**Sultanate of Oman**


**National Centre for Financial Information (NCFI)**

# Manual
# for
# Combatting Terrorism Financing

# Table of Contents

## Firstly: Manual Objectives:

1. Explaining the concepts related to terrorism financing as set forth under the Law on Combating Money Laundering and Terrorism Financing (AML/CFT Law) as well as in the relevant international standards and recommendations.
2. Defining the role and competences of the National Center for Financial Information (NCFI).
3. Defining the reporting entities.
4. Terrorism financing stages.
5. Terrorism financing red flags.
6. Assisting financial institutions, designated non-financial businesses and professions (DNFBPs), non-profit associations and entities to detect and identify suspicion of terrorism financing offenses.
7. Raising efficiency and awareness among compliance officers at reporting entities, thus enabling them to efficiently undertake their role in reporting suspicious transactions linked to terrorism financing.
8. Rising awareness of reporting authorities and competent authorities about TF crime.
9. Issuing instructions for financial institutions to develop their systems for combatting terrorism financing through their electronic systems for detecting terrorism financing independently of money laundering.
10. Timing for filing suspicious transactions reports linked to terrorism financing to the NCFI.
11. Sanctions.

## Secondly: Terms and concepts

* **Law:** The Law on Combating Money Laundering and Terrorism Financing.

* **Center:** The National Center for Financial Information (NCFI).

* **Person:** A natural or legal person (legal person establishments and companies).

* **Terrorist Act:** Any of the following acts that a person or group of persons acting with a common purpose, perpetrates, attempts to perpetrate, participates to, organizes, plans, contributes to, or directs others to the perpetration thereof:

a. Any act that constitutes a crime in accordance with relevant agreements or treaties to which the Sultanate is a signatory.
b. Any act aimed at causing the death or serious bodily injury of a civilian or other persons not participating in hostile acts in case of an armed struggle, when the purpose of such act, by virtue of its nature or context, is to terrorize the population or compel a government or international organization to take or refrain from taking an action.
c. Any act considered as a terrorist act pursuant to the Counter-Terrorism Act, or any other law.

* **Terrorist:** Any natural person present inside or outside the Sultanate of Oman who commits, attempts to commit, participates to, organizes, plans, or contributes to the perpetration of a terrorist act or directs others to do so in any means whether directly or indirectly.

* **Terrorist Organization:** Any group of terrorists and any organization considered as terrorist organization pursuant to any other law.

* **Terrorism Financing Offence :** Any of the acts specified in Article 8 of the Law on Combating Money Laundering and Terrorism Financing, stipulating the following: "Any person who willingly collects or provides funds, directly or indirectly and by any means, with the knowledge that such funds will be used in full or in part, to carry out a terrorist act, or by a terrorist individual or a terrorist organization, shall be deemed to have committed the offense of terrorism financing. Such provisions include financing the travelling of individuals to a country other than their country of residence or nationality with the intent to perpetrate, plan, prepare for, participate to or facilitate terrorist acts, or provide necessary funds for training on terrorist acts or receiving such training.

* **Predicate Offense:** Any act constituting an offence under the laws of Oman, and acts committed outside Oman if they are considered a crime in accordance with the laws of the country in question and Omani laws.

* **Proceeds of Crime:** Any funds derived or obtained directly or indirectly from a predicate offence, including profits, economic benefits and advantages, and any similar funds converted fully or partially into other funds.

* **Financial Action Task Force (FATF):** An international body established in 1989 by the members-states' ministers, and which work aims at determining the principles and standards for protecting the global financial system against money laundering, terrorism financing, and WMD proliferation financing, whereby member-states are expected to meet the relevant obligations in this respect.

*** International Standards:**

- The FATF 40 recommendations for combatting money laundering, terrorism financing, and proliferation financing, as amended in February 2012 and issued by the FATF; and
- The 11 immediate outcomes on the efficiency of the AML/CFT systems issued by the FATF.

## FATF Recommendation (5): Terrorism Financing Offence

5-1 Countries should criminalize TF on the basis of the International Convention for the Suppression of the Financing of Terrorism[1].

5-2 TF offences should extend to any person who willfully provides or collects funds or other assets by any means, directly or indirectly, with the unlawful intention that they should be used, or in the knowledge that they are to be used, in full or in part: (a) to carry out a terrorist act(s); or (b) by a terrorist organization or by an individual terrorist (even in the absence of a link to a specific terrorist act or acts)[2].

**5-2 (bis)** TF offences should include financing the travel of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training.

5-3 TF offences should extend to any funds or other assets whether from a legitimate or illegitimate source.

5-4 TF offences should not require that the funds or other assets: (a) were actually used to carry out or attempt a terrorist act(s); or (b) be linked to a specific terrorist act(s).

5-5 It should be possible for the intent and knowledge required to prove the offence to be inferred from objective factual circumstances.

5-6 Proportionate and dissuasive criminal sanctions should apply to natural persons convicted of TF.

5-7 Criminal liability and sanctions, and, where that is not possible (due to fundamental principles of domestic law), civil or administrative liability and sanctions, should apply to legal persons. This should not preclude parallel criminal, civil or administrative proceedings with respect to legal persons in countries in which more than one form of liability is available. Such measures should be without prejudice to the criminal liability of natural persons. All sanctions should be proportionate and dissuasive.

[1] The criminalization should be consistent with Article 2 of International Convention for the Suppression of the Financing of Terrorism.

[2] It is insufficient to criminalize terrorism financing on the basis of assistance, incitement, attempt, or conspiracy only to adhere to this recommendation

5-8 It should also be an offence to:

a. attempt to commit the TF offence;
b. participate as an accomplice in a TF offence or attempted offence;
c. organize or direct others to commit a TF offence or attempted offence; and
d. contribute to the commission of one or more TF offence(s) or attempted offence(s), by a group of persons acting with a common purpose[3].

5-9 TF offences should be designated as ML predicate offences.

5-10 TF offences should apply, regardless of whether the person alleged to have committed the offence(s) is in the same country or a different country from the one in which the terrorist(s)/terrorist organization(s) is located or the terrorist act(s) occurred/will occur.

## FATF Recommendation (20): Reporting of Suspicious Transactions

20-1 If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to TF, it should be required to report promptly its suspicions to the Financial Intelligence Unit[4].

