GUIDANCE NOTE ON RED FLAG INDICATORS FOR LABUAN DIGITAL FINANCIAL SERVICES

1.0 Introduction

1.1 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.

1.2 The Guidance Note on Red Flag Indicators for Labuan Digital Financial Services (the Guidance Note) is applicable to a Labuan Reporting Institution (Labuan RI) undertaking digital financial services including dealing with digital assets. The Guidance Note complements and is to be read together with the following Guidelines and Guidance Note:

(i) Guidelines on Anti-Money Laundering, Countering Financing of Terrorism, Countering Proliferation Financing and Targeted Financial Sanctions for Labuan Key Reporting Institutions (AML/CFT/CPF and TFS for Labuan KRIs); and

(ii) Guidelines on Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) - Capital Markets and Other Business Sectors and Guidance Note on Anti-Money Laundering and Counter Financing of Terrorism for Labuan Specified Entities.

1.3 The Guidance Note is intended to provide a Labuan RI with red flag indicators associated with digital assets. It is imperative for the Labuan RI to establish internal criteria based on the red flag indicators in identifying and reporting suspicious activities involving digital assets.

2.0 Guidance

2.1 A Labuan RI may utilise the red flag indicators associated with digital assets provided in this Guidance Note, in addition to indicators from other corresponding competent authorities, supervisory authorities and international organisations.

2.2 Internal criteria of red flag indicators are required to be established by a Labuan RI to detect suspicious transactions.

2.3 A Labuan RI must consider submitting a suspicious transaction report when any transactions or attempted transactions involving digital assets match the Labuan RI's list of red flag indicators.

2.4 The list of red flag indicators is not exhaustive and subject to be updated from time to time to ensure the indicators are aligned with the evolving techniques, which is influenced by the new technologies and landscape of digital financial services.

2.5 The **Appendix** which outline the red flag indicators is accessible on Labuan FSA's website at https://www.labuanfsa.gov.my/amlcft/guidelines-directives-circulars.

Labuan Financial Services Authority
21 June 2024

List of Red Flag Indicators

The list of red flag indicators is specific to the inherent characteristics and vulnerabilities associated with digital assets. They are neither exhaustive nor applicable for every transaction. Therefore, it is crucial not to consider any of the indicators in isolation, as combination of multiple indicators can indicate potential money laundering and terrorist financing exposures in a broader context.

1. Indicators Relating to Customer Due Diligence Process

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

(ii) 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;

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

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

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

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

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

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

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

(vi) 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

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

(ii) Multiple high-value transactions; and

(iii) 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

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

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

(iii) 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;

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

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

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

(vii) 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;

(viii) 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

(ix) 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 obscure funds flow with a digital asset service provider's infrastructure.

4. Indicators Relating to Technological Features

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

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

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

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

(v) 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;

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

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

5. Indicators Relating to Geographical Risks

(i) 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;

(ii) 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;

(iii) 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

(iv) A customer sets up offices in or moves offices to jurisdictions that have no regulations 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

(i) 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;

(ii) 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;

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

(iv) 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.