APPENDIX
RED FLAG INDICATORS FOR LABUAN IBFC

Introduction

The list of red flag indicators is specific to the inherent characteristics and vulnerabilities associated with financial activities. They are neither exhaustive nor exclusive. Upon applying these red flag indicators, Labuan entities must not refer to only one indicator to determine whether a transaction is suspicious or linked to a terrorist activity.

Part I: Red Flag Indicators for Labuan Digital Financial Services

The digital financial services have the potential for enhancing financial innovation and efficiency. Nevertheless, due to the unique features, the services pose money laundering and terrorist financing risks as well as the potential for transferring digital assets outside regulated systems and attribute to disability in tracing funds transfer.

1. Indicators relating to Customer Due Diligence Process

(a) Incomplete or insufficient information, or the customer declines to provide supporting documents or enquiries regarding source of funds;

(b) Lack of information or provide inaccurate of information on transaction, source of funds or counterparty. This may include the use of shell companies or those funds placed in an Initial Coin Offering (ICO) where personal data of investors may not be available or incoming transactions from online payments system;

(c) A customer provides forged documents or edited documents e.g. photographs, identification documents as follows:

(i) A customer provides identification or account credentials (e.g. a non-standard IP address, or flash cookies) shared by another account.

(ii) Discrepancies between IP addresses associated with the customer's profile and the IP addresses from which transactions are being initiated.

(iii) A customer's digital asset address appears on public forums associated with illegal activity.

(iv) A customer is known via publicly available information to law enforcement due to previous criminal association.

(d) A customer's funds which are sourced directly from third-party mixing services or wallet tumblers;

(e) The bulk of a customer's source of wealth is derived from investment in digital assets, ICOs or fraudulent ICOs, etc.; and

(f) A customer's source of wealth is disproportionately drawn from digital assets originating from other digital asset service providers that have deficiency of AML/CFT controls.

2. Indicators relating to Transaction Size and Frequency

(a) Structured transactions in small amounts and under the record-keeping or reporting thresholds;

(b) Multiple high-value transactions; and

(c) Transfers of digital assets immediately to multiple digital asset service providers, including those registered or operated in other countries.

3. Indicators relating to Irregular, Unusual or Uncommon Transaction Patterns

(a) New users make a large initial deposit to open a new relationship with a digital asset service provider, inconsistent with the customer profile;

(b) Transactions involve multiple digital assets, or multiple accounts, without a logical business explanation;

(c) Frequent transfers occur in a certain period to the same digital asset account by more than one person, from the same location or concerning large amounts;

(d) Creations of separate accounts under different names to circumvent restrictions on trading or withdrawal limits imposed by digital asset service providers;

(e) Transactions initiated from non-trusted IP addresses, IP addresses from sanctioned jurisdictions or IP addresses previously flagged as suspicious;

(f) A customer attempts to open an account frequently within the same digital asset service provider from the same IP address;

(g) A customer frequently changes his/her identification information, including email addresses, IP addresses or financial information, which may also indicate takeover of the customer's account;

(h) The use of language in digital asset message fields indicative of the transactions are related to illicit activities or for the purchase of illicit goods; and

(i) A customer repeatedly conducts transactions with a subset of individuals at significant profit or loss. This could indicate potential account takeover and attempted extraction of victim balances via trade, or money laundering scheme to obfuscate funds flow with a digital asset service provider infrastructure.

4. Indicators relating to Technological Features

(a) Transactions involving more than one type of digital assets particularly those that provide higher anonymity, such as anonymity enhanced cryptocurrency or privacy coins;

(b) Digital assets moved from a public transparent blockchain to a centralised exchange and then immediately traded for anonymity enhanced cryptocurrency or privacy coin;

(c) A customer that operates as an unlicensed digital asset service provider on peer-to-peer exchange website;

(d) Digital assets traded to or from wallets that indicated the use of mixing or tumbling services or peer-to-peer platforms;

(e) For merchants/corporate users, their Internet domain registrations are in a different jurisdiction than their jurisdiction of establishment or in a jurisdiction with a weak process for domain registration;

(f) A customer tries to enter one or more digital asset service providers from different IP addresses frequently over the course of a day; and

(g) Abnormal transaction activities of digital assets from peer-to-peer platform associated wallets with no logical business explanation.

5. Indicators relating to Geographical Risks

(a) Customer's funds originate from, or are sent to, an exchange that is not registered in the country where either the customer or exchange is located;

(b) A customer utilises a digital asset exchange or foreign-located Money Value Transfer Service in a high-risk country which has insufficient or inadequate of AML/CFT regulations for digital asset entities, including inadequate Customer Due Diligence or Know-Your-Customer measures;

(c) A customer sends funds to digital asset service providers operating in jurisdictions that have no digital asset regulation or have not implemented AML/CFT controls; and

(d) A customer sets up offices in or moves offices to jurisdictions that have no regulation or have not implemented regulations governing digital assets or sets up new offices in jurisdictions where there is no clear business rationale.

6. Indicators relating to Profile of Potential Money Mule or Scam Victims

(a) The sender does not appear to be familiar with digital asset technology or online custodial wallet solutions. Such persons could be money mules recruited by professional money launderers, or scam victims turned mules who are deceived into transferring illicit proceeds without knowledge of their origins;

(b) A customer significantly older than the average age of platform users opens an account and engages in large numbers of transactions, suggesting their potential role as a digital asset money mule or a victim of financial exploitation of the elderly;

(c) A customer being a financially vulnerable person, who is often used by drug dealers to assist them in their trafficking business; and

(d) A customer purchases large amounts of digital assets not substantiated by available wealth or consistent with the customer's historical financial profile, which may indicate money laundering, a money mule, or a scam victim.

