Terrorism Financing Red Flag Indicators

Terrorism Financing Red Flag Indicators

Practically speaking, it is difficult to provide a comprehensive and confirmed list of terrorism financing red flag indicators. Therefore, the reporting entities (financial institutions, Non-Financial Businesses and professions (NFBPs) and non-profit organizations), shall take into consideration the following general rules when referring to the Manual for Combating Terrorism Financing (Manual):

1. Upon applying these red flag indicators, the reporting entities must not refer to only one indicator to determine whether a transaction is suspicious or linked to a terrorist activity. The red flag indicators list is not exhaustive nor exclusive and should not be solely referred to in determining whether a suspicious activity is linked to terrorism financing.

2. Prior to determining whether an activity is linked to terrorism financing, the reporting entities shall consider additional factors, such as the overall financial activity of the customer and the existence of multiple apparent red flags.

3. The listed red flag indicators are general indicators that appear when transactions are reviewed, while other indicators are identified through analyzing and scrutinizing transactions.

4. Given the evolving nature of terrorism financing activities, the reporting entities shall make sure that data and information are reviewed accurately and correctly.

5. The reporting entities shall regularly look into available open sources to support terrorism financing indicators in terms of reporting suspicious transactions.

6. It is necessary to be aware of the sources providing information that identify high-risk jurisdictions in relation to terrorism financing, in order to include such jurisdictions in the suspicious transactions reporting.

Red flag indicators are generally classified in terms of their nature and category, as follows:

First Category (As per their Nature and Type)

1. Red Flag Indicators Related to Customer Identification Data:

- Customer avoids disclosing their residential address and the nature of their commercial and economic activity.
- Customers share the same address without justifiable grounds.
- Customers' phone numbers and addresses are frequently changed without justifiable grounds.
- Multiple accounts are linked to one phone number without justifiable grounds.
- Companies are established through falsified personal documents and engage in fund raising operations for terrorism financing purposes on behalf of these companies.
- Financial institutions are provided with customer names written in different forms and various residential addresses and phone numbers with the aim of deception.

2. Red Flag Indicators Related to Accounts.

- The account owner’s name is listed on terrorist lists.
- Accounts receive cash deposits or multiple transfers prior to being closed shortly after, or becoming dormant.
- A dormant account with a low balance suddenly receives a deposit(s) and is then subject to successive cash withdrawals until the account’s balance is withdrawn in full.
- An account is opened for a legal person, entity, or establishment engaged in activities carried out in favor of other entities or establishments involved or sympathizing with terrorism organizations.
- Transactions carried out in a customer’s accounts mostly involve amounts that are less than the regulatory threshold.

- An account is opened for a foreign person without clear grounds justifying their residence in the country.
- Bank accounts are managed by individuals whose names are similar to those listed in terrorist lists.

3. Red Flag Indicators Related to Cash Deposits.

- Cash deposits are made by persons who have no clear relation with the account's owners/ third parties.
- Small and repeated deposits are made by third parties into the accounts of high-risk non-Omani customers without clear justification.
- Cash deposits/cheques are deposited into salary accounts, where the amounts are not commensurate with the nature of the work of the account's owner.
- Cash deposits are made by multiple parties into an account followed by transfer(s) made to security/political conflict zones or neighboring zones.
- Cash deposits are made into the accounts through transfers made by local or foreign non-profit entities, especially if such entities are known to support terrorism.
- Cash deposits are made into the accounts and followed by ATM withdrawals in security/political conflict zones or neighboring zones.
- Cash deposits are followed by accessing the same account through online financial services in security/political conflict zones or neighboring zones.
- Frequent cash deposits through cross-border funds into accounts of persons from high-risk jurisdictions.

4. Red Flag Indicators Related to Transfers.

- Incoming or outgoing transfers are carried out from or to jurisdictions linked to terrorist activities or among the list of countries which are not implementing FATF recommendations.
- Transfers are received from countries with security and political instability and conflicts.

