وحدة المعلومات المالية
Financial Information Unit

TERRORIST FINANCING GUIDANCE

Table of Contents

INTRODUCTION

This guidance on TF suspicious transactions, designed within the Qatar Financial Information Unit's (QFIU) outreach program, is applicable to all reporting entities under Law No. (20) of 2019 and should be read in conjunction with other guidance issued by the QFIU and other competent authorities in Qatar.

This guidance provides terrorist financing (TF) indicators that were developed by QFIU through a review of ML/TF cases and Suspicious Transection Reports (STRs), Manuals, Guides and Best Practices by international organizations such as the Financial Action Task Force (FATF) and the Egmont Group, counterpart FIUs, and consultation with the competent authorities.

These indicators do not cover every possible situation, but were developed to provide reporting entities with a general understanding of what is or could be unusual or suspicious, and help identify relationships between individuals and entities and determine significant events to identify the possible existence of a TF related activity.

I. PURPOSE OF THIS GUIDANCE

1. Raising awareness among reporting entities of the significance and priority of combatting terrorist financing, by developing a Guidance on reporting TF suspicious transactions or any attempts to perform TF-related transactions, and making CFT a strategic objective for the State of Qatar.

2. Enhancing the understating of the reporting entities of TF risks and the threats that may pose to the State of Qatar and to the reporting entity itself.

3. Educating the reporting entities regarding TF patterns and types of TF-related transactions at the regional and international levels.

4. Raising awareness among the reporting entities of jurisdictions with a high-risk of terrorism financing and Foreign Terrorist Fighters (FTFs), and the methods used by terrorism financiers to raise and move funds to finance their operations.

II. GENERAL RULES

- In applying the indicators, reporting entities should be advised that **no single transactional indicator is a clear barometer of terrorist activity. The TF indicators in this guidance are not an exhaustive list of TF indicators to support all suspicious scenarios.** Reporting entities should consider additional factors, such as a customer's overall financial activity and whether multiple indicators are exhibited, before determining a possible association to Terrorist Financing and/or ***Foreign Terrorist Fighters*** (FTFs). Some indicators below may be observed during general transactional screening, while others may be more readily identified during in-depth case reviews.

- Due to the ever-evolving nature of the ML/TF environment, high-risk jurisdictions are often subject to change. To ensure that you are referencing accurate information, QFIU encourages you to research publicly available sources on a regular basis to support these ML/TF indicators as part of your STR program.

- There are multiple sources that identify jurisdictions of concern, including the FATF which publishes contextual information on high-risk jurisdictions in relation to their risk of money laundering and terrorist financing. You may also observe funds coming from or going to jurisdictions that are reported in the media as locations where terrorist operate/carry out attacks and/or where terrorists have a large support base (state sponsors or private citizens). Identifying high-risk jurisdictions or known trends can also be included as part of your risk-based-approach and internal STR program.

III. TIMELINE FOR REPORTING TF-RELATED TRANSACTIONS

Reporting Entities shall **promptly** submit STR to QFIU to report any suspicious financial transaction or any attempts to perform such transactions. When there is suspicion that the transaction is linked to, or to be used in terrorist acts or by terrorist organizations, the STR must be sent **within 24 hours of the financial entity determining that the transactions were suspicious** as per the relevant QFIU guidelines.

IV.GENERAL TERRORIST FINANCING INDICATORS

The indicators below are some examples of general indicators relating to terrorist financing:

1. Transactions involving certain high-risk jurisdictions such as locations in the midst of or in proximity to, armed conflict where terrorist groups operate or locations which are subject to weaker ML/TF controls.

2. An account opened in the name of an entity, a foundation or association, which may be linked or involved with a suspected terrorist organization.
3. Transactions in the name of an entity, a foundation or association, which may be linked or involved with a suspected terrorist organization.
4. The use of funds by a non-profit organization is not consistent with the purpose for which it was established.
5. Customer who privileges secrecy, by avoiding providing or revealing the necessary, required or relevant information when engaging in a transaction.
6. Raising donations in an unofficial manner without having the proper license or permission.
7. Transactions involve customers identified by media as having travelled, attempted or intended to travel to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
8. Transactions involve individual(s) or entity (ies) identified by media and/or sanctions lists [1]as being linked to a terrorist organization or terrorist activities.
9. Customer conducted travel-related purchases (e.g. purchase of airline tickets, travel visa, passport, etc.) linked to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.
10. Individual or entity's online presence supports violent extremism or radicalization.
11. Customer donates to a cause that is subject to derogatory information that is publicly available (e.g. crowdfunding initiative, charity, non-profit organization, non-government organization, etc.).
12. Value of transactions is inconsistent with the suspect's profile, financial standing or usual pattern of activities.
13. Unexplained frequent transfers on an in-and out basis, without any apparent link between the suspect and the individuals or entities involved.

