RED FLAG INDICATORS FOR DIGITAL PAYMENT TOKEN SERVICE PROVIDERS

General Comments

The list of situations given below is intended to highlight some basic ways in which money may be laundered or used for TF purposes. While each individual situation may not be sufficient to suggest that ML/TF is taking place, a combination of such situations may be indicative of a suspicious transaction. The list is intended solely as an aid, and must not be applied as a routine instrument in place of common sense.

The list is not exhaustive and may be updated due to changing circumstances and new methods of laundering money or financing terrorism. Payment service providers are to refer to STRO's website for the latest list of ML/TF red flags[1].

A customer's declarations regarding the background of such transactions should be checked for plausibility.

It is not unreasonable to proceed with caution any customer who is reluctant to provide normal information and documents required routinely by the payment service provider in the course of business relations or when undertaking any transaction without an account being opened. Payment service providers should pay attention to customers who provide minimal, false or misleading information or, when establishing business relations or undertaking a transaction without opening an account, provide information that is difficult or expensive for the payment service provider to verify.

Transactions Which Do Not Make Economic Sense

i) Transactions that cannot be reconciled with the usual activities of the customer.

ii) A customer relationship with the payment service provider where a customer has a large number of accounts with the same payment service provider, and/or makes frequent transfers between different accounts.

iii) Transactions in which assets are withdrawn immediately after being deposited, unless the customer's business activities furnish a plausible reason for immediate withdrawal.

iv) Transactions which are incompatible with the payment service provider's knowledge and experience of the customer in question.

v) Unnecessary routing of funds through multiple intermediary payment service providers, FIs or persons.

vi) Substantial increase(s) in account activity by a customer without apparent cause, especially if value transfers are made to an account/ person not normally associated with the customer.

vii) Concentration of payments where multiple senders make value transfers to a single individual's account.

[1] The website address as at 2 April 2024: https://www.police.gov.sg/Advisories/Crime/Commercial-Crimes/Suspicious-Transaction-Reporting-Office

viii) Transactions which lack an apparent relationship between the sender and beneficiary, and/or personal transfers of value sent to countries or jurisdictions that have no apparent family or business link to customer, and/or the customer has no relation to the country where he/she sends/receives the value transfer and cannot sufficiently explain why value transfer is sent there/received from there.

ix) Large amounts of funds or DPT deposited into an account, which is inconsistent with the source of funds and/or wealth of the customer.

x) Transactions which, without plausible reason, result in the intensive use of what was previously a relatively inactive account, such as a customer's account which previously had virtually no personal or business related activities, but is now used to received or disburse unusually large sums which have no obvious purpose or relationship to the customer or his business.

Transactions Involving Large Amounts

i) Frequent transactions involving large cash amounts or a high value of DPT that do not appear to be justified by the customer's business activity or background.

ii) Customers making large and/or frequent value transfers, mostly to individuals and firms not normally associated with their business.

iii) Customers making large value transfers to persons outside Singapore with instructions for payment in cash.

iv) Numerous transactions by a customer, especially over a short period of time, such that the amount of each transaction is not substantial, but the cumulative total of which is substantial.

v) Customers who together, and simultaneously, use separate branches to conduct large (cash) transactions.

vi) Customers whose transactions involve counterfeit notes or forged instruments.

vii) Large and regular payments of funds or DPT that cannot be clearly identified as bona fide transactions, from and to countries associated with (a) the production, processing or marketing of narcotics or other illegal drugs or (b) other criminal conduct.

viii) Fund or value transfers made to a single person by a large number of different persons without an adequate explanation.

ix) Customers who receive frequent and/or large transactions from virtual asset kiosks.

Tax Crimes Related Transactions

i) Negative tax-related reports from the media or other credible information sources

ii) Unconvincing or unclear purpose or motivation for establishing business relations or conducting business transactions in Singapore.

iii) Originating sources of multiple or significant deposits/withdrawals are not consistent with declared purpose of the account.

iv) Inability to reasonably justify frequent and large fund or value transfers that originate from or are being made to a beneficiary in a country or jurisdiction that presents higher risk of tax evasion.

v) Customers send or receive (regular) payments from persons in countries which are regarded as “tax havens” or which are known to be exposed to risks such as drug trafficking, terrorism financing, smuggling. Amounts transacted are not necessarily large.

Other Types of Transactions

i) The customer fails to reasonably justify the purpose of a transaction when queried by the payment service provider.

ii) Transactions for which customers fail to provide a legitimate reason when asked.

iii) Account activity or transaction volume is not commensurate with the customer’s known profile (e.g. age, occupation, income).

iv) Account has undergone a long period of dormancy, followed by a large volume or velocity of transactions.

v) Transactions with persons in countries or entities that are reported to be associated with terrorism activities or with persons that have been designated as terrorists.

vi) Frequent changes to the customer’s address or authorised signatories.

vii) When a young person opens an account and either withdraws or transfers the funds within a short period, which could be an indication of terrorism financing.

viii) When a person receives funds or DPT from a religious or charitable organisation and exchanges the funds or DPT, utilises the funds or DPT for purchase of assets or transfers the funds to another person within a relatively short period.

ix) Transactions where funds are deposited from or withdrawn to virtual asset addresses with direct or indirect links to known suspicious sources (e.g. darknet marketplaces, mixing/tumbling services, or addresses associated with illegal activities such as ransomware attacks).

x) Transfers from one or more senders often from different countries and/or in different currencies to a local person over a short period of time.

xi) Periodic transfers made by several people to the same person or related persons.

xii) False information during the identification process/ lack of co-operation. Use of third parties to effect funds or value transfers aimed at concealing the sender and/or receiver of moneys.

xiii) The customer uses intermediaries that are not subject to adequate AML/CFT laws.

xiv) No or limited information about the origin of funds or DPT.

xv) Funds or DPT used by a customer to settle his obligations are from a source(s) that appears to have no explicit or direct links to the customer.

xvi) Banknotes brought by customer are in small denominations and dirty; stains on the notes indicating that the funds have been carried or concealed, or the notes smell musty; notes are packaged carelessly and precipitately; when the funds are counted, there is a substantial difference between the actual amount and the amount indicated by the customer (over or under).

xvii) Transactions that are suspected to be in violation of another country's or jurisdiction's foreign exchange laws and regulations.

Customer Behaviour

i) Use of Virtual Private Network ("VPN") and/or The Onion Router ("TOR") to access his online account.

ii) Customer registers for an account using an encrypted, anonymous or temporary email service.

iii) Frequent changes in the customer's identification information, such as home address, IP address or linked bank accounts/wallet addresses.

iv) Customer shows uncommon curiosity about internal systems, controls and policies.

v) Customer is overly eager to provide information or details that are not requested for.

vi) Customer is willing to pay high commission fees for services in comparison to typical rates charged by other payment service providers.