Lists of Red Flag Indicators for Terrorist Financing

Four Lists of Red Flag Indicators for Terrorist Financing

1. Financial and Behavioral Indicators Published by The Egmont Group of Financial Intelligence Units

Indicators linked to the financial transactions:

1. The use of funds by the non-profit organization is not consistent with the purpose for which it was established.
2. The transaction is not economically justified considering the account holder's business or profession.
3. A series of complicated transfers of funds from one person to another as a means to hide the source and intended use of the funds.
4. Transactions which are inconsistent with the account's normal activity.
5. Deposits were structured below the reporting requirements to avoid detection.
6. Multiple cash deposits and withdrawals with suspicious references.
7. Frequent domestic and international ATM activity.
8. No business rationale or economic justification for the transaction.
9. Unusual cash activity in foreign bank accounts.
10. Multiple cash deposits in small amounts in an account followed by a large wire transfer to another country.
11. Use of multiple, foreign bank accounts.

Behavioral Indicators:

1. The parties to the transaction (owner, beneficiary, etc.) are from countries known to support terrorist activities and organizations.
2. Use of false corporations, including shell-companies.
3. Inclusion of the individual in the United Nations 1267 Sanctions list.
4. Media reports that the account holder is linked to known terrorist organizations or is engaged in terrorist activities.
5. Beneficial owner of the account not properly identified.
6. Use of nominees, trusts, family member or third party accounts.
7. Use of false identification.
8. Abuse of non-profit organization.

2. Potentially Suspicious Activity That May Indicate Terrorist Financing Published in the FFIEC BSA/AML Examination Manual

Activity Inconsistent With the Customer's Business:

1. Funds are generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from higher-risk countries (e.g., countries designated by national authorities and FATF as noncooperative countries and territories).
2. The stated occupation of the customer is not commensurate with the type or level of activity.
3. Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g., student, unemployed, or self-employed).
4. Regarding nonprofit or charitable organizations, financial transactions occur for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.
5. A safe deposit box opened on behalf of a commercial entity when the business activity of the customer is unknown or such activity does not appear to justify the use of a safe deposit box.
6. Funds Transfers:
7. A large number of incoming or outgoing funds transfers take place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves higher-risk locations.
8. Funds transfers are ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
9. Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected.
10. Multiple personal and business accounts or the accounts of nonprofit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.
11. Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to higher-risk countries.
12. Other Transactions That Appear Unusual or Suspicious:
13. Transactions involving foreign currency exchanges are followed within a short time by funds transfers to higher-risk locations.
14. Multiple accounts are used to collect and funnel funds to a small number of foreign beneficiaries, both persons and businesses, particularly in higher-risk locations.
15. A customer obtains a credit instrument or engages in commercial financial transactions involving the movement of funds to or from higher-risk locations when there appear to be no logical business reasons for dealing with those locations.
16. Banks from higher-risk locations open accounts.
17. Funds are sent or received via international transfers from or to higher-risk locations.
18. Insurance policy loans or policy surrender values that are subject to a substantial surrender charge.

3. Financial Red Flags Published by DML Associates LLC:

    1. IP logins in areas of conflict such as near the Syrian border, to include Jordan and Lebanon, but particularly in Turkey
    2. Periods of transaction dormancy, which could be the result of terrorist training or engagement in combat
    3. ATM cash withdrawals in areas of conflict
    4. Wire transfers to areas of conflict
    5. Charitable activity in areas of conflict especially in Syria
    6. Financial activity identifiable with travel [purchase of airline tickets] to Syria through Turkey and other points of entry to include Jordan, Lebanon and Israel

4. Terrorist Activity Financing Related Indicators Published by FINTRAC (Canada's Financial Intelligence Unit)

It may be noted that a single indicator on its own may seem insignificant, but combined with others, could provide reasonable grounds to suspect that the transaction is related to terrorist financing activity.

1. Client accesses accounts, and/or uses debit or credit cards in 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.
2. Client identified by media or law enforcement as having travelled, attempted/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.
3. Client 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.
4. The client mentions that they will be travelling to, are currently in, or have returned from, a high risk jurisdiction (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.
5. Client depletes account(s) by way of cash withdrawal.
6. Client or account activity indicates the sale of personal property/possessions.
7. Individual/Entity's online presence supports violent extremism or radicalization.
8. Client indicates planned cease date to account activity.
9. Client utters threats of violence that could be of concern to National Security/Public Safety.
10. Sudden settlement of debt(s) or payments of debts by unrelated 3rd party(ies).
11. Law enforcement indicates to reporting entity that the individual/entity may be relevant to a law enforcement and/or national security investigation.
12. Client's transactions involve individual(s)/entity(ies) identified by media or law enforcement as the subject of a terrorist financing or national security investigation.
13. Client donates to a cause that is subject to derogatory publicly available information (crowdfunding initiative, charity, NPO, NGO, etc.).