20-2 Financial institutions should be required to report all suspicious transactions, including attempted transactions, regardless of the amount of the transaction.

[3] Such contribution must be intentional and be made (i) with the aim of furthering the criminal activity or criminal purpose of the group, if such activity or purpose involves the commission of a terrorist financing offence, or (ii) be made with knowledge of the group's intent to commit a Terrorism financing crime.
[4] The FIU in the Sultanate of Oman is represented by the National Center for Financial Information.

## Thirdly: Establishment, mandate and powers of the NCFI.

### NCFI Establishment:

- The National Center for Financial Information (NCFI) was established in the Sultanate of Oman pursuant to the Law on Combating Money Laundering and Terrorism Financing, promulgated by Royal Decree No. (30/2016). Article (16) of Chapter Four of the Law stipulates the following: "A center under the name of National Center for Financial Information shall be established with the status of legal entity and administrative and financial autonomy under the Inspector General of the Police and Customs. The operating procedures of the Center shall be issued by a decision of the Inspector General upon approval of from the Cabinet."

### Mandate and Powers of the NCFI:
### Under the Law on Combating Money Laundering and Terrorist Financing, articles ( 18- 32)

- Pursuant to Article (18) of the Law, the Center shall have the mandate of receiving, analyzing and requesting reports and information, suspected of being related or linked to proceeds of crime, money laundering or terrorism financing activities. It shall also receive other information related to cash transactions, wire transfers, cross-border declarations and other threshold reports set by the supervisory authority.



- Pursuant to Article (19) of the Law, the Center may obtain any additional information and documents related to the reports and information it receives and other information it deems necessary to carry out its duties from reporting entities. Such entities shall provide the information at the time and in the form determined by the Center.

- Pursuant to Article (20) of the Law, governmental and non-governmental institutions in the Sultanate shall cooperate with the Center in carrying out its function, and provide it with information related to reports and information it receives from inside or outside, and that it deems necessary to carry out its duties without invoking confidentiality provisions.

- Pursuant to Article (21) of the Law, the Center shall provide reporting entities with the necessary guidance and instructions on how to report suspicious transactions, including the specifications of the report and reporting procedures.

- Pursuant to Article (22) of the Law, the Center should notify the competent supervisory agency in case reporting entities subject to its supervision fail to meet their obligations as stated in the Law for appropriate action.

- Pursuant to Article (23) of the Law, when there are sufficient grounds to suspect that funds are related to proceeds of a crime or suspected of being related or linked to money laundering or terrorism financing activities, the Center shall forward the information and analysis results to the public prosecutor or any other competent authority for appropriate action.

- The Center shall provide financial institutions, DNFBPs, non-profit associations and entities, and supervisory agencies with feedback regarding reports received by the Center, in accordance with rules and controls set by the Center. Pursuant to Article (24) of the Law, feedback means reporting on the use of provided information or result thereof, in order to enhance the effectiveness of implementing AML/CFT procedures.

- Pursuant to Article (25) of the Law, the Center may, in cases where it suspects that any of the crimes mentioned in the Law are being perpetrated, suspend the execution of a transaction for a period not to exceed 72 hours to proceed with the analysis procedures. If the Center concludes within this period, and based on the results of its analysis, that there are no sufficient grounds for suspicion, it shall issue an order to revoke the suspension of the transaction.

- Pursuant to Article (26) of the Law, the Public Prosecution may, upon request of the Center order the extension of the transaction suspension period for up to 10 days for further analysis, if there is evidence indicating that the transaction is in violation of the provisions of the Law. The Public Prosecution shall revoke the transaction suspension order if the grounds for suspicion were overturned.

- Pursuant to Article (27) of the Law, the Center may enter into memorandums of understanding and exchange information automatically or upon request with competent entities, while taking into consideration the necessary rules of confidentiality in this regard. The Center shall have the authority to make the final decision regarding providing the information to the requesting party or not.

- Pursuant to Article (28) of the Law, the Center may exchange information automatically or upon request with counterpart foreign centers or entities, while taking into consideration the necessary rules of confidentiality in this regard and without prejudice to the principle of reciprocity. The Center may also enter into memorandums of understanding or agreements with such centers or entities based on applicable procedures in the Sultanate.

- Pursuant to Article (32) of the Law, the Center shall prepare an annual report on its activities in the area of combating money laundering and terrorism financing, specifically including a general analysis of suspicious transaction reports it receives and activities and trends in money laundering and terrorism financing and submit it to the Chairman. A summary of such report shall also be prepared for publication.

## Fourthly: Regulatory and competent authorities

### 1. Regulatory Authorities:


### 2. Competent authorities:

Judicial and Security Authority and NCFI and other authorities concerned with combating money laundering and terrorism financing in the Sultanate.

## Fifthly: Reporting entities

### 1. Financial Institutions: **(Banks, Exchange Companies, Financing Companies, Securities, and Insurance Companies).**

Any person that engages, as a business, in one or more of the activities listed under Article (3) of the Law on Combating Money Laundering and Terrorism Financing for or on behalf of a customer, whereby the aforementioned Article stipulates the following:

**Financial institutions shall be subject to the provisions of the Law when carrying out any of the following functions:**

A- Receiving deposits and other payable funds from the public, including special banking services, lending, financial transactions including trading in securities, financing, financial leasing, services for transferring funds or value, buying, selling and exchanging currencies, issuing and managing payment instruments, guarantees, or obligations.

B-Trading, investing, operating, or managing funds, financial options or futures, exchange rate and interest rate operations, other financial derivatives, or negotiable instruments.

C-Participating in the issuing of securities and providing financial services related to such issues.

D-Managing funds and portfolios of various types.

E-Safeguarding funds.

F-Insurance activities, including insurance companies, brokers, and agents.

G-Any other activity or transaction specified by a resolution of the Committee.

## 2. Designated Non-Financial Businesses and Professions (DNFBPs): (Precious metals and Stones Traders, Lawyers, Notaries, Accountants, Legal auditors and CFSPs.

Any business listed under Article (4) of the Law on Combating Money Laundering and Terrorism Financing, including the following:

### a. Real Estate Brokers and Agents.

When carrying out transactions related to property sale and purchase in favor of customers.

### b. Dealers in Precious Metals and Stones.

When carrying out cash transactions equal to or greater than the threshold decided by the supervisory authority, whether the transaction occurs in a single phase or multiple linked phases.

