1.2.5 The customer is involved in the provision of informal financial services⁵;
- 1.2.6 The customer is known to have close personal or professional links or is involved in transactions with the persons specified in the five points above.

2. Indicators of suspiciousness in relation to terrorism financing

2.1 Indicators related to customer

- 2.1.1 The customer uses accounts of intermediaries, trusts, family members or third parties with no plausible reason;
- 2.1.2 The customer provides vague or incomplete information about transactions with higher risk⁶ countries or territories;
- 2.1.3 The customer provides vague or incomplete information about transactions related to traveling arrangements;

³ All references to the customer apply to the beneficial owner, as well.

⁴ E.g. social media posts, tweets, hashtags, manifestos etc.

⁵ E.g. in the so-called "Hawala" transfers.

⁶ In this section, "higher risk" refers to the elevated risk of terrorism and terrorist financing.

- 2.1.4 The customer provides forged or falsified identification documents, fails to provide sufficient information for verification of his identity;
- 2.1.5 The customer carries out transactions apparently following the instructions of another person, in whose company he usually appears at the financial institution.

2.2 Indicators related to accounts

- 2.2.1 Several individuals with no apparent family/business relationships hold signature authority in one or several accounts;
- 2.2.2 The account is opened by an individual/entity with the same address or contact number as those of other individuals/entities with no apparent economic or other legitimate rationale;
- 2.2.3 The accounts of individuals/entities are used or controlled by persons in or from higher risk countries or territories;
- 2.2.4 Unusual facts are disclosed in the course of identification and verification of the potential customer, which are not reasonably explained by his person or by the available circumstances.

2.3 Indicators related to transfers

- 2.3.1 Transfers are made/ received to/from higher risk countries without any economic or other legitimate rationale;
- 2.3.2 Transfers are made to the same beneficiary account where the recipient is identified with different, sometimes similar names;
- 2.3.3 Transfers are generated by a business owned or controlled by persons in or from higher risk countries or territories;
- 2.3.4 Frequent private transfers are made through a business account with no apparent economic or other legitimate rationale;
- 2.3.5 Frequent transfers are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements;
- 2.3.6 Frequent transfers are made in small amounts to the same beneficiaries through money transfer systems⁷;
- 2.3.7 Currency exchange transactions are performed on behalf of a customer by a third party, followed by transfers to locations with no apparent business connection with the customer, or to higher risk countries or territories;

⁷ E.g. Western Union, MoneyGram

- 2.3.8 Multiple personal or business accounts are used to collect and funnel funds to a small number of foreign beneficiaries, both individuals and businesses, in or from higher risk countries or territories.

2.4 Indicators related to other features

- 2.4.1 Transaction details (contact name, email address, fund totals, remittance information, etc.) make references to words, phrases or numbers linked to terrorist/violent extremist actors, groups, activity, or iconography;
- 2.4.2 Money transfers, cheque deposits, online payments or cash deposits are made periodically, often in small amounts, with no apparent economic or other legitimate rationale⁸;
- 2.4.3 Crowdfunding issuer is reluctant to provide information about the crowdfunding offer;
- 2.4.4 Transactions are made with crowdfunding or crypto-asset exchange platforms, where transaction counterparties are persons associated with terrorism/violent extremism;
- 2.4.5 Payments are related to the acquisition of substances and materials that are not commensurate to, or in quantities that are unusual for, the person's known activities and can be used in the construction of explosive devices⁹;
- 2.4.6 Bank account activity is conducted remotely¹⁰ in or from higher risk countries or territories;
- 2.4.7 E-wallets or pre-paid cards are used at a location within or in close proximity of areas where terrorist groups are active or are known to enjoy support.

2.5 Indicators related to travelling arrangements

2.5.1 Pre-departure

- 2.5.1.1 The person indicates a planned cease date to account activity;
- 2.5.1.2 Actions of the person indicate total sale of personal possessions;
- 2.5.1.3 Airline ticket is purchased to a country in close proximity of a conflict zone;
- 2.5.1.4 Payments are related to travelling arrangements to/ from locations within or in close proximity of areas where terrorist groups are active or are known to enjoy support; payments are made for communication services provided in such areas;

⁸ E.g. the purpose is vaguely identified as "membership fee" and the like.

⁹ E.g. acquisition of aluminum pipes, fertilizers, metal scrap, etc.

¹⁰ E.g. through on-line banking, ATMs, debit/credit cards etc.

- 2.5.1.5 Funds from social assistance, student loans or other credit products (“debt financing”) are used for expenses related to travelling to a country in close proximity of a conflict zone;
- 2.5.1.6 Available credit products are used (often through cash advances, maxing out card limits) not for making normal recurrent payments but for transferring the balance to personal debit accounts;
- 2.5.1.7 Accounts are depleted through cash withdrawals within a short period of time;
- 2.5.1.8 Account activity shows a significant shift compared to historical activity on the account.

