Terrorism Financing

Anomalies noted during customer/supplier due diligence

1. Unable to determine relationship between entity and counterparties who make frequent cash deposits into entity's accounts.
2. Entity suddenly procuring and/or shipping oil equipment to conflict zones, where the activity is not consistent with the entity's line of business or occupation.
3. Sudden increase in insurance policy purchases.
4. Customer seeks multiple changes in identity.
5. Customer is a holder of a replacement identification card.
6. Customer exhibits reluctance to provide Know Your Customer (KYC) information.
7. Customer exhibits signs of confusion and nervousness during the execution of their transaction.
8. Presentation of the identity document of a third party upon collection of a payment.
9. New customers who are reluctant to provide information or request to cancel the transaction as soon as the bank employees seek important missing information.
10. Customer attempts to make a large initial deposit when opening the account, where the amount provided is inconsistent with their economic profile.
11. Customer's wealth is disproportionately drawn from investments in virtual assets (VAs) originating from Virtual Assets Service Providers that lack AML/CFT controls, Initial Coin Offerings (ICOs), or fraudulent ICOs.
12. Customer's only source of funds is that of an inheritance from a foreign jurisdiction. Funds are transferred from an investment account to a savings account and are disposed of via day-to-day point of sale purchases.
13. Customer owns a business that involves trading in arms and ammunition without authorization or control.
14. Directors and/or operators of programs have no background in that type of operation, (for example, childcare operator with no previous deposits related to childcare).
15. Account opened in the name of a recently formed legal entity and in which a higher-than-expected level of deposits are made in comparison with the income of the founders of the entity.
16. Transactions with entities located in conflict zones (where terrorism-related activities or entities are present), and where the declared purpose for the transaction does not match the profile of the parties involved.
17. Entities log on to their online accounts from locations in conflict zones, in a manner that does not appear to have a lawful or legitimate purpose.
18. Customer using money and value transfer services or VASPs located overseas in a high-risk jurisdiction or known to have inadequate AML/CFT regulations including insufficient Customer Due Diligence (CDD)/KYC measures.
19. Selling off personal items prior to travel, including family homes. [Particularly relevant in the context of foreign terrorist fighters (FTFs)].
20. Taking out loans and maximizing spend on local credit cards prior to departure. [Particularly relevant in the context of FTFs].
21. Use of bank accounts owned by militant's relatives, neighbours and employees.
22. Entity(s) featured in adverse news/Transactions with entity(s) featured in adverse news.
23. Open-source analysis tools indicate a customer has transacted with dark web sites or sites linked to terrorist groups.
24. Customer has previously been investigated by law enforcement agencies (LEAs) for terrorism-related offences.

25. Use of agriculture companies (or those doing business with agriculture companies) due to their capital-intensive nature and use of raw materials used to produce improvised explosive devices (IEDs) as a decoy to move significant amounts of monies.
26. Online payments without delivery or service rendered.
27. Use of an electronic payment card by a person other than its holder.
28. Project fund is started by people subject to LEA interest.
29. Funding goals of the project are met quickly and the page is closed quickly after funding.
30. Partner mainstream charities and popular online fundraising platforms to gain trust and generate more funds using latest payment technology (e.g. e-wallet as method of transfer).
31. Crowdfunding websites are linked to VAs.
32. Crowdfunding is being organised to raise criminal defence fees for a known LEA target.
33. Project is seeking funding for children in conflict zones by individuals or groups not linked to registered charities.
34. Crowdfunding and social media used to solicit donations, then online presence vanishes or shuts down.
35. Customer's information contains encrypted email accounts.
36. Attempts to obtain multiple credit cards, overdrafts and/or loans; especially within an expedited timeframe.
37. Customer acquires agricultural land that could be used for illegal cultivation of narcotics (including but not limited to cannabis and opium products).
38. Unusual activities carried out by the relatives/entities related to the Designated Individuals and Entities.
39. Publicly available information/ Paid financial crime screening services indicates that the customer is known to LEAs for links to ethnically or racially motivated violence or terrorism [e.g. the customer establishing the account is a known leader of an extreme-right wing (ERW) group].
40. Elements of the customer's KYC information such as email accounts contain ERW rhetoric or ERW related terms.
41. Customer exhibits a connection to known ERW entities subject to media reporting and open sources.
42. Customer openly propagates extremism and violence, e.g., the customer wears clothing with symbols associated with ERW groups and ideology.
43. Customer establishing the account is a known member of an ERW group and is attempting to establish a bank account on behalf of an organisation.
44. Organisation and advertisement of ERW-themed fundraising campaigns on ERW-focused forums specifically seeking VAs.
45. Customer acquires land and/or real estate that could be used to host events (e.g. music or cultural festivals, sport or training events) that promote ERW ideology or serve as a meeting place for ERW groups.
46. Customer rents land and real estate to obtain revenue for ERW ideology and violence.
47. Commercial entities with known links to ERW groups hosting cultural and sporting events involving online ticket sales.
48. Nonprofit Organisation (NPO) has projects and/or partners in an area where terrorist entities are known to operate.
49. Address provided by the NPO or its affiliates belong to or is used by organisations suspected of terrorist activity.
50. Entities connected to a NPO were previously or are currently connected to Designated Organizations or terrorist activities.