### c. Attorneys, Notaries Public, Accountants/Auditors/Reviewers.

When they prepare or carry out transactions for or on behalf of their customers related to one of the following activities :

1. Purchase or sale of real estate;
2. Managing funds;
3. Managing bank accounts, savings accounts, or securities accounts;
4. Organizing participation in establishing, operating, or managing companies;
5. Creating, operating, or managing legal persons or arrangements and buying and selling of business entities.

### d. Trust and company service providers.

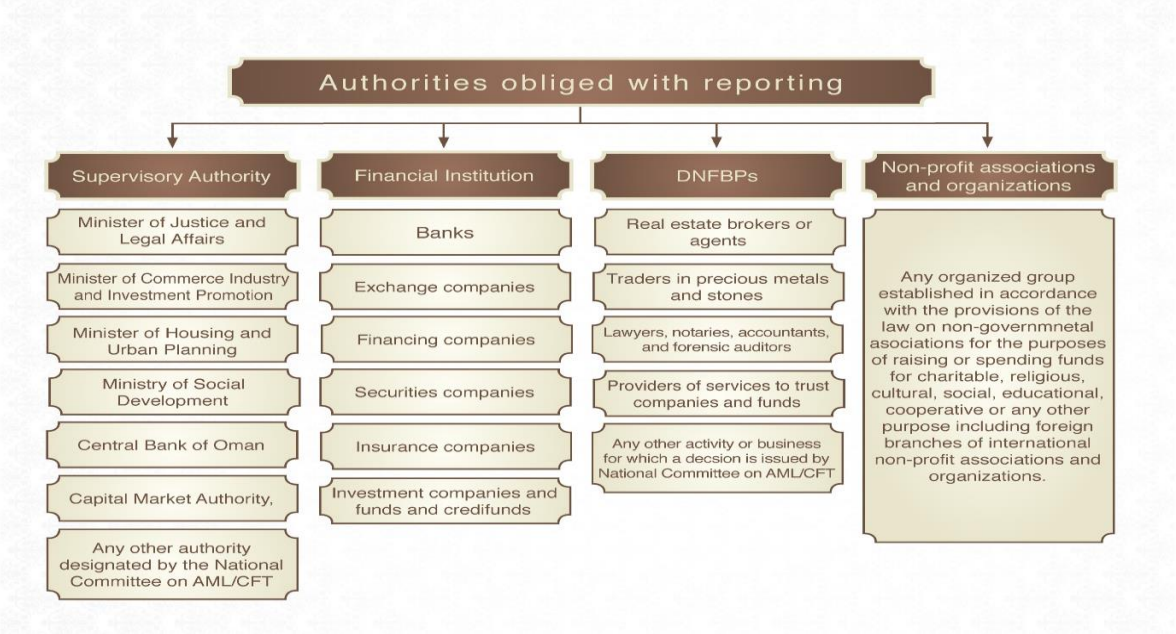
When they prepare or carry out transactions for or on behalf of customers related to one of the following activities :

1. Acting as a formation agent of legal persons;
2. Acting as a director or secretary of a company, a partner in a partnership, or a similar position in relation to other legal persons, or arranging for another person to act as such;
3. Providing a registered office, business address or accommodation, correspondence or administrative address for a legal person or arrangement;
4. Acting as or arranging for another person to act as a trustee of an express trust or performing the equivalent function for another form of legal arrangement;
5. Acting as or arranging for another person to act as a nominee shareholder for another person.

### e. Any other activity determined by a decision of the Committee.

### 3. Non-Profit Associations and Entities.

Any organized group established in accordance with the provisions of the Law on Civil Associations, for the purposes of raising or spending funds for charitable, religious, cultural, social, educational, cooperative, or any other purpose, including foreign branches of international non-profit associations and entities.




## Sixthly: Terrorism Financing Stages

### First Stage (Raising Funds)

- Raising funds for supporting and funding terrorist organizations for the purpose of carrying out terrorist acts depends on the size of terrorist organizations. In fact, simple (small) or individual terrorist organizations require the use of relatively small amounts in terms of terrorist acts. In other terms, the smaller the size of the terrorist organization or cell is, the more difficult it is to detect and track it by the supervisory systems applied by financial institutions and AML/CFT regulations. On the other hand, complex (large) terrorist cells require larger amounts and more efforts for raising funds for supporting their members and covering their operational expenses, such as travel, flight tickets purchase, training, livelihood, personal, medical, promotion, and recruitment expenses. Raising funds in favor of terrorist organizations is carried out through the following means:

#### a. Charities and Non-Profit Associations:

- Charities are among the entities that are abused by donors or terrorists for raising and laundering funds for terrorism-related purposes, namely since they are trusted by the public, have access to large sums of money, and are often located close to conflict zones where terrorist activities may take place. In fact, charities are usually established in conflict zones for humanitarian and relief purposes. Terrorists abuse charities and non-profit associations by using them as a safe cover for money transfers in high-risk zones and neighboring areas. Moreover, funds raised in other countries for humanitarian assistance may be mixed with funds raised for terrorism financing purposes.

### b. Financing from Legitimate Sources

- Terrorist organizations may establish legitimate investment projects as a business cover serving as a continuous source of income that is independent of the funds directly used for financing terrorist activities. The aforementioned raises an obstacle for financial institutions in terms of identifying daily and usual financial operations and those actually used for financing terrorist activities.

### c. Self-Funding

- This concept refers to cases where terrorist organizations rely on themselves to meet their needs in terms of financing, weapons, and equipment to perpetrate terrorist acts or recruit foreign terrorist fighters. Such sources of funds include the following:
- Salaries.
- Sale of personal property.
- Small short-term loans, thus making them hard to detect.
- Family assistance for members of terrorist organizations.
- Support by other terrorist organizations, where older terrorist organizations may offer assistance, including money, weapons, training, and a safe haven for newer terrorist organizations.
- Exploiting small economic projects.

### d. Proceeds of Predicate Offenses

- Proceeds of predicate offenses, including fraud, theft, drug trafficking, currency and cheques counterfeiting, human trafficking, kidnapping, illegal arms trafficking, and child sexual exploitation, among others, are deemed a considerate and fast source for financing terrorist activities, which is why terrorists attempt to conceal the proceeds of such offenses through resorting to methods and means that are similar to those applied in money laundering.