V. FOREIGN TERRORIST FIGHTERS INDICATORS[2]

Foreign Terrorist Fighters (FTFs) are Individuals who travel to a state other than their states of residence or nationality for the purposes of perpetrating, planning, preparing, or participating in terrorist acts; or for providing or receiving terrorist training, including in connection with armed conflicts.[3]

Preventing terrorists and terrorist entities, including FTFs, from exploiting the global financial system is a key priority for QFIU. The actions of terrorist organizations, including al-Qa'ida, the Islamic State in Iraq and the Levant (ISIL/Da'esh) and their respective affiliates, and the proliferation of FTFs, pose a serious threat to international peace and security.

To address the increasing and serious threat posed by these terrorist organizations, and **further to the FTFs indicators issued by QFIU in 2015**, QFIU provides the following additional indicators describing specific characteristics of financial transactions that are more likely to be involved with or linked to FTFs financing:

---

[1] *See*, Definition of the "Sanctions List" in Law No.(27) of 2019 Promulgating the law on Combatting Terrorism, Articles (1) and (31)

[2] A Financial Typology of Foreign Terrorist Fighters in Iraq and the Levant, The Egmont Group of FIUs, February 2017.

[3] *See*, United Nations Security Council Resolution 2178 (2014).

1) Use of ATMs Near ISIL-Controlled Territory

To avoid reporting false positives, such as international aid workers or travelers with family near the conflict zone, reporting entities should review such data to consider both positive and negative indicators that the subject is a possible FTF.

The following are some high-risk and low-risk criteria that can help determine whether an ATM user near ISIL-controlled territory should be reported:

 Higher-risk:

- A period of account inactivity preceding the ATM transactions, which could indicate that the account holder had been present in ISIL-controlled territory.
- Purchases prior to travel where the merchant is a camping, sporting goods, or military surplus store.
- The account holder's home address is close to the location of other known FTFs.
- Cash deposits into the account preceded the ATM withdrawals.
- Money transfers paid out or ATM withdrawals in non-local currencies, such as US dollars or euros.

 Lower-risk:

- The financial institution associated with the account is affiliated with a UN, a government, or a non-governmental aid organization.
- The account holder is a citizen of the country in which the activity takes place, indicating the account holder may be visiting family.
- The account holder's profession is indicated as a journalist or other profession with reason to travel to the area for benign purposes.

2) Money Services Businesses (MSB) Transactions to Unrelated Individuals in High-Risk Areas

FTFs in high-risk areas receive funds via MSB transactions. The funds are commonly from unrelated individuals, and most payments probably are completed through third parties for ease of transaction, particularly for individuals based in conflict zones, and also in an attempt to hide the relationship between the sender and receiver, as well as the purpose of the funds. The use of MSBs appears to be one of the preferred methods of transferring funds to individuals in conflict areas.

- MSB payments to high-risk areas will often have a common receiver from unrelated individuals. Some of the senders were identified as having known links to FTFs.

3) Detecting Facilitators Using Common Counterparties

One of the most successful techniques for identifying FTFs was to begin with individuals identified by reliable law enforcement reporting and then trace their financial transactions to identify common counterparties among them.

1. Common counterparty analysis can help identify possible financial facilitators. The facilitators primarily act as recipients of funds; they collected the funds and then delivered cash to ISIL members in conflict zones.
2. Each financial facilitator operated for a few months at a time before switching to another facilitator. The facilitators appear to be active in one to two-month spurs, receiving large numbers of transactions before becoming inactive, at which time a different facilitator becomes active.

4) Returning FTFs

Analysis of STR information on returning FTFs can be divided into two categories: (1) financial activity while in transit or located in countries bordering ISIL- controlled territory, and (2) financial activity following the return to their homeland.

