LearnAML

www.LearnAML.org

Terrorist Financing – Red-Flag Checklist (Foundational)

This checklist helps frontline and operations staff identify patterns that may indicate terrorist financing risk. No single point proves wrongdoing – staff should look for combinations of indicators and follow internal escalation procedures.

1. Customer Profile and Behaviour

- Customer provides vague, scripted, or inconsistent explanations about the purpose of accounts or transactions.
- Customer appears to act on behalf of others without a clear business or family reason.
- Customer shows unusual interest in how quickly funds can be moved to or from higher-risk areas.
- Customer is reluctant to provide basic information on source of funds or key counterparties.

2. Transaction Patterns

- Multiple low-value transfers to or from higher-risk jurisdictions with no clear family, trade, or remittance explanation.
- Frequent small incoming payments from different senders that are quickly consolidated and sent abroad.
- Use of personal accounts to receive and distribute funds that look like organisational or fundraising activity.
- Rapid movement of funds through accounts with low residual balances and no obvious commercial purpose.

3. Geography and Counterparties

- Payments involving countries, regions, or areas associated with terrorism, conflict, or weak controls.
- Transfers to or from entities whose names are similar to known organisations of concern.
- Regular payments to a small set of foreign beneficiaries without transparent documentation or reporting.

4. Use of Non-Profit Organisations

- Non-profit or charitable accounts sending a high share of funds overseas with limited programme detail or reporting.

- Frequent cash deposits into NPO accounts that are quickly withdrawn or remitted outside normal project cycles.
- Significant changes in donation patterns, beneficiaries, or destinations without a clear explanation.

5. Sanctions and List Indicators

- Possible matches to terrorism-related sanctions or watchlists for customers, beneficiaries, or counterparties.
- Repeated near-matches or spelling variants connected to higher-risk geographies or organisations.
- Transactions blocked or flagged by screening systems that are dismissed without adequate review or documentation.

When to Escalate

Staff should escalate to the MLRO or designated compliance contact when one or more of these indicators appear and cannot be reasonably explained by the customer’s known profile or legitimate activity.

Escalate to MLRO if you see combinations of unusual patterns, unclear purposes, higher-risk locations, or potential links to listed persons or organisations.