ශ්‍රී ලංකා මහ බැංකුව
இலங்கை மத்திய வங்கி
CENTRAL BANK OF SRI LANKA

මූල්‍ය බුද්ධි ඒකකය
நிதியியல் உளவறிதற் பிரிவு
FINANCIAL INTELLIGENCE UNIT

අංක 30, ජනාධිපති මාවත, කොළඹ 01, ශ්‍රී ලංකාව
இல. 30, சனாதிபதி மாவத்தை, கொழும்பு - 01, இலங்கை
No. 30, Janadhipathi Mawatha, Colombo 01, Sri Lanka

Ref: 37/03/009/0002/025

February 14, 2025

To: Compliance Officers of Financial Institutions

Dear Compliance Officer,

Red Flag Indicators – No. 01 of 2025
Red Flag Indicators on Large Scale Scam Operations

Please find the attached Red Flag Indicators, No. 01 of 2025 relating to the Large Scale Scam Operations.

Yours faithfully,

Director,
Financial Intelligence Unit

011-2477125
011-2477509
011-2477692
011-2477708
flu@cbsl.lk
dflu@cbsl.lk
www.flusrilanka.gov.lk

Red Flag Indicators on Large Scale Scam Operations

The following concerns were observed during investigations conducted by the Law Enforcement Agencies into the recent high-profile scams perpetrated through call centers operating locally while networking in foreign/ domestic nationals.

The operational set-up

- Major commercial complex situated in Colombo has served as the main center of operations.
- These centers have employed young individuals who are proficient in the use of computers, phones and the internet. They have been allocated to separate sections to handle different geographical areas, globally.
- The interactions between the employees have been restricted and nicknames are given for the identification of these individuals.

How is the scam executed?

- Scammers often target foreign nationals in these fraudulent activities.
- They contact the victims via phone and inform them that their bank account has been frozen due to some reason.
- After that they force victims to deposit/transfer a certain amount of money to recover the account.
- Due to the urgency or fear created by the situation, the victims end up transferring money.
- The calls are made using a phone application, so that the phone numbers appear to be from a foreign country.
- These scammers force victims to deposit/transfer money from foreign nationals' time to time, providing various reasons each time.
- To build trust with foreigners, scammers provide fraudulently prepared bank documents, IDs etc.

- When making calls, scammers use nick names given by the entity to hide their identity.

Red Flag Indicators

Accordingly, the financial institutions are cautioned to be extra vigilant about the following 'red flag' indicators.

- Accounts opened under different names, but using the same contact details and/or same correspondence address
- Multiple accounts opened by the same person but with slightly different details, such as alternate names, addresses or phone numbers
- Receiving significant volume of funds that do not match with the declared profile of the account holder
- Failure to provide clear information about the source of funds
- Receiving transfers or deposits from unknown or unrelated individuals, especially if there is no legitimate reason for these transactions
- Receiving multiple foreign remittances without any valid or apparent reason
- Failure to provide valid documents for inward remittances
- Sudden changes in account signatories or individuals authorized to access or manage funds without reasonable justification
- Newly opened accounts showing large or complex transactions that don't align with expected behavior for a new customer
- Any third-party complaint received quoting that a particular account is being used for collecting funds fraudulently