- Transfers received to individual accounts from unknown sources and without a known relation between the sender and receiver, whereby these transfers are described as “family assistance”.
- Transfers are received from other countries and followed by unjustified cash withdrawals that are not commensurate with the nature of the activity of the customer.
- Incoming transfers followed by transfer orders in favor of a third party/other parties.
- Transfers are made in favor of persons or entities adversely mentioned in the media for having extreme political stances and supporting certain conflict zones and entities as well as for supporting political and security instability.
- Transfers are made in favor of more than one beneficiary in more than one country, for family assistance purposes, where there is no clear relation between the transfer's senders and receivers.
- Transfers are recurrently sent to high-risk jurisdictions without a reasonable justification.
- Transfers are sent or received by individuals of various nationalities, residing in a high-risk country or in countries sharing borders with high-risk jurisdictions which have a terrorist organization(s), without clear justification.
- A person or more making frequent transfers to one person or more who are present in areas where there are terrorist organizations or in neighboring countries to those areas.
- A person writing their name in different forms upon transferring funds to make transfers appear as being sent by different persons.
- Funds are transferred through accounts of recently established companies to the accounts of companies that operate in the field of manufacturing chemicals that can be used to manufacture explosives.
- Funds are transferred from various accounts into one account, before they are withdrawn, upon accumulating them, either directly or through a single transfer.
- Funds are transferred through accounts of individual or entities designated on international lists, or which have been mentioned in the media as being linked to terrorist acts or terrorist organizations.

5. Red Flag Indicators Related to Credit and Payment Instruments:

- Payments are suddenly made for financial facilities or financing schemes obtained by the customer through a third party with the absence of a clear relation between them.
- Installments for facilities granted to the customers are not settled.

6. Red Flag Indicators Related to Bank Cards.

- A customer's ATM and credit cards are used by other parties with no clear justification.
- ATM and credit cards are used in high-risk jurisdictions or regions, particularly those known to have terrorist organizations.
- ATM and credit cards are used for carrying out frequent daily withdrawals of equal amounts from various locations that are far of the customers' place of residence or business without a clear justification.
- ATM and credit cards are used for purchasing chemicals used for manufacturing explosives.
- ATM and credit cards are used for purchasing flight tickets to countries where conflicts are taking place or to neighboring countries.
- Foreign ATM or credit cards are used in local ATMs to make frequent or large withdrawals.

7. Red Flag Indicators Related to Online Banking Channels.

- Using online banking channels to make recurrent outgoing transfers in favor of various persons without clear justifications.
- Accessing bank accounts via the Internet from regions neighboring or deemed to be a transit location to conflict zones, and making ATM cash withdrawals using the banks located in these zones.
- Accessing bank accounts via the Internet while in conflict zones and transferring funds to third parties that may use them to finance activities, facilitating terrorist fighters' movements, and purchasing flight tickets and other logistic facilities.
- Using various technologies to make transfers and change IP addresses to conceal the tracking facility.

8. Red Flag Indicators Related to Currency Exchange.

- Large sums of small denomination banknotes are exchanged with larger denomination banknotes and with the same currency.
- Currency exchange is followed by transfers made to high-risk jurisdictions.

9. Red Flag Indicators Related to the Transaction Purpose.

- Financial transactions are carried out for the purchase of camping and weapons equipment.
- Purchasing flight tickets and filing visa applications with the purpose of travelling to political or security conflict zones, regions with security or political instability, regions supporting terrorist organizations or terrorist acts, or travelling to countries adjacent to these zones and regions.
- Unusual purchases of chemicals that are used in explosives manufacturing with no commercial activity justifying the purchase of such materials.

10. Red Flag Indicators Related to Charitable Organizations and NPOs.

- Donations or transfers are received from foreign entities into the accounts of the charitable organizations and non-profit companies (NPCs) without a clear relation between them.
- Cash withdrawals or withdrawals against cheques are made in favor of persons who have no relation with the charitable organizations or NPCs.
- Large cash deposits are made into the accounts of charitable organizations, especially by non-related foreign entities, where such deposits are followed by outgoing transfers to high-risk countries.
- Transfers between individuals' personal accounts and charitable organizations' accounts without a clear justification.
- Large amounts are deposited and withdrawn from and into the accounts of charitable organizations and NPCs.

11. Red Flag Indicators Related to Donations.

- Donations are raised through a personal account, and the relationship between the nature of the account holder's activity and the depositors is not clear.
- Cash deposits and funds transfers are carried out under the umbrella of charitable donations and humanitarian assistance.
- Humanitarian assistance donations are collected in areas controlled by terrorist organizations through individuals and establishments believed to be fronts for such organizations, and using the accounts of such individuals and establishments for sending donations to high-risk jurisdictions.
- Sending transfers to persons in return for offering in-kind donations in favor of persons or entities located at a proximity to conflict zones.
- Change in terms of the activity nature of a person or an establishment by suddenly starting to raise funds for humanitarian purposes, given the fact that this change happens in a specific date coinciding with the rise and expansion of a terrorist organization.
- Transactions to charitable organizations abroad.
- Repeated transactions for donation purposes.