### e. Other Sources for Raising Funds

- Bank robberies.
- Theft, smuggling, and selling of antiquities in global markets.
- Smuggling oil and its derivatives.
- Smuggling machines and equipment.
- Imposing taxes and fees.
- Imposing royalties on local residents.

## Second Stage (Moving Funds)

- Various channels are targeted by terrorists for moving their funds. These channels include:

### a. Banks:

- Terrorism financing through the banking sector is limited. In fact, it is difficult to identify financial transactions related to terrorism financing since normal financial flows go through accounts on a daily basis, and since some terrorist acts require small sums only. It is possible to use the banking sector for moving funds used for terrorism financing purposes through the following means:
- Cash deposits.
- Bank transfers.
- Using credit cards, ATM cards, and prepaid cards.
- Using electronic banking channels.

### b. Currency Exchange Companies and Remittance Companies.

- Currency exchange and remittance companies are among the major channels targeted by terrorists to move their funds from a country to another or within the same country since their characteristics may be abused by terrorists including:
- Low transfer cost.
- Multiple systems used for transferring funds.
- Possibility of transferring funds to high-risk jurisdictions or to regions where no effective AML/CFT controls are applied, contrary to banking systems. This offers terrorists an opportunity to finance their activities without proper tracking.
- Remittances are often transferred for "family assistance" purposes, where the company is not aware of the relation between the involved parties. As such, terrorists conceal the actual purpose of their transfer. The risk lies in the fact that such funds may be used for terrorism financing purposes.

### c. E-Payment Systems.

- E-payment systems are among modern technologies that may be used for fund transfers and for terrorism financing as well, namely since they are accessible from anywhere in the world to easily and rapidly transfer funds. Moreover, the non-face-to-face nature of such e-payment systems offers a suitable cover for terrorists and terrorist organizations to hide their identities.
- E-payment systems that are not subject to effective supervisory controls may be easily hacked by terrorists, among others, especially those used in regions and jurisdictions where effective AML/CFT controls are not applied.
- The possibility of terrorists resorting to virtual currency (Bitcoins) was recently seen, since such transfers may be carried out in electronic black markets where suspicious transactions may be processed using digital currencies.

### d. Cross-Border Transfer of Funds.

- Cross-border transfer of funds is one of the most dangerous methods used by terrorists for the purpose of international terrorism financing. In fact, borders between countries form a channel targeted by terrorists to move funds into conflict zones or neighboring countries to provide all forms of support in favor of terrorists organizations in these zones, where such funds would be used for recruiting foreign terrorist fighters, training and arming terrorists, and funding terrorists acts. Cross-border funds transfer may take various forms, including:

- Physical movement of funds with a natural person or through their luggage or vehicle.
- Shipping currencies or bearer negotiable instruments through containers.
- Sending currencies or bearer negotiable instruments by post through a natural or legal person.
- Moving funds through informal border crossings.

## Third Stage (Using Funds).

- Funds raised by terrorists for financing their various activities are used for:

- Purchasing weapons, equipment, and ammunition;
- Purchasing chemicals used for manufacturing explosives, such as nitrate and acetone, among others;
- Training terrorist fighters for carrying out terrorist acts;
- Promoting and recruiting, either directly or through using social media platforms or other media;
- Financing the livelihood of terrorists (housing, food, and transportation, among others);
- Purchasing flight tickets, credit cards, and prepaid cards; and
- Searching for a safe haven.

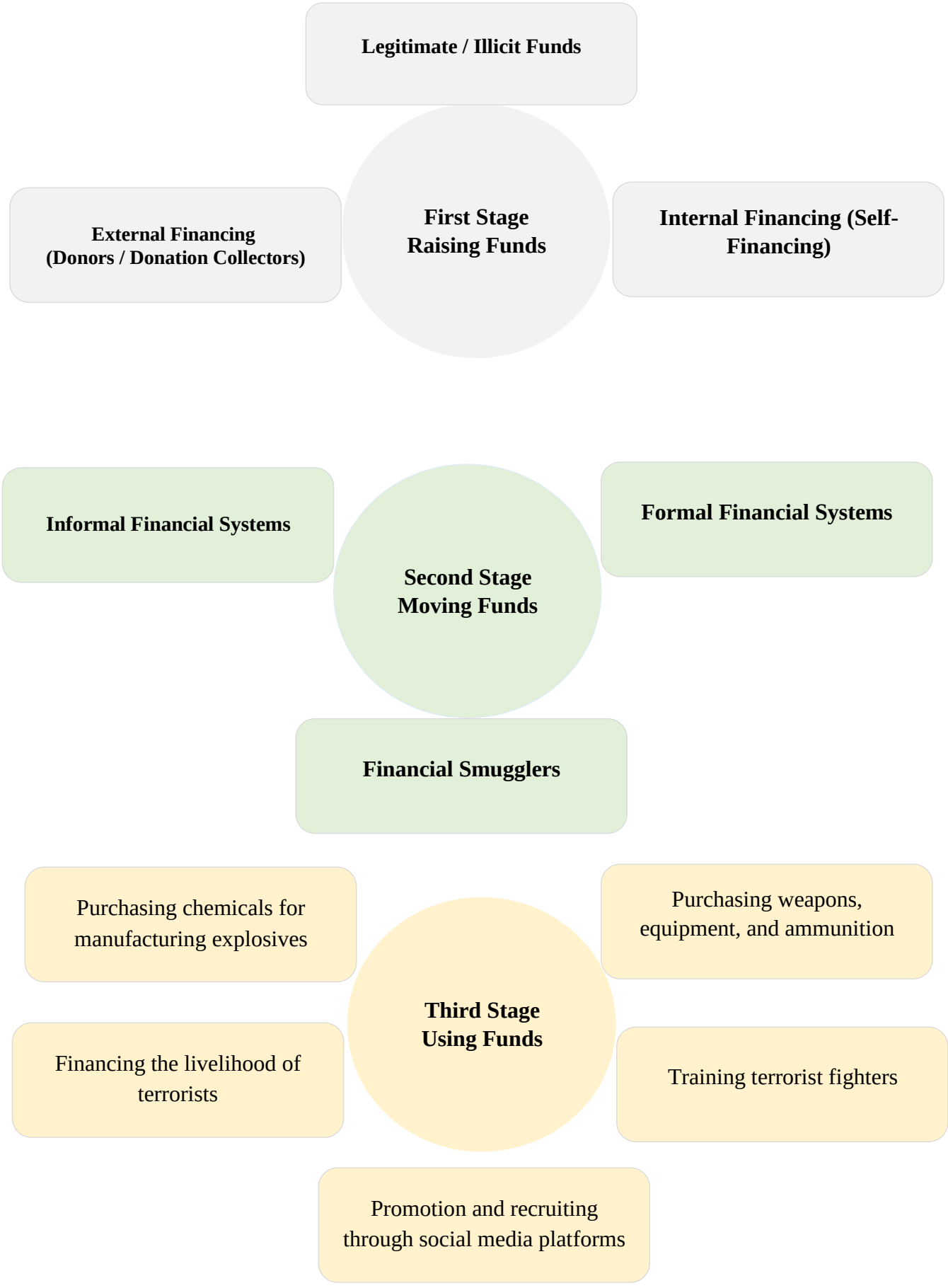
### Terrorism Financing Risks.

