Annex A: Risk indicators for CEF

The following potential risk indicators draw from the experience and data received from jurisdictions across the FATF Global Network, the Egmont Group, and the private sector. These indicators aim to enhance the detection of suspicious transactions relating to CEF. The list is further categorised into various perspectives from account opening to transaction monitoring. The indicators can be relevant to regulated entities, including FIs, VASPs, DNFBPs and other financial and payment institutions.

The existence of a single indicator in relation to a customer or transaction may not alone warrant suspicion of a CEF offence, nor will a single indicator necessarily provide a clear indication of such an activity. However, it could prompt further monitoring and examination as appropriate.

Transaction patterns

- Rapid or immediate, high or low value transactions after opening of an account, inconsistent with the purpose of the account
- Rapid or immediate cash withdrawals or transfers of large amounts following the receipt of a funds transfer in order to empty the account
- Frequent and large transactions, which are inconsistent with the account holder's economic profile (e.g., sudden international transfers, withdrawals of cash performed through payment cards at foreign ATMs, large purchases of VA or goods to be exported abroad, or payments in favour of unlicensed foreign MVTS)
- Transfers of funds to and from high-risk money laundering jurisdictions
- Large frequent transactions with recently established companies and/or whose main activities are not consistent with the activities carried out by the beneficiary or have a general purpose
- Small payment to a beneficiary, which once successfully completed, is rapidly followed by larger value payments to the same beneficiary
- Round value amount purchases that are frequent and/or in large amounts, which can indicate gift card purchases

Customer transaction instructions and remarks

- A customer transaction requests for additional payments immediately following a successful payment to an account not previously used by the customer to pay its suppliers/vendors. Such behaviour may be consistent with a criminal attempting to issue additional unauthorised payments upon learning that a fraudulent payment was successful
- A customer's seemingly legitimate transaction instructions contain a different language vernacular, timing, and amounts than previously verified transaction instructions.
- Transaction instructions include markings, assertions, or language designating the transaction request as "Urgent", "Secret" or "Confidential"

- A customer presents poorly formatted messages / emails (spelling and/or grammar mistakes) as justification of a transaction.

- Transaction instructions direct payment to a known beneficiary; however, the beneficiary's account information is different from what was previously used
- The intended beneficiary in the transaction description and the name of the account holder known to the beneficiary bank are inconsistent
- Transfers ordered by natural persons (alleged investors) with no financial experience and expertise, in favour of companies (in many cases established in high-risk jurisdictions) with reasons for payments related to investments and financial products
- Counterparties incommensurate with the business/company name of the account might suggest which may provide cover for the movement of large amounts of funds internationally (e.g., the company reported as a furniture company made multiple large transfer to a company named as petroleum trading company)
- Transactions conducted with device time zone mismatch

Suspicion in account holder's profile

- Account holder is unwilling or unable to pass CDD checks
- Account holder is unfamiliar with the source of the funds moving through their account or claiming they are transacting for someone else
- Frequent changes of legal entities'/sole proprietorships' names using foreign expressions and terminology
- The customer shows to have inadequate knowledge on the nature, object, amount or purpose of the transaction/s or relationship or provides non-realistic, confusing or inconsistent explanations, which drive to the suspicion that the customer is acting as a mule.

Suspicion in account user's identity

- The user is attempting to conceal their identity by using shared, falsified, stolen or altered identification (address, telephone number, email)
- Frequent changes of contact details, phone numbers, email addresses after opening of the account
- E-mail addresses that do not seem compatible with the name of the account holder, or a pattern of similar email addresses seen across multiple accounts
- Irregularities in customer profile particulars, such as shared credentials (e.g., shared by two or more users) with other accounts
- Abnormalities identified via online behaviour, such as hesitation inputting data, keystroke delays, signs of automation, multiple failed login attempts, etc
- Accounts relating to entities who could be expected that they are no longer active in the jurisdiction (e.g., overseas students' account sold when completed study)

- IP addresses or GPS coordinates originating from high-risk money laundering jurisdictions
- Use of virtual private networks (VPNs), compromised devices (such as IOT devices), and hosting companies that may mask a user's IP address
- Multiple IP addresses or electronic devices associated with a single online account
- Single static IP address or electronic device associated with multiple accounts of various account holders
- Remote desktop connection access to an account through computer ports used by applications such as TeamViewer etc. which prevents the true device and location to be seen
- Accounts operated with excessively quick keystrokes or navigation suggesting possible bot control

Adverse information on the account holder

- Presence of material relevant and verifiable negative news on customer or counterparties, e.g., account held by a known or suspected previous victim of scam, mule, or identity takeover activity
- Fraud report or recall from a correspondence institution, or other 3rd party fraud databases
- Presence of wire transfers' recall requests
- Presence of adverse information provided by FIUs or LEAs about persons involved in a transaction

VA transactions

- Sending/receiving large volumes or high frequency low amounts worth of VAs to unhosted wallet addresses; or addresses associated with darknet marketplaces, child sexual abuse material platforms, cyber exploit marketplaces, ransomware groups, mixing/tumbling services, high-risk jurisdictions, gambling sites, and scammers
- Maxing out daily funding limits at Bitcoin ATMs
- No documents proving the origin of VA or of the money converted in crypto-assets
- Transfers of VAs to wallets linked to illegal activities on the dark web (e.g., terrorism, child pornography, narcotics, etc)
- Transactions involving more than one type of VAs, particularly those that provide higher anonymity
- Abnormal transaction activity of VAs from peer-to-peer platform associated wallets with no logical business explanation

Other

- Mismatch of account number and name of the holder of the account

- The user is seen on the phone or accompanied by an individual through Closed Circuit Television (CCTV) and being instructed or coached during the transaction
- Beneficiary companies manage Internet Web Sites providing trading/investment services, in many cases not authorised or listed by the domestic Supervisory Authority