2.5.2 En-route

- 2.5.2.1 The customer notifies of travel to a third country via a location in close proximity of a conflict zone;
- 2.5.2.2 There is financial activity, such as debit or credit card usage, along a known travel route to a conflict zone or an area of concern;
- 2.5.2.3 The customer accesses or attempts to access his online or mobile banking application at a location within or in close proximity of a conflict zone;
- 2.5.2.4 The customer receives transfers from a location within or in close proximity of a conflict zone;
- 2.5.2.5 The customer purchases multiple prepaid SIM cards or prepaid data plans.

2.5.3 At the scene

- 2.5.3.1 The person receives money transfers from family or friends at a location within or in close proximity of a conflict zone;
- 2.5.3.2 Publicly available information and media indicates that the person has travelled to a conflict zone;
- 2.5.3.3 Customer accounts go dormant for a relatively long period of time.

2.5.4 Returning

- 2.5.4.1 The customer restarts activity on a dormant account;
- 2.5.4.2 The customer starts receiving income from new sources unrelated to regular employment;
- 2.5.4.3 The customer sends or receives atypical domestic or international transfers.

2.5.5 Disrupted travel

- 2.5.5.1 The customer makes travel-related purchases, such as airline tickets or visa, which are subsequently returned/ refunded;
- 2.5.5.2 The customer indicates that he would be travelling out of the country, but transaction history suggests the travel has not occurred;
- 2.5.5.3 Publicly available information indicates that the person has been banned to travel for security reasons.

2.6 Indicators related to non-profit organizations (hereinafter referred to as NPOs)

- 2.6.1 Donations are made to NPOs/ charities operating in locations within or in close proximity of areas where terrorist groups are active or are known to enjoy support;
- 2.6.2 The employee of the NPO withdraws cash from the NPO account and then deposits it into a personal account, then sends the funds to a third party's account;
- 2.6.3 A large international NPO based in a higher risk country or territory sends funds to its regional branch further channeled to local NPOs based or operating in conflict zones;
- 2.6.4 The NPO sends funds to multiple persons (individuals and companies) in a higher risk country or territory;
- 2.6.5 The NPO raises funds through a major public event and then authorizes a third party to be the signatory to the NPO account, who uses it to send the funds to a higher risk country or territory;
- 2.6.6 Unusual or atypical large cash withdrawals are made from the NPO account, particularly after the financial institution refuses the order on cross-border transfer of the NPO funds (thus raising cross-border cash smuggling suspicions);
- 2.6.7 Vague justifications and insufficient documentation is provided when the financial institution questions the NPO's order to transfer funds to higher risk countries or territories;
- 2.6.8 The NPO accounts are used to accept funds from subjects of requests from the financial intelligence unit or law enforcement agencies, who are suspected for links with terrorism/ violent extremism;
- 2.6.9 The NPO uses crowdfunding platforms and social media to solicit donations, then its online presence vanishes or shuts down;
- 2.6.10 The NPO's account demonstrates signs of unexplained increases in deposits and transactional activity;
- 2.6.11 The NPO is unable to account for the final use of all its funds/resources;

- 2.6.12 The NPO uses unnecessarily complex banking arrangements or financial networks for its operations, particularly for cross-border transactions;
- 2.6.13 The NPO or its representatives use falsified or contradictory documentation;
- 2.6.14 There is unusual absence of contributions from donors domiciled in or having nexus with the country of origin of the NPO;
- 2.6.15 The NPO appears to have few or no staff and limited or no physical presence, which is at odds with its declared purpose and scale of financial activity;
- 2.6.16 The NPO's funds are commingled with personal/private or business funds.

Part B: Criteria of higher risk and indicators of suspiciousness in relation to proliferation financing

3. Criteria of higher risk in relation to proliferation financing

3.1 Criteria related to jurisdiction

- 3.1.1 There is information from law enforcement agencies or credible media outlets suggesting that individuals or groups carry out proliferation activities in the country or territory;
- 3.1.2 Mutual assessment reports or other credible sources identify strategic gaps in the implementation of FATF standards and relevant UN Security Council Resolutions, weak control of proliferation-sensitive goods in the country or territory;
- 3.1.3 The country or territory is subject to financial sanctions, embargoes or similar measures related to proliferation or its financing imposed by the UN or other international organizations.

3.2 Criteria related to customer

- 3.2.1 The customer is involved in the purchase, supply, sale or delivery of proliferation-sensitive goods¹;
- 3.2.2 The customer is affiliated with a business, university or research institution involved in the production, trade, research development or similar activities concerning proliferation-sensitive goods;
- 3.2.3 The customer is identified by law enforcement agencies or credible media outlets as being linked to proliferation activities;
- 3.2.4 The customer is resident of, domiciled in or connected with² a country of proliferation concern;
- 3.2.5 The customer is known to have close personal or professional links or is involved in transactions with the persons specified in the five points above.

¹ E.g. weapons, equipment and technology for the production of weapons of mass destruction, dual-use goods, or other goods subject to export control.

² E.g., through business or trade relations.

