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: 37/09/010/0002/024

August 06, 2024

To: Compliance Officers of Financial Institutions

Dear Compliance Officer,

Red Flag Indicators – No. 03 of 2024
Red Flag Indicators on Large Scale Scam Operations

Please find the attached Red Flag Indicators, No. 03 of 2024 relating to the recently reported large scale scam operations.

Yours faithfully,

Director
Financial Intelligence Unit

☎ 011-2477125
011-2477509
011-2477692
011-2477708
fiu@cbsl.lk
dfiu@cbsl.lk
www.fiusrilanka.gov.lk

Red Flag Indicators on Large Scale Scam Operations

The followings were revealed in the investigations conducted by the Law Enforcement Agencies into the recently reported large scale scams operated by way of call centers functioned by criminal cartels, including several foreign nationals.

The operational set-up

The centers are operated largely:

- through the deployment of foreign nationals who are resident in Sri Lanka bearing 'Tourist Visa' and locals who are recruited through deceptive job postings or targeting more vulnerable category of population driven by the need for employment;
- from central locations such as boutique hotels, apartments taken on a short-term lease by paying higher rentals than the market prices in the areas of tourists' attraction such as Colombo, Kandy, Negombo and Chilaw;
- by setting up necessary equipment such as computers, phones with caller ID capabilities, high-speed internet.

How is the scam executed?

- Scammers either publish or circulate false advertisements to sell some items, make a fake job offer or require the victim to complete some tasks on internet or make a fake proposal to commence an affair and etc.;
- Social media platforms such as Facebook, WhatsApp, Telegram, Skype, WeChat were used to connect and build trust with the victims;
- Sometimes, sense of urgency or fear is created to compel the victim to act quickly and without rational thinking.
- Initially, small amounts are deposited to victims' accounts to induce them;
- In certain instances, fraudulent cryptocurrency investment wallets/platforms were used to attract significant amounts of funds into scammers accounts.

How are the financial operations being carried out?

- Create fake applications and hyperlinks to access and steal confidential secure information sent to persons such as One-Time Password (OTP), Personal Identification Number (PIN), or Card Verification Value (CVV);
- Use a network of intermediary accounts opened through identity theft or using third party accounts on the basis of paying an incentive for account opening or commission on the funds collected into the account, to launder the stolen funds and obscure the money trail;
- Ultimately, convert funds into cryptocurrencies to make tracing difficult.

Red Flag Indicators

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

- Accounts opened by foreign nationals bearing 'Tourist Visa';
- Accounts which are apparently operated by a third party other than the original owner;
- Account of a local person being operated by a foreign national;
- Accounts opened under different names, but using the same contact details and/or same correspondence address;
- Attempts to open accounts using forged identity documents;
- The account holder cannot be contacted or every time a third party introduced as a relation, is answering through the given contact details;
- Receiving significant volumes of funds that do not match with the declared profile of the account holder;
- Attempts to remit significant volume of funds out of the country without complying with the foreign exchange regulations;
- If the customer says he/she has to send large/ unusual/ repetitive sums of money to a third party while insisting on keeping confidentiality;

- A customer appears to be unduly influenced to make transactions by a third party;
- Repetitive account withdrawals or payments done from a different geographical location inconsistent with the customer's address;
- The account withdrawals are often done through other bank's ATM machines;
- Fake/fraudulent/suspicious messages sent by third parties by giving the appearance as it is from a financial institution;
- Any third-party complaint received quoting that a particular account is being used for collecting funds fraudulently.