Press Release
28.03.2024

Directorate of Enforcement (ED), Hyderabad has provisionally attached Rs. 32.34 Crore lying as balance in 580 bank accounts under the provisions of Prevention of Money Laundering Act (PMLA), 2002 in a case relating to a part-time job scam in the guise of review and ratings of websites, hotels, resorts, etc.

ED initiated investigation on the basis of FIR registered by the PS Cyber Crime, Hyderabad under various sections of Information Technology Act and IPC, 1860 against unknown persons. During investigation, it was revealed that more than 50 related FIRs have been registered at various police stations spread across the country in relation to the part-time job scam.

ED investigation revealed that cyber scamsters would approach gullible persons on Whatsapp & Telegram apps and lure them by offering part-time jobs by performing simple tasks of giving 5-star ratings to tourist websites, hotels, resorts, tourist destinations, etc. with daily income ranging between Rs. 1000-1500. The scamsters used to collect basic details and ask the victims to join certain Whatsapp & Telegram groups using links provided by them, where the associates of scamsters would speak highly of the jobs and post thanks messages showing high income for gaining trust of the victims. The victims would then be asked to register on bogus websites/ android apps using their basic details including bank account numbers. For further luring them, the scamsters would even offer e-money/tokens worth Rs. 10,000 on the e-wallets on the bogus websites and apps. The victims were asked to deposit money to various different bank accounts to top-up their online wallet and start working. The wallet balance would get exhausted with every task set. The commission/ earnings were initially allowed to be withdrawn to the bank accounts to gain trust. Later, the agents on Whatsapp/Telegram would coerce the victims to deposit additional money to work more and earn more.

During the tasks of providing ratings, random pop-ups would appear with premium tasks carrying higher commission/ rewards but requiring more deposit leading to the wallet balances turning negative. Victims were then asked to top up their wallets to continue the ratings tasks. In case of non-payment, the wallet balances were frozen and could not be withdrawn. The premium tasks would pop-up more often requiring additional deposits from victims and the ones who could not pay would be coerced to anyhow deposit the money failing which their entire wallet balance would be forfeited.

Despite completing all tasks, when the victims tried to withdraw money reflecting in their online wallets, the transactions would be declined citing various random reasons and asking for depositing more money as refundable withdrawal fee. Even after some victims deposited such fees, the withdrawals could not be made and the Whatsapp agents would stop communicating.

The main masterminds of the scam operated the bank accounts sitting in UAE and had already collected a large number of bank account kits containing internet banking credentials, debit cards and cheque books with related SIM cards sourced from several middlemen who got the bank accounts opened in the names of shell entities using fake/forged documents or obtained such kits for commission.

ED investigation revealed that the scamsters collected more than Rs. 524 Crore in more than 175 bank accounts, used only for a brief period ranging from 1-15 days and the money would be regularly diverted to other accounts. Money trailing revealed that the scam money collected in these 175 bank accounts were transferred to more than 480 bank accounts and used mainly for purchasing crypto currencies, making hawala payments in India and remitting abroad in the guise of import payments.

Further investigation is under progress.