12. Red Flag Indicators Related to Customer Behavior.

- Customers declare to their financial institution that they intend to travel or have previously travelled to regions known as being conflict zones, regions suffering from security or political instability, or countries neighboring these high-risk areas.
- Individuals or companies supporting extremism and racism through their various activities and social media statements.
- Customers indicate their intention to suspend or close their financial accounts.
- Customers express their intention to engage in violent acts that may impact national security and public safety.

13. Other Red Flag Indicators.

- Customers making unusual cash withdrawals for the purpose of withdrawing funds with no method to track these funds.
- Sudden selling of personal properties without a clear justification.

- Reports issued by law enforcement authorities stating that the customer (natural / legal) is subject to investigation related to national security cases.
- Financial transactions which are related to customers connected with individuals or establishments about whom there is adverse information on the media or from security authorities accusing them of terrorism financing or being subject to investigations for court cases.
- Suspicious email messages are shared between a customer and a third party without a known relation between them in a suspicious way.
- Funds (Value) are moved through trade by purchasing goods in a country and selling them in another country.
- The name of a customer/beneficiary is identical with a name in terrorism designation lists.

Second Category (The most Important Red Flag Indicators)

General terrorist financing indicators include but are not limited to the following:

- Elements related to transactions involving high-risk countries, such as countries located in or close to armed conflict zones where terrorist organizations are active, or in areas lacking effective AML/CFT controls.
- Accounts opened in the name of an entity, establishment, or association affiliated to or related to a suspected terrorist organization.
- Transactions carried out in the name of an entity, establishment, or association affiliated to or related to a suspected terrorist organization.
- Transactions involving an NPO using funds in a way that is not in line with its objectives and roles.
- Transactions carried out by a customer who prefers secrecy, by avoiding providing or disclosing essential, required, or relevant documentation when carrying out such transactions.
- Transactions indicating a connection to informal fundraising without obtaining the relevant license or permit.
- Transactions related to a customer who, according to media reports, has travelled, attempted to travel, or decided to travel to a high-risk jurisdiction (including high-

risk regions and cities), namely countries (or neighboring countries) where a conflict is taking place, suffering from political instability, or known to support terrorists or terrorist organizations.

- Transactions related to an individual or entity which, according to media information or sanctions lists, is related to a terrorist organization or involved in terrorist activities.
- Transactions where the customer engages in purchases related to travelling (such as purchasing flight tickets, obtaining visas and passports, etc.) to high-risk jurisdictions (including high-risk regions and cities), namely countries (or neighboring countries) where a conflict is ongoing, suffering from political instability, or known to support terrorists or terrorist organizations.
- Information indicating an individual or entity's support of violent extremism or radicalism through their personal internet pages.
- Transactions involving customers donating funds in favor of a public case about which adverse information is published (such as crowdfunding initiatives, charitable organizations, NPOs, non-governmental organizations, etc.).
- The value of transactions is not consistent with the information available on the suspect, their activity, income, and lifestyle.
- Carrying out multiple transactions, whether locally or abroad, with persons or entities that are not clearly related to the suspect.

Third Category (The Nature of Transaction and Geographic Location)

1. Red Flag Indicators Related to Customers.

- Frequent change of persons authorized to use a specific account, including beneficiaries, and beneficial owners, etc.
- Ties with extremist persons, organizations or establishments.
- Information indicating the support of extremist publications or acts.
- Clear customer's behavior in abstaining from engaging in personal communication with the entity's employees (such as refusing to deal with women employees).
- Behavior reflecting clearly extremism or extremist concepts and ideologies.

- Submitting new or falsified identity documents (such as forged stamp, photo, or a photo displayed over a stamp, or having a date of issue that is not indicative of the document's typical level of wear and tear).
- New customers excessively asking the entity's employees about the requirements of disclosure, reporting or record keeping.
- New customers abstaining from providing information.
- Customers carrying out transactions on behalf of other persons.
- An account is opened in the name of a legal person having the same address of a natural person who is not linked to the account.
- Using a shared account by a large number of persons who are not personally or professionally related to each other or to the account owner.
- A natural person opening multiple accounts (bank accounts, credit cards, and e-wallets etc.), to receive small transfers.
- A natural person opening an account solely for the purpose of receiving transfers, then withdrawing them, or transferring them to other persons.
- Recurrent use of the same address, phone numbers, and references (such as job) for various accounts.
- Non-residents opening accounts shortly after their entry into the country.
- Opening accounts in areas that are different from their place of residence or work without justification.
- Customers unexpectedly liquidating their personal assets, such as pension accounts and personal properties.
- Information or indicators on relations with extremist persons, organizations, or establishments.
- Information or indicators on supporting extremist publications or acts.
- A group of beneficiaries using ATM cards where they are not apparently related to the account owner.
- A group of two or more individuals, who have no family relationship, gather around an ATM when entering a PIN code to withdraw money.
- Cash withdrawals by signatories.