- Although there are multiple negative economic, political, and social impacts arising from money laundering and terrorism financing, it is worth noting that terrorism financing offenses, given their nature and motive, often have the biggest impact at the political level. Such impacts include:

- Financing terrorist organizations disturbs the country's stability and security.
- Member of terrorist organizations may reach high-level political positions.
- The political system may be undermined in the interest of terrorist groups.

- Terrorism financing also holds negative impacts on the banking sector in the Sultanate of Oman. The sector could become subject to fines and financial sanctions as a result of being abused for terrorism financing purposes and violating United Nations Security Council Resolutions. The aforementioned would impact the overall assessment of the financial sector in Oman, which could, in turn, negatively impact the international AML/CFT/CPF mutual evaluation of Oman.

## Terrorism Financing Mechanism and Stages



## Similarities and Differences between Money Laundering and Terrorism Financing

- Both offenses are similar in terms of the following:
  - Both involve hiding, deceit, and concealment.
  - Both require international strategic cooperation given their cross-border nature.
  - Both require supervisory measures and financial investigation procedures.
- The table below displays the differences between both offenses. Such differences may assist at drawing the distinction between money laundering and terrorism financing suspicions, especially since both offences share common red flags.

| Difference | Money Laundering | Terrorism Financing |
|---|---|---|
| Source of Funds | Legitimate | Legitimate / Illicit |
| Volume of Funds | Large amounts | Small / Limited amounts |
| Purpose | Profitability / Financial | Political / Ideological |
| Funds Movement Cycle | Circular<br>(Begins and ends with the laundering party) | Linear<br>(Begins with the financier and ends with the terrorist organization) |
| Use of Financial Institutions | Funds are mostly moved through financial institutions | Funds are not mostly moved through financial institutions |
| Channels | Formal financial systems | Financial smugglers or informal financial systems |
| Detection Sphere | Identification of the relationship between the involved persons | Funds movement |

## Seventhly: Terrorism Financing

### Red Flags

- Although the National Center for Financial Information may theoretically provide a comprehensive overview of these red flags, it is practically difficult to provide a confirmed and exhaustive list of such. Therefore, the reporting entities (financial institutions, DNFBPs and non-profit organizations, when referring to this Manual, financial institutions shall take the general rules below into consideration:

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

2. Prior to determining whether an activity is linked to terrorism financing, the reporting entites 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 flags are general indicators that appear when transactions are reviewed, while other indicators are identified through analyzing transactions.

4. Given the complex aspect of terrorism financing activities, the reporting entites, shall verify that data and information sources are accurate and correct.

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

6. It is necessary to refer to sources available for determining high-risk jurisdictions within the field of terrorism financing, to include such jurisdictions in terms of reporting suspicious transactions.

- **Red flags are generally classified in terms of their nature and category, as follows:**

- **First Category (As per their Nature and Type)**

### 1. 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.
- Their phone number and address is frequently changed without justifiable grounds.
- More than one account is 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 misleading them.

### 2. Indicators related to accounts.

1. The account owner's name is listed on terrorist lists.
2. Accounts receive cash deposits or multiple transfers prior to being closed shortly after, or becoming dormant.
3. 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.
4. 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.
5. Transactions carried out in terms of the customer's accounts involve amounts that are less than the regulatory threshold.
6. An account is opened for a foreign person without clear grounds justifying their residence in the country.
7. Bank accounts are managed by individuals whose names are similar to those listed under terrorist lists.
8. Frequent cash credits through cross-border funds into accounts of persons from high-risk countries.

### 3. Indicators related to cash deposits.

1. Cash deposits are made by persons who have no clear relation with the account's owners.
2. Small deposits are frequently made by third parties into the accounts of high-risk non-Omani customers without clear justification.
3. Cash deposits/cheques are deposited into salary accounts, where the amounts are not reflective of the business nature of the account owner.
4. Cash deposits are made into the account by many parties. Such deposits are followed by transfer(s) made to security/political conflict zones or neighboring zones.
5. Cash deposits are made into the accounts through transfers made by local or foreign non-profit entities, especially if known to support terrorism.
6. Cash deposits are made into the accounts and followed by ATM withdrawals in security/political conflict zones or neighboring zones.
7. Cash deposits are followed by accessing the same account through online financial services in security/political conflict zones or neighboring zones.

### 4. Indicators related to transfers.

- Incoming or outgoing transfers are carried out from or to jurisdictions linked to terrorist activities or countries listed as not applying 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 clear relation with the sender, whereby these transfers are described as "family assistance".
- Transfers are received from other countries and followed with unjustified cash withdrawals that are not reflective of the business nature of the customer.
- Incoming transfers are followed with transfer orders in favor of a third party/other parties.
- Transfers are made in favor of persons or entities adversely mentioned in the media, where their extreme political ideology and support for some conflict zones and entities as well as for political and security instability were highlighted.
- Transfers are made in favor of more than one beneficiary in more than one country, for "family assistance" purposes, upon lacking a clear relation between the transfer's sender and beneficiary.
- 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 bordering high-risk jurisdictions where terrorist activity exist, without clear justifying grounds.
- A person or more making frequent transfers to one person or more present in areas where there are terrorist organizations or in neighboring countries.
- 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 the accounts of recently established companies to the accounts of companies manufacturing chemicals that may be used to produce 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 individual accounts, entities designated on international lists, or entities mentioned in the media as being involved in terrorist acts or linked to terrorist organizations.