51. NPOs' activities or assets, including its bank accounts, involve entities that are subject to administrative orders.
52. NPO has unreported activities, programs, or partners, for example, a financial report does not tally with the activity report.
53. NPO or its administrators are linked, or seemingly linked, to third parties that support or are engaged in terrorist activity.
54. NPO disburses funds to initiatives which are deemed vulnerable targets for organised crime groups or individuals for ML/TF purposes.
55. Account opened in the name of an NPO with an agent who is not a member of the board of the NPO.
56. Notable links between NPOs and individuals or groups known to LEAs for having links to ethnically or racially motivated terrorist (EoRMT) through online chat forums, crowdfunding campaigns, or physical events.

Unusual fund movement

57. Transactions indicated as 'donations' or 'contributions to humanitarian aid' (in particular to non-profit or religious organisations in a conflict zone).
58. Red-flag words such as 'prisoners' (Aseer) and 'martyr' (Syuhada, Mujahid/mujahidin) are included in transactions.
59. Use of messages that indicate that the transaction is related to terrorism in general or in the context of specific event.
60. Donations to cryptocurrency addresses and/or bank accounts published on Designated Individuals and Entities affiliated social media platforms.
61. Sudden increase in credit card debts.
62. Deposits are made into an account in an amount significantly higher than is usual for that account, with unknown sources.
63. Incomplete remittance information in wire transfers.
64. Cash deposits outside a customer stated line of activity are made in a location near an area associated with terrorist activities.
65. Customer sending funds (fiat or in the forms of VAs) to high-risk jurisdictions.
66. Sender and beneficiary have no relation to country where he/she sends/receives the money and cannot sufficiently explain why money is sent there/received from there (especially when receivers are foreign citizens).
67. Kidnapping for ransom schemes seek funds to be paid in a foreign jurisdiction via a local Hawala dealer or in the form of VAs.
68. Large cash deposits into the accounts of illegal money service operators and immediate transfer to bank accounts nominated by the depositor.
69. Large cash deposits into the operator's foreign currency account followed by immediate transfer of the equivalent (in domestic currency) to the account of the depositor or the bank account nominated by the depositor.
70. Sudden use of credit/payment cards in (a) high-risk territories (e.g., increased cash advances) when that use has been proceeded/followed by a few months inactivity (FTFs) or (b) in a FTF's country of provenance

or surrounding areas after a period of time when the cards were used in high-risk territories remained dormant (returnees).

