OpenVoiceNews U.S.

Transparent. Unbiased. Yours.

Lucknow Identified as Key Hub in Global Crypto-Linked Cyber Fraud

August 10, 2025

— Categories: Crypto

Download IPFS

Authorities in Uttar Pradesh, India, have uncovered an alarming rise in ‘mule accounts’ used to launder proceeds from international cyber fraud, with Lucknow emerging as a focal point in the illicit network.

The scheme came to light when Ajay, a 24-year-old restaurant waiter from Old Lucknow, was approached by an acquaintance offering ₹20,000 (approximately USD 240) to allow his

bank account to be used for a single day of transactions. Tempted by the easy cash, Ajay agreed. The following day, large sums flowed into his account, quickly withdrawn and handed over to strangers on instructions from intermediaries.

Weeks later, police informed him the funds were linked to a cross-border cybercrime operation. Ajay cooperated with investigators, helping to identify other account holders and local recruiters working in coordination with handlers based in Cambodia, Vietnam, Laos, and Thailand.

Police investigations by Lucknow's Crime Branch and Cyber Cell over the past three months have revealed dozens of mule accounts operated by young locals, many employed in restaurants, small shops, contract work, or studying in college.

Lured by commissions of ₹10,000 to ₹30,000 ($120–USD 360), participants knowingly hand over account credentials and identity documents to local facilitators, often bypassing legitimate Know Your Customer (KYC) checks through forged papers.

According to investigators, encrypted Telegram channels, often in the Chinese language, are used to coordinate transfers. On transaction days, mule account holders are escorted to banks to immediately withdraw large sums received through NEFT, RTGS, or IMPS. The cash is handed to crypto brokers, who convert it into USDT (Tether) via decentralized, non-KYC wallets, with Binance among the preferred platforms.

The illicit funds originate from scams including fake investment schemes, bogus job offers, sextortion, and fraudulent online trading platforms. Victims' payments are funneled into mule accounts, then converted into cryptocurrency and transferred abroad, evading taxation and oversight.

Investigators have noted concentrations of mule accounts in both historic and newly developed areas of the city, including Chowk, Indira Nagar, Madiyaon, Malihabad, Bakshi Ka Talab, Sushant Golf City, Vrindavan Yojna, and the suburbs of Mohanlalganj and Gosainganj.

Around 60 individuals have been detained for questioning in recent months, most of them in their 20s.

"These young people aren't hardened criminals, but their actions enable large-scale fraud," Additional Deputy Commissioner of Police (Lucknow South) Rallapalli Vasanth Kumar told

PTI. He added that many later expressed regret, admitting they had underestimated the legal consequences.

Authorities warn that these mule account operations are connected to the darker side of global cybercrime, cyber slavery rackets in Southeast Asia. Thousands of Indians have reportedly been trafficked or deceived with false job offers, then forced to work in scam centers targeting individuals worldwide, with proceeds funneled back to networks in India.

Despite several successful busts, police admit that the scale and sophistication of these operations make detection difficult. Encrypted communications, decentralized crypto wallets, and disposable accounts leave little traceable evidence.

The Uttar Pradesh Police, working with the Indian Cyber Crime Coordination Centre (I4C) under the Union Ministry of Home Affairs, has created a joint plan to bolster cybercrime enforcement.

At a meeting chaired by DGP Rajeev Krishna on August 6, authorities agreed to establish a dedicated Cyber Crime Centre, form a special unit for crimes against women and children, identify fraud hotspots, and train specialized personnel. Public awareness campaigns will also be expanded.

In a follow-up video conference on August 8 with district police chiefs, the DGP ordered that cyber cells be staffed exclusively by trained officers, directed the full utilization of the National Cybercrime Reporting Portal (NCRP), and set a 15-day deadline for CyTrain enrollment via I4C.