### 5. 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 in the absence of a clear relation between them.
- Installments for facilities granted to the customers are not settled.

### 6. Indicators related to bank cards.

- The customer's ATM and credit cards are used by other parties in the absence of a clear justification.
- ATM and credit cards are used in high-risk jurisdictions or regions, namely 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 neighboring countries.
- ATM and cards are used for frequent or high withdrawals from external cards through local cards.

## 7. Indicators related to Online Banking Channels:

- Using online banking channels for making recurrent transfers in favor of various persons without clear justifications.
- Accessing bank accounts online from regions neighboring or deemed to be a transit location to conflict zones, and making (ATM) cash withdrawals through resorting to banks located in such zones.
- Accessing bank accounts online while in conflict zones and transferring funds to third parties that may use them for financing activities, facilitating terrorist fighters' movements, and purchasing flight tickets and other logistic equipment.
- Using various technologies for making transfers and changing IP addresses to conceal tracking elements.

## 8. Indicators related to currency exchange.

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

## 9. Indicators related to the transaction purpose.

- Financial transactions are carried out for purchasing camping and weapons equipment.
- Purchasing flight tickets and filing visa applications for travelling into political or security conflict zones, regions with security or political instability, regions supporting terrorist organizations or where terrorist acts take place, or neighboring countries.
- Unusual purchases of chemicals used for manufacturing explosives are carried out in the absence of a commercial activity justifying the purchase of such materials.

## 10. Indicators related to Charities and Non-Profit Associations.

- Donations or transfers are received from foreign entities into the accounts of charities and non-profit associations without a clear relation between both parties.
- Cash withdrawals or withdrawals against cheques are made in favor of persons who are not related to charities and non-profit associations.
- Large cash deposits are made into the accounts of charities, especially by non-related foreign entities, where these deposits are followed by outgoing transfers made to high-risk jurisdictions.
- Transfers made between the accounts of individuals and those of charities without a clear justification.
- Large amounts are deposited and withdrawn from the accounts of charities and non-profit associations.

## 11. Indicators related to donations.

- Donations are raised through a personal account, and the link between the business nature of the account holder and the depositors is not clear.
- Cash deposits and funds transfers are carried out under the description 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 business nature of a person or an establishment by suddenly raising funds for humanitarian purposes, while noting that this change is connected to a specific date, being the rise and expansion of a terrorist organization.

## 12. 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 support 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 on national security and public safety.

## 13. Other Indicators.

- Customers making unusual cash withdrawals to withdraw their funds without providing means to track such funds.
- Suddenly selling 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.
- Financial transactions are carried out by customers connected to individuals or establishments in relation to whom there is adverse media or information accusing them of terrorism financing or being subject to investigation in cases at the level of the State Security Court.
- Suspicious email messages are shared between the customer and a third party without a relation between them.
- Funds (Value) are moved through trade by purchasing goods in a country and selling them in another.

- **Second Category (The most Important Indicators)**

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

- Elements related to transactions involving high-risk jurisdictions, 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 suspect terrorist organization.
- Transactions carried out in the name of an entity, establishment, or association affiliated to or related to a suspect terrorist organization.
- Transactions involving a non-profit association using funds in a way that is not in line with its establishment objective.
- Transactions carried out by a customer who prefers secrecy, by avoiding providing or disclosing essential, required, or relevant documentation upon 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 shown to be related to a terrorist organization or involved in terrorist activities as per the media or sanctions lists.
- Transactions where the customer engages in purchases related to travelling (such as purchasing flight tickets, obtaining visas and passports, among others) 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 pages.
- Transactions involving customers donating funds in favor of a public case on which adverse information is published (such as crowdfunding initiatives, charities, non-profit associations, non-governmental organizations, etc.).
- The value of transactions is not aligned with the information available on the suspect, their activity, income, and lifestyle.
- Carrying out multiple transactions with persons or entities that are not clearly related to the suspect, whether locally or abroad.

- **Third Category (Transaction Type and Geographic Location)**

  - Indicators related to customers

- Frequent change of persons authorized to use a specific account, including beneficiaries, and beneficial owners, among others.
- 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 engage with women employees).
- Behavior reflecting 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 using an issue date that does not reflect the document status, whereby the document could be torn, for instance).
- New customers excessively asking the entity's employees about disclosure and reporting requirements or record keeping requirements.
- New customers abstaining from providing information.
- Customers carrying out transactions on behalf of other persons.
- Account 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 the account owner.
- A natural person opening multiple accounts (bank accounts, credit cards, and e-wallets), to receive small transfers.
- A natural person opening an account solely for the purpose of transferring or receiving transfers, 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 after a short period of their entry into the country.
- Opening accounts in areas that are different from the 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 withdrawal cards where they are not apparently related to the account owner.
- A group of two or more unrelated persons meeting when using a pin code and withdrawing sums from ATMs.
- Cash withdrawals from signatories .

## 2. Indicators related to transactions

- Transactions related to humanitarian organizations that are not duly registered.
- A person carrying out multiple transactions through one branch / office and various employees.
- Extended use of joint accounts.
- Recurrent transfers by traders to foreign countries, where no business relationship is apparent in the destination country.
- Business accounts used for receiving or paying large sums, in the absence of usual transactions aligned with business activities, such as salaries and bill payments, among others.
- 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 surrounding areas while carrying money.
- Transfers incoming in favor of beneficiaries of countries linked to terrorist activities.
- Individual accounts receiving large transfers from unknown sources, where the declared purpose is livelihood support.

## 3. 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 requesting party in a foreign country by a family member or non-related organizations.
- Unemployed persons receiving governmental subsistence staying abroad for a long period.
- Indicators showing the customer's travel (or regular travel) to conflict zones or surrounding areas while carrying money.

## The fourth category: Misuse of Non-Profit Associations

### 1. Main Red Flags

The following red flags indicate potential cases of terrorism financing or non-profit organizations' involvement in terrorism financing. Meeting an indicator or more of these main indicators raises the possibility of suspecting terrorism financing.

- The NPO's treasurer or employees withdrawing sums from the association's account and depositing such amounts in their personal account, before transferring them to an account suspected to 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 to 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 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 upon the financial institution's refusal to transfer the funds of the NPO abroad (thus raising doubt around 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).
- Providing unclear justifications and refraining from submitting sufficient documentation upon the request of the financial institution to the NPO regarding information and details on transferring funds to high-risk locations or entities.
- Using the NPO's accounts for receiving funds from suspected terrorists or accomplices (in accordance with 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 entities designated by the United Nations Security Council.