Part II (A): Red Flag Indicators for Labuan Non-Profit Organisations (Labuan NPOs) to Screen Potential Donors

This list outlines red flag indicators for Labuan Non-Profit Organisations (Labuan NPOs[1]) to consider when screening potential donors as part of their "Know-Your-Donor" (KYD) process. Ensuring that donations are sourced from legitimate and transparent origins is a critical component of safeguarding the financial integrity and reputation of Labuan NPOs. The indicators provided are intended to assist Labuan NPOs in identifying and addressing potential risks associated with donations received by the Labuan NPOs that may be linked to terrorism financing (TF), criminal activity or other illicit purposes.

1. Indicators Relating to Donor's Identity and Background

(a) Donations originating from individuals or entities located in jurisdictions with known ties to terrorism or prevalent TF;

(b) Donors with known affiliations to groups or activities associated with terrorism or criminal organisations;

(c) Donors identified as Politically Exposed Persons (PEPs), or closely associated with PEPs, that potentially exposed to higher risk of involvement in corruption, bribery or illicit financial activities;

(d) Donors providing false, incomplete, or fraudulent identification or documentation to conceal their true identity or origin;

(e) Donors unwilling or unable to provide adequate documentation or be transparent regarding their identity, source of funds or the purpose of the donation; and

(f) Donors providing inconsistent contact information, financial details, or other identifying information across multiple donations made.

2. Indicators Relating to Donor's Source of Funds

(a) Donations coming from individuals or entities directly listed on terrorism watchlists, or whose funds are suspected to be linked to terrorist organisations;

(b) Donations coming from sources or financial institutions that cannot be easily traced or verified;

[1] Labuan Non-Profit Organisations (Labuan NPOs) refer to Labuan charitable foundations and Labuan charitable trusts.

(c) Donors contributing large sums or assets with no clear explanation, or the source of funds is highly obscure;

(d) Donors making large, unexplained cash donations or deposits into the Labuan NPO's account, particularly from high-risk jurisdictions;

(e) Donors providing in-kind donations that could potentially have a hidden or disguised value, complicating the traceability of the donation; and

(f) Large or frequent donations made anonymously, or through third parties, making it difficult to trace the origin or purpose of the funds.

3. Indicators Relating to Donation Amount and Patterns

(a) Donors making unusually large or repeated donations disproportionate to the size and operational needs of the Labuan NPOs;

(b) Fluctuating or sudden changes in donation patterns, such as a significant increase in donations shortly before a major event or after an international crisis, especially when these donations are not linked to any immediate and visible charitable response;

(c) Donors contributing from multiple international locations with no apparent link to the Labuan NPOs' declared mission or region of operation, particularly when these regions are known for terrorism activity;

(d) Donors contributing through complex banking arrangements or financial networks, especially transfers from abroad;

(e) Donors attaching conditions to their contribution or explicitly request that portion of the donation be returned to them or redirected to their preferred regions or individuals; and

(f) Donors providing funds on the condition that the Labuan NPOs engage certain people or organisations with known link to high-risk regions to handle work or projects.

Part II (B): Red Flag Indicators to Identify the Misuses of NPOs

NPOs are targeted by terrorist entities due to their ability to legitimately access materials, funds and networks. Terrorist organisations may exploit NPOs, including Labuan NPOs to raise and move funds, provide logistical support, recruit members, or provide a veil of legitimacy for their operations. The following red flag indicators reflect potential cases of terrorism financing (TF) or NPOs' involvement in TF. These indicators can assist Labuan entities to better identify and mitigate suspicious NPOs' activity potentially linked to TF.

1. Indicators Relating to Founder/Settlor or Employee/Volunteer

(a) The founder/settlor, employees or volunteers located in high-risk jurisdictions known to support terrorism or have been identified as TF hubs;

(b) The founder/settlor, employees or volunteers with link to individuals or entities listed on terrorism watchlists;

(c) The founder/settlor, employees or volunteers affiliated with known terrorist groups influencing the operations and decision-making of the NPOs;

(d) The founder/settlor, employees or volunteers affiliated with unregistered charitable organisations that link to terrorist groups or originated from high-risk jurisdictions; and

(e) Use of fake or fraudulent identification by employees or volunteers to gain employment within the NPO for purposes of facilitating TF.

2. Indicators Relating to NPO's Transactional Activities

(a) Transactions that are disproportionately large or complex compared to the size or nature of the NPO's activities;

(b) Discrepancy between the NPO's financial activities and its declared mission or charitable objectives, suggesting funds may be misused or diverted for illicit purposes;

(c) Use of crowdfunding or social media platforms to raise funds, which are later suspended or redirected to high-risk areas;

(d) Fundraising events used to raise substantial amounts, only for the funds to be transferred through unauthorized third parties or into regions known for terrorist activity;

(e) Funds raised by the NPO diverted for personal use or transferred to accounts linked to terrorism;

(f) The NPO providing unclear justifications and refraining from submitting sufficient documentation when the financial institution requests information regarding transfers to high-risk locations or entities;

(g) The NPO unable to explain the end-use of its funds/resources when requested; and

(h) The NPO resorting to complex banking arrangements or financial networks that are not necessary for its transactions, especially for transfers abroad.