Press Release
20.11.2025

Directorate of Enforcement (ED), Hyderabad Zonal Office, has provisionally attached bank balances amounting to **Rs. 8.46 Crore** spread across **92 bank accounts**, including that of CoinDCX and a few crypto wallets, under the provisions of the Prevention of Money Laundering Act (PMLA), 2002 in connection with an ongoing investigation in large-scale cyber fraud committed through fake e-commerce platforms and money-making fake mobile applications and websites.

ED initiated investigation on the basis of multiple FIRs registered by the Kadapa Police u/s 420 of IPC, 1860 and Sections 66-C & 66-D of the IT Act against unknown cyber fraudsters. Investigation revealed several other FIRs registered across the country revealing a broader web of similar scams orchestrated through deceptive part-time job schemes and fraudulent investment applications, including the NBC App, Power Bank App, HPZ Token, RCC App, Making App, and several other online platforms.

ED investigation revealed that the scamsters targeted gullible individuals using WhatsApp and Telegram groups, and through bulk SMS campaigns, luring them with promises of high commissions and quick profits. The victims were persuaded to register on fake apps or links purporting to offer investment or e-commerce-based earnings. They were instructed to perform simple tasks such as buying or selling items on fictitious e-commerce websites, after which reward points or earnings would appear in their online wallets. Before participating in any activity, however, the victims were required to deposit money into their app wallets, typically through UPI payments made to bank accounts or VPA IDs linked to shell entities and shared by the whatsapp agents. To gain the trust of investors, the fraudsters initially credited small profits or commissions into their bank accounts, encouraging them to deposit higher amounts for greater returns. Once substantial sums had been deposited, withdrawal attempts by victims would consistently fail.

When victims contacted the helpline numbers or support agents on WhatsApp or Telegram, they were falsely informed that additional payments were required for taxes or other regulatory clearances. Even after making such payments, withdrawals remained unsuccessful. Eventually, the apps crashed, websites became inaccessible, user accounts were deactivated and customer support vanished. Victims were also urged to recruit new members with the promise of higher commissions, further expanding the scam network.

Proceeds of Crime to the tune of Rs. 285 Crore, generated through this scheme, were collected in more than 30 primary-layer bank accounts, used only for short periods ranging from 1 - 15 days, followed by swift transfer to over 80 other bank accounts to minimize the risk of detection or account freeze by banks and law enforcement agencies. A significant portion of the crime proceeds was found to be converted into cryptocurrency or distributed through hawala channels within India.

Money trail analysis revealed that the scamsters frequently purchased USDT (Tether) through peer-to-peer (P2P) transactions on Binance using third-party payments sourced from crime proceeds. They exploited price differentials between crypto exchanges and investigation revealed that sellers on WazirX, Buyhatke and CoinDCX bought USDT at lower rates and sold it to scamsters at marginally higher prices on Binance P2P, accepting third-party transfers from the crime proceeds. Investigation also revealed that the scamsters converted USDT worth Rs. 4.81 Crore through CoinDCX using non-KYC-compliant user accounts and unverified third-party payments.

Further investigation is under progress.