## 2. Secondary Suspicion Red Flags:

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

Secondary red flags support carrying out further research and inquiries to establish preliminary doubts and attempt to determine whether such indicators relate to terrorism financing or another offenses.

- **These red flags 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 the existence of 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 in 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 to no employees and limited or non-existent financial presence, in a way that is not in line with its declared objective and financial activity.
- The NPO's funds are mixed with personal, private, or commercial funds.

### The fifth category: Social Media Platforms Abuse:

- Global terrorism and its related threats are constantly evolving. Despite the various financial requirements of terrorist groups and individuals, 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 are often misused for terrorism financing purposes through various means and methods, including the following:
- Social media services and content hosting are mainly used 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 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 upon donors to make donations to support a known terrorist organization.
- Using social media services to contact potential donors and invite them to make donations.
- Using social media services by charities to raise donations for humanitarian causes, whereas such funds are used for supporting foreign terrorist fighters.
- Using social media services by charities related to terrorism for publishing visual support material 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 weapons training.
- Using social media services for raising funds in favor of a humanitarian cause and physically moving such funds across the borders upon dividing the overall amount among several travelers, so as not to exceed the threshold for declaration.
- Using social media for announcing enrollment with a terrorist organization designated under the UN list, and posting relevant events daily.
- Using social media services for raising funds in favor of the family members of persons 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, for raising funds to be allocated for covering travel expenses for foreign terrorist fighters, and ensuring the livelihood of the terrorists' families.

- Establishing contact with 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 the instructions made by a terrorist, for organizing and depositing donations into the bank account of one of the group members.
- Using social media services and Internet communication services for various purposes that are different from the main announced 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, as it was sent to a private account available via social media services or made through phone calls.
- Most donations are directly collected by the requesting parties, whereas the remaining amounts would be secretly moved through banks, exchange houses, and prepaid cards held by members of a terrorist group (close or trusted members).
- Using social media accounts featuring a large number of followers for raising funds and publishing the phone number of the persons responsible for raising such funds.

## Eighthly: Resolution No. (3/2022) of the National Committee for Combatting Money Laundering and Terrorism Financing on Identifying High-Risk Countries.

Based on Article (13) paragraph (k) of the AML/CFT Law issued by Royal Decree No. (30/2016), on the competence of the National AML/CFT Committee to identify high ML/TF risk countries,

And based on the decision of the National Committee at its 2020 meeting to adopt the FATF list of high-risk countries, and to ensure public interest,

**It was decided:**

**Article (1)** : Each country listed in the FATF general statement shall be considered a high ML/TF risk country.

**Article (2)** : FIs, DNFBPs, and NPOs shall implement the attached EDD measures on high-risk countries, attached under Annex (1), and shall apply due diligence measures on countries under increased monitoring, as listed in Annex (2).

**Article (3)** : Supervisory authorities shall verify that FIs, DNFBPs, and NPOs under their supervision are implementing EDD measures towards high-risk countries.

**Article (4) :** This Resolution shall enter into force as of its date of issue. Parties concerned shall implement this decision, each within their field of competence.

## Due Diligence Measures for High-Risk Jurisdictions

**1.All FIs, DNFBPs, and NPOs must abide by the following:**

- Apply EDD measures on all business relationships and transactions with persons from designated high-risk countries, including natural and legal persons, financial institutions, and those acting on their behalf;
- Comply with internal reporting mechanisms related to monitoring transactions and activities associated with high-risk countries and submit STRs to the NCFI, as required;
- Refrain from relying on third parties located in designated high-risk countries when applying due diligence measures; and
- Impose targeted financial sanctions pursuant to the relevant UNSC resolutions.

**2. Supervisory authorities on financial institutions must abide by the following:**

- Prohibit or impose additional procedures and assess risks before authorizing the establishment of any branches, subsidiaries, or representative offices of financial institutions in designated high-risk countries.
- Pursuant to the situation and the relevant country, impose further monitoring and supervision procedures on the branches, subsidiaries, and representative offices in cases where establishing such entities is authorized pursuant to Paragraph (a) above.
- Applying enhanced external auditing requirements for branches or subsidiaries of Omani financial institutions in high-risk countries.
- Following up on the compliance of all institutions under their supervision, including FIs, DNFBPs, and NPOs, in term of applying compliance requirements related to targeted financial sanctions in accordance with the UNSC resolutions.
- Applying measures or penalties set forth under Article (52) of the AML/CFT Law, issued by Royal Decree No. (30/2016), against FIs, DNFBPs, and NPOs, including their directors and senior management, in the event of their failure to implement the measures stipulated under this Resolution and its annexes.

## Due Diligence Measures for Countries under Increased Monitoring.

- All FIs, DNFBPs, and NPOs should regularly review the list of jurisdictions under increased monitoring (high risk countries jursdictions) and their identified vulnerabilities and take them into account when developing and implementing risk-based compliance measures.
- Due diligence measures taken by FIs, DNFBPs, and NPOs must be proportionate to the risks arising from business relationships and transactions with natural or legal persons of such jurisdictions in all cases. They should be sufficiently efficient to mitigate such risks. Measures taken may require implementing EDD measures.

## Ninthly: NCFI Electronic Reporting System

- The Center has developed high-quality integrated systems and programs in line with international standards and requirements enabling it to professionally carry out its mandate, including the Electronic Reporting System.
- This system makes it easier for compliance officers of reporting entities to submit all types of suspicious transaction reports, such as bank transactions, threshold transactions, transfers and currency exchange, guarantees, bonds and securities, sales and purchases of precious metals and stones, among other non-financial businesses and professions, pursuant to Article (4) of the Law, and in accordance with the reporting entity type. The window for reporting allows for the entry of data aligned with the work nature of each reporting entity separately. The system window offers the following:
  - Guaranteeing information security and communication through using a secure electronic window rather than resorting to the manual delivery of suspicious transaction-related information and data on paper, whereby this process is slow and dangerous in terms of security, as these paper documents may be lost or damaged, or even subject to access by unauthorized persons;
  - Possibility of sending all suspicious transactions data of all types electronically by the reporting entities registered with the National Center for Financial Information;
  - Offering a feature for establishing electronic communication between the relevant Center employees and compliance officers, through the system window, whereby such communication would be related to the transactions sent by the reporting entities, or the requests or inquiries made by the Center; and
  - Providing statistical reports on the reporting entity's performance and number of transactions sent by each entity separately.