2. Red Flag Indicators Related to Transactions

- Transactions related to humanitarian organizations that are not officially registered.
- A person carrying out multiple transactions through a single branch / office but through different employees.
- Extended use of joint accounts.
- Recurrent transfers by traders to foreign countries, where no business relationship is apparent with the destination country.
- Business accounts used for receiving or paying large sums, with the absence of usual transactions typical of business activities, such as salaries and bill payments, etc.
- Recurrent deposits of cheques or financial transactions in favor of third parties to their commercial or personal accounts.
- Indicators showing the customer's travel (or regular travel) to conflict zones or their surrounding areas while carrying money in cash.
- Transfers incoming in favor of beneficiaries hailing from countries linked to terrorist activities.
- Individual accounts receiving large transfers from unknown sources, where the declared purpose is livelihood support.

3. Red Flag Indicators Related to Geographic Location

- Frequent change of the address, phone number, account owners or authorized persons.
- A number of customers transfer funds to the same beneficiaries located in high-risk jurisdictions.
- One customer transferring funds to various beneficiaries located in high-risk jurisdictions.
- Frequently sending/receiving cross-border transfers of small amounts to/from unrelated persons.
- Paying additional sums in favor of the student in a foreign country by a family member or non-related organizations.
- Unemployed persons, who receive governmental remuneration, staying abroad for a long period of time.

- Indicators showing the customer's travel (or regular travel) to conflict zones or their surrounding areas while carrying money in cash.

The fourth category: Misuse of NPOs' Services

1. Main Red Flag Indicators

The following indicators reflect potential cases of terrorism financing or non-profit organizations' involvement in terrorism financing. Having an indicator or more of the following main red flag indicators raises the possibility of suspecting terrorism financing.

- The NPO's treasurer or employees withdrawing sums from the organization's account and depositing such amounts in a personal account, before transferring them to an account suspected of being linked to terrorism.
- The NPO has been known, through the media, to be linked to terrorist organizations or entities involved or suspected to be involved in terrorist activities.
- Parties of a transaction, such as the account owner, sender, beneficiary, or receiving party, are from jurisdictions known to support terrorist activities and organizations.
- Major NPOs sending funds to their regional branches, located in high-risk jurisdictions, then to local non-profit associations located or operating in local conflict zones.
- NPOs sending funds to various entities (individuals and companies) located in high-risk jurisdictions.
- NPO raising funds through large public events, then appointing a third party as an authorized signatory for its account to send funds to high-risk jurisdictions.
- Large and unusual cash withdrawals, especially following a financial institution's refusal to transfer the funds of the NPO abroad (thus raising doubt of cross-border money smuggling).
- Transactions, including local and international transfers, involving NPOs, featuring terminology linked to violent extremism and other terrorist ideologies,

such as “spoils” or “al-fay’” (justified stolen funds), “mujahid”, or “mujahidin” (members of “Jihad” movement).

- An NPO providing unclear justifications and refraining from submitting sufficient documentation when the financial institution requests information and details about transferring funds to high-risk locations or entities.
- Using the NPO’s accounts for receiving funds from suspected terrorists or their accomplices (based on information provided by law enforcement authorities on suspected persons).
- Parties involved in the transactions (cash transactions and transfers) are among the main employees of foreign NPOs and related to terrorist individuals and entities designated by the United Nations Security Council.

2. Secondary Suspicion Red Flag Indicators:

Secondary red flag indicators related to some terrorism financing cases involving NPOs are generally seen in illicit activities, such as fraud and money laundering. They may also be identified when a main indicator requires carrying out an in-depth analysis of the NPO’s behavior and upon applying customer due diligence or monitoring transactions.

Secondary red flag indicators support carrying out further research and examination to confirm initial suspicions and attempt to determine whether such indicators are related to terrorism financing or other offenses.