4. Indicators of suspiciousness in relation to proliferation financing

4.1. Indicators related to customer

- 4.1.1 The potential customer provides vague or incomplete information about his anticipated trade activities;
- 4.1.2 The customer is vague, particularly about end-users of the traded goods, provides incomplete information or is reluctant to respond to questions seeking additional information;
- 4.1.3 The customer is engaged in complex trade deals involving numerous third-party intermediaries in lines of business that are inconsistent with its stated business profile established at onboarding;
- 4.1.4 The customer, who has declared a commercial business, conducts transactions suggesting that it is acting as a money remittance business or a pay-through account;
- 4.1.5 Counterparties of transactions appear to be entities possibly connected with a proliferation program (are linked to countries of proliferation concern);
- 4.1.6 Beneficiaries of transactions appear to be associated with manufacturers or shippers of goods subject to export controls;
- 4.1.7 Customer or end-user activity is inconsistent with their business profiles;
- 4.1.8 The customer or the counterparty, or their address or other descriptors, is the same or similar to one of the parties found on public sources with a history of export control contraventions;
- 4.1.9 Customers or counterparties to transactions are interconnected³.

4.2 Indicators related to transactions

- 4.2.1 The customer carries out transactions characterized by incoming or outgoing transfers from or to countries of proliferation concern, with rapid movement of large funds and a small end-of-day balance with no apparent economic or other legitimate rationale;
- 4.2.2 The transaction demonstrates a link between representatives of companies exchanging goods, such as same owners or management, in order to evade scrutiny of the composition and other characteristics of the goods exchanged;
- 4.2.3 The transaction involves goods that are inconsistent with trade profile of the involved country⁴;
- 4.2.4 The transaction involves goods that are incompatible with the technological development level of the destination country⁵;

³ E.g. they share a common physical address, IP address or telephone number, or their activities may be coordinated.

⁴ E.g. where the country involved does not normally export or import the types of goods concerned.

⁵ E.g. semiconductor manufacturing equipment being shipped to a country that has no electronics industry.

- 4.2.5 The order for goods is placed by individuals or companies from foreign countries other than the country of the stated end-use;
- 4.2.6 The transactions involve companies with opaque ownership structure, front or shell companies⁶;
- 4.2.7 The customer of a manufacturing or trading firm wants to use cash in transactions for industrial items or generally in trade transactions through sudden influxes of cash deposits to the firm's accounts followed by cash withdrawals;
- 4.2.8 The transactions are made on the basis of "ledger arrangements"⁷ that obviate the need for frequent cross-border wire transfers;
- 4.2.9 The account activity demonstrates circuitous route of financial transactions, or circuitous route of shipment (where data is available on the latter);
- 4.2.10 The trade finance transaction involves shipment routes (where data is available on the latter) through a country with weak export control laws or weak enforcement of such laws;
- 4.2.11 The transaction involves individuals or companies domiciled in countries with weak export control laws or weak enforcement of such laws;
- 4.2.12 The transactions include wire transfer or payment orders from or to parties not identified in the original letter of credit or other documentation.

4.3 Indicators related to other features

- 4.3.1 Based on the documentation obtained in the transaction, the declared value of the shipment is obviously underestimated vis-à-vis the shipping costs;
- 4.3.2 Lack of full information or data inconsistencies are identified in trade documents and financial flows, such as names, companies, addresses, final destinations, end-users, etc.
- 4.3.3 Fraudulent identities and documents are used, e.g. false sender/ receiver names, forged export or re-export certificates, etc.
- 4.3.4 Identifying documents or cargo documentation related to trade, especially within international trade, seem to contain inconsistencies or irregularities with no reasonable explanation;
- 4.3.5 Nonspecific, innocuous or misleading descriptions are provided on the customs declaration/export license⁸ without further explanation of the purpose or use of the respective goods;
- 4.3.6 A freight forwarding firm is listed as the final destination for the shipped goods;
- 4.3.7 There is no information about the person carrying out cargo transportation, as well as about the form and mode of cargo transportation;

⁶ E.g., entities with insufficient capitalization, little or no assets, no real place of business, etc.

⁷ "Ledger arrangements" are conducted by linked companies that maintain a record of transactions made on each other's behalf. These companies occasionally make transfers to balance the accounts.

⁸ E.g. agriculture, electronics etc.

- 4.3.8 Cargo transportation is carried out in a country that is not known for importing, exporting or marketing the given type of goods;
- 4.3.9 Cargo transportation directions, documents or other details are unexpectedly modified without any reasonable explanation;
- 4.3.10 Cargo transportation route fails to conform with the routes applicable in the business practice.

4.4. Indicators related to crypto-assets

- 4.4.1 The customer having crypto-asset accounts or wallets opens new crypto-asset accounts or wallets to conceal their relation with the sanctioned crypto-asset platforms;
- 4.4.2 Crypto-asset platforms of non-compliant countries are used to conduct large-scale transactions;
- 4.4.3 The salary of the customer is paid in virtual assets, where such practice is uncommon in the given employment field or region, or does not comply with the job description of the employee;
- 4.4.4 The customer describes their activities as self-employment in the IT sector, presenting the receipt of crypt-assets as receipt of salary;
- 4.4.5 Self-employed IT employee that receives salary in crypto-assets makes various transfers with the received salary, the economic purpose of which cannot be determined.

***(The Guidance was published on 3 February 2025.
The Guidance was edited on September 2025.)***