The following are "red flags" associated with possible FTF return travel:

1. Reactivating bank account after long period of inactivity by deposits in cash or from other accounts by family members or FTSs;
2. Reactivating bank account after long period of inactivity by using debit card to withdraw cash at ATMs in countries bordering the ISIL occupied territories;
3. Reactivating the use of credit cards;
4. Wire transfers to FTFs' bank account by family members or by associates associated with known FTF/FTS networks;
5. Funds transfers via MSBs to countries adjacent the conflict zone; and
6. Cash withdrawals or debit card transactions in countries adjacent to the conflict zone after a long period of inactivity.
7. Money transfers sent to the region by family members or FTSs
8. Money transfers sent by family members or FTSs to places along the travel route back home, including those picked up by other people (because of lack of identity documents or an effort to avoid scrutiny).
9. Pay out in currency other than the local one (usually in US dollars or euros)

Upon return to their homeland, FTFs have been involved with the following type of financial transactions:

1. Sending money transfers of small amounts to peer-group members residing in countries bordering their homeland;
2. Cash deposits to their personal bank account and transferring small amounts to private bank accounts of peer-group members;
3. Cash withdrawals from personal bank account;
4. Transferring small amounts to the accounts of NPOs known to be related to extremists;
5. Money transfers sent to countries bordering ISIL-controlled territory;

6. Receiving money transfers sent from Iraq and Syria.

VI. ABUSING THE SERVICES OF NON-PROFIT ORGANIZATIONS (NPOs)[4]

The following primary red flag indicators reflect possible cases of TF misuse, or would be present in scenarios of NPO involvement in TF. The presence of more than one of these primary indicators should increase the weight given to any suspicion of TF misuse.

1. NPO treasurer or employee withdraws cash from the NPO account and then deposits it into a personal account, before diverting the funds to a suspected terrorist's account.
2. Media reports the NPO is linked to known terrorist organizations or entities that are engaged, or suspected to be involved, in terrorist activities.
3. Parties to the transaction (for example: account owner, sender, beneficiary or recipient) are from countries known to support terrorist activities and organizations.
4. Funds sent from large international NPOs based in high-risk countries, to their branches in regional countries, are channeled to local NPOs based or operating in domestic conflict areas.
5. An NPO sending funds to multiple entities (individuals and companies) in a high-risk country.
6. NPO raises funds from a major public event and then authorizes a third party to be a signatory to the NPO account, who uses it to send funds to high-risk countries.
7. Unusual or atypical large cash withdrawals, particularly after the financial institution refuses to wire NPO funds overseas (thus raising cross-border cash smuggling suspicions).
8. Transactions, including international and domestic transfers, with NPOs that contain terms associated with violent extremism and other terrorist ideologies; for example, ghanimah or fai/fay (justified stolen funds) and mujahid/mujaheed/mujahideen (the term for one engaged in Jihad).
9. Vague justifications and a lack of documentation when the financial institution questions NPO requests to transfer funds to high-risk locations or entities.
10. Use of NPO accounts to accept funds from suspected terrorists and their associates (based on law enforcement agency alerts on persons of interest).
11. Transactions (cash and transfers) involving key personnel of foreign NPOs associated with United Nations Security Council designated individuals and terrorist entities.

The following are secondary red flag indicators in some TF cases involving NPOs, but also appear in more general illicit activity (such as fraud and money laundering). Secondary indicators may come to light after a primary indicator triggers deeper checks of an NPO's behavior. Enhanced

[4] 2018 Non-Profit Organization & Terrorism Financing Red Flag Indicator, AUSTRAC, PPATK, and AMBD.

due diligence or transaction monitoring may also identify these indicators. This should prompt further searches to corroborate initial suspicions and try to determine whether the indicators relate to TF or another crime.

A combination of primary and secondary indicators should be considered highly suspicious and likely grounds to file an STR.

1. NPO transactions for which there does not appear to be a logical economic purpose or link between the NPO's stated activities and the other parties in the transaction.
2. NPO uses crowd funding and social media to solicit donations, and then its online presence vanishes or shuts down.
3. NPO's account shows signs of unexplained increases in deposits and transaction activity.
4. NPO is unable to account for the final use of all its funds/resources.
5. NPO uses unnecessarily complex banking arrangements or financial networks for its operations, particularly overseas.
6. NPO, or NPO representatives, use falsified or conflicting documentation.
7. Inconsistencies between the pattern or size of financial transactions and the stated purpose and activity of the organization.
8. Unexpected absence of contributions from donors located in the country.
9. Large outgoing transactions to the country of origin of NPO directors who are foreign nationals, particularly if the country is high risk.
10. NPO appears to have few or no staff and limited or no physical presence, which is at odds with its stated purpose and scale of financial activity.
11. NPO funds commingled with personal/private or business funds.