71. Illicit purchases and/or smuggling of gold in or nearby a high-risk jurisdiction.
72. Engaging in extensive financial activity for humanitarian purposes immediately after the account is opened.
73. Request to transfer funds to a Designated Entity or Organisation or an entity linked to a Designated Entity or Organisation.
74. Funds being moved through online payment platforms with ERW symbols and memorabilia.
75. Transactions, using fiat currency or VAs, with references to specific ERW symbols and memorabilia.
76. Transactions at retailers linked to foreign ERW actors and/or conflicts relevant to ERW actors.
77. Individual within a network is dispersing funds to other parties, including payments for propaganda materials, media products and merchandise.
78. Transactions to entities in locales where para-military is training available.
79. Travel related payments that may indicate planned travel to high-risk jurisdictions or jurisdictions with particular relevance to ERW actors and those that sympathise with ERW-related terror.
80. Accounts with minimal activity previously and now showing inflows from unknown origins, followed by fund transfers to beneficiaries or ATM withdrawals in conflict zones.
81. Individuals attempting a cross-border transport of physical money to conflict zones or other localities with significant deficiencies in their AML/CFT systems. [Particularly relevant in the context of FTFs].
82. ERW entities or individuals pooling funds in an account with references to ERW festivals or gatherings and/or payments sent to an association or company run by a member.
83. Entities receiving payments with descriptions indicative of ERW ideological interests. This may include payment notation including references to extreme-right wing and anti-Semitic terminology.
84. Donations from ERW blogs and websites, which propagate ERW violence or terror.
85. Donations from domestic or foreign ERW groups or individuals, especially those known to LEAs for propagating ERW ideology and violence.
86. Donations from individuals to various ERW-aligned think tanks and online fundraisers.
87. NPO receives funds from a major public event but then authorises a third party to use the account to send funds to high-risk countries.
88. NPOs operating in conflict areas have wired significant funds to local companies whose activities are not related in any way to humanitarian services.
89. Use of multiple personal and business accounts or the accounts of NPOs to collect and then funnel funds immediately or after a short time to a small number of foreign beneficiaries.

Structuring/layering of transactions

90. Use of false corporations, shell-companies, shell-banks.
91. Multiple transactions/beneficiaries are involved in the transfer of funds.
92. Large cash transactions - Request by counterparty to bring cash over to their country/region to pass the money to them.
93. Mismatch between cash withdrawal location / stated purpose of transactions and the charity's activities.
94. Structuring of cash or VA withdrawals from multiple ATMs.
95. Transactions involving the use of multiple accounts, without a logical commercial explanation.

96. Uses of “smart” ATMs to make cash deposits without bank/ATM cards to several accounts. (A “smart” ATM is one that has more functionality than simply dispensing cash; it is intended to automate many of the functionalities that would have in the past required a bank teller.)
97. Foreign exchange transactions are performed on behalf of a customer by a third party followed by wire transfers of the funds to locations having no apparent business connection with the customer or to countries of specific concern.
98. Importing goods from abroad and selling them in conflict zones when the payment for the goods is made by a third party.
99. Cash deposits from a wide geographical base, or donations in the form of electronic transfers with references from known ERW terror groups.

Transactions with no apparent business/lawful purpose

100. Customer seeks to convert a large amount of fiat currency without a logical business explanation.
101. Regular transfer of funds in particular to jurisdictions where there is no connection with the place where the client lives or carries out his activities.
102. Declared purpose of the transaction does not match the profile of the parties involved. (Transactions linked to the purchase of items that may be used for terrorism activities.) E.g. During a review, entity had purchased large quantities of fertiliser. According to entity’s profile, it is a corporate services firm which has no need of fertiliser.
103. Purchases of chemicals that are usually used in the agricultural sector and may be used in the manufacture of explosive materials.
104. Frequent change of credit cards, involving requests for new/replacement cards.
105. Marked increase in transactions at firearms retailers/gun stores or an increase in frequency and value of transactions at these retailers where not previously observed.
106. Purchase of training that may increase a person’s capabilities to inflict violence such as, martial arts or shooters' associations or clubs.
107. Entity using membership fees to pay external service providers to conduct self-defence or survival training for its members.
108. Purchase of tactical equipment and weapons, such as firearms, IED precursors, tactical gear, clothing, training materials, or weapons manuals, including uses of VAs for such purchases.
109. Use of dedicated payment and crowdfunding platforms, which have explicitly declared their willingness (or even business model) to offer services to ERW actors (including financial services as well as hosting ERW forums or chats).
110. Multiple successive purchases of ERW-related merchandise, especially where the activity is outside the customer’s normal purchasing behaviour.
111. Escalation in ERW related merchandise purchases directly before or after an ERW attack; or purchases of ERW iconography consistent with the attack.
112. Online sales of ERW-related merchandise.
113. Payment from ticket sales that relate to an ERW event being hosted domestically or abroad.