### Suspicious Transactions Reports

- **When should suspicious transactions be reported?**

  In accordance with Article (47) of the Law on Combating Money Laundering and Terrorism Financing:

  "As an exception to the provisions on the confidentiality of banking transactions and professional and contractual secrecy, financial institutions, non-financial businesses and professions, NPOs, their managers, members of the board of directors, owners, authorized representatives, employees, agents, partners and professionals performing any work for their account, must notify the Center immediately if they suspect or have reasonable grounds to suspect that funds are proceeds of a crime, or are related to money laundering or terrorism financing. The reporting obligation also extends to attempted transactions regardless of their value.

  There shall be no penal, civil, or administrative liability for reporting persons when reporting according to the provisions of the present article."

**Recommendation (20) of the FATF Recommendations**

20-1 If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to TF, it should be required to report promptly its suspicions to the Financial Intelligence Unit.

20-2 Financial institutions should be required to report all suspicious transactions, including attempted transactions, regardless of the amount of the transaction.

**Suspicion:**

- Suspicion refers to the stage of doubt that the transaction features an unusual activity or an activity resulting of a criminal activity, in accordance with any of the red flags monitored by the reporting entity.
- The difference between certainty and suspicion, it is important to note that certainty arises from the existence of clear and conclusive evidence. A suspicion report shall be filed before the NCFI in both cases (certainty and suspicion).

- **Challenges of detecting terrorism financing operations.**

In general, the Sultanate of Oman may be generally far from terrorism financing operations. However, the challenge lies in the low number of reports received from the reporting entities. In any case, reporting of these reports and suspicious information received may face some challenges, most importantly the following challenges:

1. Many indicators of suspicion of terrorism financing crimes are similar to money laundering crimes.

2. Sometimes financial transfers to countries suffer from security or political instability, and then there is difficulty in communicating with the counterpart centers in those countries.

3. Lists, although updated, may not include people or entities in suspicion.

4. Financial transfers may be for people, associations or entities actually working in humanitarian work, but they are not famous or licensed in their countries.

5. The goodwill is available to many financiers for his lack of knowledge or knowledge of the nature of the person's activities or the group to which the money is transferred.

6. Although there is not enough evidence for the use of digital currencies in terrorist activities now, in the future it may represent the most important challenges.

- **Recommendations of the National Center for Financial Information for Financial Institutions.**

  What distinguishes operations related to terrorism financing from operations related to money laundering are as follows:

1. Small transactions including bank transfers and currency exchange can be used to finance terrorist activities.
2. It is possible to finance terrorists using funds obtained legally, and therefore it is difficult for the financial institution to determine the stage at which legitimate funds have become funds used to finance terrorist operations, where the terrorist can obtain sources of financing terrorist operations from legitimate and / or illegal sources.

- **Therefore, financial institutions should:**

1. To ensure that the internal control and follow-up systems do not focus only on high-value transactions.
2. To include in the control systems indicators related to terrorist financing.
3. Search for processes that have no clear economic purpose.
4. Apply effective controls and procedures to know and verify the customer.
5. Monitor operations continuously and report suspicious operations to ensure that the financial system in the Sultanate is not misused to finance terrorists, terrorist organizations or terrorist acts.
6. Effective monitoring of cash deposits through all withdrawal channels.

## Tenthly: Sanctions

**Law No. (30/2016) on Combatting Money Laundering and Terrorism Financing has stipulated two essential obligations:**

1. Immediately notifying the Center, in accordance with Article (47), stipulating the following: "As an exception to the provisions on the confidentiality of banking transactions and professional and contractual secrecy, financial institutions, non-financial businesses and professions, NPOs, their managers, members of the board of directors, owners, authorized representatives, employees, agents, partners and professionals performing any work for their account, must notify the Center immediately if they suspect or have reasonable grounds to suspect that funds are the proceeds of crime, or are related to money laundering or terrorism financing. The reporting obligation also extends to attempted transactions regardless of their value.

   **There shall be no penal, civil, or administrative liability for reporting persons when reporting according to the provisions of the present article.**

3. Abstaining from disclosing to the customer, the beneficial owner, or any other party, whether directly or indirectly, of any information related to the procedures applied in combatting money laundering or terrorism financing in accordance with Article (49) stipulating the following: "Reporting persons as identified under Article 47 of the present Law shall not reveal to the customer, beneficial owner or any other party, directly or indirectly and by any means whatsoever, that they have issued or are about to issue a suspicious transaction report nor should they give any information or data in relation with such reports or alert them to any investigation in this regard."

**The Law on Combatting Money Laundering and Terrorism Financing includes two Articles on sanctions for non-compliance:**

**Article (95) sets forth a general sanction for all obligations, as follows:**

A penalty of imprisonment for a term of no less than six months but not exceeding two years and a fine of no less than RO 10,000 but not exceeding RO 50,000, or one of these two punishments, shall be imposed on any of the chairmen and members of the boards of financial institutions, non-financial businesses and professions and NPOs, their owners, authorized representatives or employees who, acting intentionally or because of gross negligence, contravene any of the obligations specified in Articles (33) to (50) of Chapter Five of this law.

**Article (96) tackles non-compliance with Articles (47) and (49) only, as follows:**

Chairmen and members of the boards of financial institutions and non-financial businesses and professions, non-profit associations and entities, their owners, authorized representatives or employees who have failed to comply whether intentionally or by gross negligence with obligations stipulated in Articles 47 and 49 of the present Law, shall be punishable with imprisonment for a term of no less than six months but not exceeding three years and a fine of no less than RO 10,000 but not exceeding RO 20,000 or one of these two sanctions. If the violation is in the interest or on behalf of a legal person, they shall be punishable with a fine of no less than RO 50,000 but not exceeding RO 100,000.


**Sultanate of Oman**

**National Centre for Financial Information (NCFI)**
**P.O.Box 3443 , PC 111**

**Tel. (+968) 24569459 , 24569192**

**Fax: (+968) 24569165**

**E-mail: info@fiu.gov.om**

**website: www.fiu.gov.om**