14. Client conducts uncharacteristic purchases (e.g. camping/outdoor equipment, weapons, ammonium nitrate, hydrogen peroxide, acetone, propane, etc.).
15. A large number of email transfers between client and unrelated 3rd party(ies).
16. Client provides multiple variations of name, address, phone number or additional identifiers.
17. The sudden conversion of financial assets to a virtual currency exchange or virtual currency intermediary that allows for increased anonymity.

The red flags indicators noted above can conveniently be shared with staff to create the awareness amongst them for tracking and reporting suspicious transactions and for enhancing the efforts to counter terrorism.

Consolidated Red Flag Indicators (RHO for detecting suspicious transaction by the Depository Participants)
(As per FIU- IND Guidelines 9-2/2021/Intermediaries/FIU-IND dated 31st December 2024)

Alert Source	Alert Indicator
Customer verification	CV1 - Customer left without opening account
	CV2 - Customer offered false or forged identification documents
	CV3 - Address found to be wrong
	CV4 - Difficult to identify beneficial owner
Law Enforcement Agency Query	LQ1 - Customer is being investigated for criminal offences
	LQ2 - Customer is being investigated for TF offences
	LQ3 - SEBI has passed orders under the SEBI Act, 1992 with Rules and Regulations made thereunder.
Media Reports	MR1 - Adverse media report about criminal activities of customer
	MR2 - Adverse media report about TF or terrorist activities of customer
Employee Initiated	EI1- Customer did not complete transaction
	EI2- Customer provides inconsistent information
	EI3 - Customer wants to avoid reporting
	EI4 - Customer could not explain source of funds
	EI5 – Transaction is unnecessarily complex
	EI6 - Transaction has no economic rationale
	EI7 - Transaction inconsistent with business
	EI8 – Power of Attorney Transactions
	EI9 – Suspicious Closure of Account
Public Complaint	PCI-Complaint received from public
Business Associates	BA1 - Alert raised by agent
	BA2 - Alert raised by other institution

Typology	TY1-Transactions similar to typologies found in Orders passed under the SEBI Act
Transaction Monitoring	TM1 - High value Deals - Single transaction
	TM 2 - High value Deals - Aggregate transaction
	TM3 - Synchronized, Cross and Self Trades
	TM 4 - Turnover vis-à-vis financial income submitted by the client
	TM 5 - High value transactions in a new account
	TM 6 - High value transactions in a dormant account
	TM 7 - Frequent Small quantity transactions in an account
	TM 8 - Transaction in illiquid strips/ unlisted strips
	TM 9 – Off Market transfer to unrelated accounts
	TM 9A – Suspicious Off Market Credit and Debit
	TM 9B – Off market delivery in unlisted scrip
	TM 9C – Gift, Donation related off-market transfer
	TM 9D – Off Market transfer at variance with market value
	TM 9E – Off Market transfer in suspicious scrip

Notes:

✓ Depository Participants have to generate alerts independently based upon the alert scenarios mentioned in TM9, TM9A, TM9B, TM9C, TM9D, TM9E and EI 9. Depository Participants have to undertake meaningful analysis, closure and filing of STRs of these alerts as defined under the PML rules.

✓ Depositories were also advised to generate and forward alerts to the depository participants based upon the above alert scenarios (TM9, TM9A, TM9B, TM9C, TM9D, TM9E and EI 9), which are mentioned as TM13, TM13A, TM13B, TM13C, TM13D, TM13E and EI13 in the 'Supplemental Guidelines for Detecting Suspicious Transaction for Depositories' dated 21/07/2022.

✓ Alerts thus generated by the Depository Participants, need to be cross checked with the alerts being forwarded by the Depositories to ensure that all the alerts are carefully generated by the Depository Participants and meaningful analysis of these alerts have been conducted for detecting suspicious transactions.

✓ These RFI guidelines issued for the Depository Participants are common minimum alerts and parameters for generation of alerts. Depository Participants are advised to develop additional parameters for generation of additional alerts. Depository Participants can also set the thresholds depending upon the client profile. These thresholds are required to be reviewed periodically.

✓ The thresholds prescribed in these RFIs are indicative. Depository Participants are free to adopt stricter criteria thresholds, but may not adopt criteria less strict than that which is prescribed in these RFIs.