These indicators include the following:

- NPO transactions have no reasonable economic purpose. In other terms, the announced NPO activities and those of the other parties to the transactions are not related.
- The NPO uses crowdfunding and social media platforms for fundraising, before suspending its social media presence or activity.
- The NPO’s account indicates an extensive and unjustified deposit or transaction-related activity.
- The NPO is unable to explain the end-use of its funds/resources.

- The NPO resorts to complex banking arrangements or financial networks that are not necessary for its transactions, especially abroad.
- The NPO or its representatives use falsified or conflicting documentation.
- Contradiction between the pattern or volume of financial transactions, and the declared objective and activity of the NPO.
- Unexpected absence of contributions by donors inside the country.
- Large financial transfers to foreigners located in the country of the NPO's director, especially if the country is deemed as a high-risk jurisdiction.
- The NPO has little or no employees and limited or non-existent financial presence, in a way that is not consistent with its declared objective and financial activity.
- The NPO's funds are mixed with personal/private or commercial funds.

The fifth category: Exploiting Social Media Platforms for fundraising:

Global terrorism and its related threats are constantly evolving. Despite the differences between financial requirements of terrorist groups and individual terrorists, all terrorist categories seek to obtain sufficient income and manage their funds to finance their operations. The global AML/CFT network concluded that social media services can be misused for terrorism financing purposes through various means and methods, including the following:

- Using social media services and content hosting mainly for fundraising, encouraging terrorism through advertising campaigns, and spreading extremism.
- Crowdfunding services are used in many cases, where involved parties often conceal the main financing purpose under the pretext of using such funding for humanitarian causes.

The following offers effective indicators assisting in determining the entities or individuals involved or linked to terrorism financing through social media platforms:

- Using social media services to call for donations and support an organization involved in extremist activities related to terrorism.

- Using social media services to publish messages and pictures calling donors to make donations to support a known terrorist organization.
- Using social media services to contact potential donors and encourage them to make donations.
- Using social media services by charitable organizations to raise donations for humanitarian causes, whereas such funds are used for supporting foreign terrorist fighters.
- Charitable organizations related to terrorism using social media services to publish visual materials defending the legitimacy of their activities and for contacting donors.
- Using social media services by charity members to film their involvement with terrorists and terrorist organizations, including their training in the use of weapons.
- Using social media services for raising funds for a humanitarian cause, physically moving such funds across the borders and then dividing the overall amount between several travelers so that the values do not reach the minimum threshold for declaration.
- Using social media for announcing joining to a terrorist organization designated under the UN list, and posting relevant daily events.
- Using social media services for raising funds in favor of the families of individuals convicted with terrorism offenses.
- Using content hosting services for raising funds in favor of supporting terrorist groups, covering travel expenses for foreign terrorist fighters, and ensuring the livelihood of the terrorists' families.
- Publishing the bank account details of a person known to be located in a conflict zone, through social media and content hosting services, in order to raise funds to be allocated for covering travel expenses for foreign terrorist fighters, and ensuring the livelihood of the terrorists' families.
- Establishing contact between the content creator on content hosting and social media services and family members of persons linked to terrorist groups.
- Use of social media services, Internet communication services, and crowdfunding websites by NPOs for raising funds allegedly to be used for supporting terrorists, terrorist entities, and their activities.

- Using crowdfunding websites for raising funds in favor of terrorists and their families;
- Using crowdfunding websites offering options for making donations for relief in the event of conflicts in order to raise funds used by local residents for travelling to conflict zones.
- Using crowdfunding websites offering options for making donations in favor of countries where conflicts are taking place.
- Using Internet communication services for organizing withdrawals and deposits through the bank account of a terrorist's family member.
- Using Internet communication services for organizing banking transactions as well as transfers for financing a terrorist in return for a commission.
- Using Internet communication services for organizing funds transfers to regions located close to ISIS strongholds.
- Using Internet communication services for pledging loyalty for a group led by a designated terrorist.
- Using Internet communication services, pursuant to instructions given by a terrorist, for organizing and depositing donations into the bank account of one of the group's members.
- Using social media services and Internet communication services for various purposes that are different from the main declared purpose, mainly for promoting fundraising and contacting persons located in conflict zones;
- Making a public call for raising funds whereas the fundraising method remains confidential, by sending funds to a private account on social media or through phone calls.
- Most donations are directly collected by the requesting parties, whereas the remaining amounts would be secretly moved through banks, money exchange companies, and prepaid cards held by members (close or trusted members) of a terrorist group
- Using social media accounts featuring a large number of followers for raising funds and publishing the phone numbers and bank accounts of the persons responsible for raising such funds.