VII. ABUSE OF SOCIAL MEDIA[5]

The threats of global terrorism are continuing to evolve. Irrespective of the differences in financial requirements between terrorist groups or individual terrorists, all terrorist actors seek to ensure adequate revenue and management of funds to fund their operations. The global anti-money laundering/combating the financing of terrorism (AML/CFT) network has recognized that social media services are susceptible to be abused for terrorism financing (TF). Cases have shown that social networking services (e.g. Facebook), content hosting services (e.g. YouTube), crowd funding services (e.g. GoFundme.com) and Internet Communication Services (e.g. WhatsApp) are being abused in a variety of ways for TF, as follows:

a. Social networking services (SNS) and content hosting services (CHS) are primarily used to solicit donations, promote terrorism through propaganda and radicalization.
b. Crowdfunding services were used in a number of cases, with campaigners often disguising the use of funds for humanitarian causes.

[5] Social Media and Terrorism Financing, Asia Pacific Group on Money Laundering & Middle East and North Africa Financial Action Task Force, January 2019.

The following are useful indicators to help identify individuals or entities possibly involved with or linked to terrorist financing through their use of social media:

1. Use of SNS to call for funds to support specific organisation that involves in terrorism-related extremism and radicalization movement.
2. Use of SNS via messages and pictures to call for funds from donors to support a known terrorist front.
3. Use of SNS to initiate contact with potential donors for donation.
4. Use of SNS by charities to call for funds for humanitarian causes while funds were actually directed to support FTFs.
5. A terrorism-related charity uses SNS to share visual media to attest legitimacy of their activities and communicate with donors.
6. Use of SNS by the members of the charity to portray involvement with terrorists and terrorist entities, including their weaponry training activities.
7. Use of SNS to raise funds under the pretext of humanitarian cause then physically moving the funds across borders via several passengers and structuring the funds below declaration threshold.
8. Use of personal Facebook profile to declare joining a UN listed terrorist organisation and posting related daily life incidents.
9. Use of SNS to raise funds for the families of parties convicted of terrorism offences.
10. Use of CHS to call for funds to support terrorist groups to support travel expenses of FTFs and family members of terrorists.
11. Post bank details (belonging to a known person in a conflict zone) for donations on CHS and SNS to support travel expenses of FTFs and family members of terrorists.
12. Contact between content creator on CHS and SNS and family member of persons associated with terrorist groups.
13. Use of SNS, ICS and crowd funding sites by a NPO to raise funds allegedly to support terrorists, terrorist entities and their activities.
14. Use of crowd funding websites to generate funds for terrorists and their family members.
15. Use of crowd funding services which provides donation options to conflict relief to raise funds prior for the locals to travel to conflict locations.
16. Use of crowd funding services which provides donation options to countries with conflict.
17. Use of ICS to organise deposits and withdrawals using the bank account of a terrorist's family member.
18. Use of ICS to organise bank and remittance transactions for financing an individual terrorist in exchange for a commission.
19. Use of ICS to organise remittance of funds to areas close to ISIL strongholds.
20. Use of ICS to swear allegiance to group led by listed terrorist.
21. Use of ICS, upon instruction of terrorist, to organise and to deposit donations into a member of the group's bank account.

22. Use of SNS and ICS are used for the purpose other than the real purpose it is intended for, to promote operations for donations, and to communicate with persons located in conflict zones.
23. Calling of funds is made publicly but the method of collecting the funds remains discrete by accessing the private account on SNS or through telephone communication.
24. Most of the funds are collected by fund raisers, while the other part is privately transferred through banks or exchange companies or through prepaid cards belonging to (close or trusted) members of the terrorist organization.
25. Accounts that have a large number of followers on the social media were used to raise donations, advertising bank account numbers and phone numbers of persons in charge of collecting funds.

VIII. SUSPICIOUS TRANSACTION REPORTING BASED ON THIS GUIDANCE

Reporting entities should reference this Guidance (#TFI2021) when reporting to QFIU potential TF-related transactions based on indicators contained in this Guidance, using the required STR Form.

Referencing this Guidance in Suspicious Transaction Reports (STRs) will allow QFIU to identify and prioritize terrorist-related reports.

Entities reporting terrorist financing through STRs are reminded to include all relevant and detailed information as is permissible, such as identifying information, account numbers, counterparties, and associates.