Press Release
04.11.2026

Directorate of Enforcement (ED), Hyderabad Zonal Office has arrested four accused persons, namely Harshil Nayanbhai Raval, Jaswant Singh, Chetan Munjal and Pranav Pithadia, on 03.11.2026 under Section 19(1) of the Prevention of Money Laundering Act (PMLA), 2002 in connection with an ongoing money laundering investigation into a fake call centre scam targeting nationals of the United States (US). The accused persons were produced before the Hon'ble Special Court (PMLA),Nampally, Hyderabad, and the Hon'ble Court has remanded all the four accused to judicial custody.

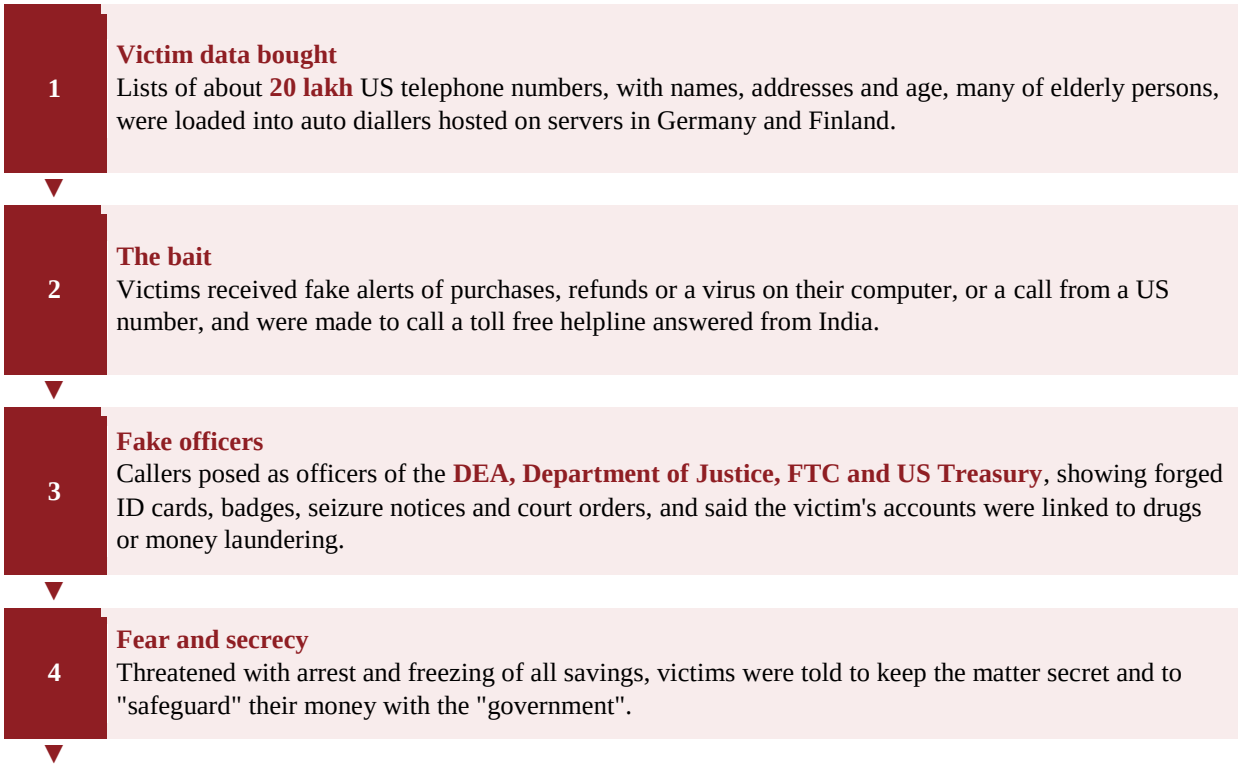
Further, it is pertinent to mention that earlier in the same case, ED had arrested Vikas Nimar on 27.07.2026, Tarachand Nimar on 05.08.2026 and Mohd. Irfan Ansari on 10.08.2026 under the provisions of PMLA, 2002, who are presently lodged in Central Prison, Chanchalguda. With the present arrests, the total number of persons arrested by ED in the case has risen to seven.

Earlier, ED had conducted search operations on 15.09.2026 under Section 17 of the PMLA at four premises in Patiala, Pune and Chandigarh, wherein three live call centres, two at Patiala and one at Pune, were detected with around 220 persons working at the time of the searches. During the searches, digital devices along with cash and records were seized. Forensic examination has so far been completed on 79 digital devices, comprising 65 mobile phones, 13 laptops and computers and one data storage disk, which were found to hold the chats, ledgers, calling data, victim records and crypto wallets of the syndicate.

ED investigation wasinitiated in respect of the scheduled offences of cheating, forgery and criminal conspiracy under Sections 318, 336, 340 and 61 of the Bharatiya Nyaya Sanhita, 2023 (corresponding to Sections 420, 467, 471 and 120B of the IPC, 1860), committed on residents of the US through call centres operated from India, involving impersonation of government officials and use of forged government documents and identity cards.

Investigation has revealed that the syndicate operated organised calling floors (fake call centre) in which the staff worked as dialers, bankers and closers. US nationals were contacted on the pretext of fraudulent purchases or charges on their accounts and were thereafter intimidated by callers impersonating officials of US agencies such as the Drug Enforcement Administration, Department of Justice, Federal Trade Commission and Department of the Treasury, using forged identity cards, badges, official letters and court documents. Under the threat of legal action, the victims were induced to hand over cash and gold to pick-up persons, send cash in parcels through courier services, transfer funds to US bank accounts of money mules and purchase gift cards. The proceeds so collected were converted into Indian Rupees through cryptocurrency and hawala channels and were also routed through accounts in Dubai and other countries.

Figure 1: How the fake call centre cheated US nationals



5	**Money collected** Victims bought **gold bars**, handed over cash to pick up persons, sent cash hidden in parcels by courier, wired money to mule accounts and Dubai companies, deposited cash at **Bitcoin ATMs** or bought gift cards.
▼	
6	**Money brought to India** Dollars were settled at a daily rupee rate and moved to India through **hawala and angadia** tokens, **crypto (USDT)** and accounts in Dubai and Hong Kong, and invested in properties, gold, vehicles and businesses.

On the calling floor: "dialers" made the first contact, "bankers" checked the victim's savings, and "closers" posing as US officers took the money.

Scale recorded: 927 approved collections of about US$ 27.39 million (about Rs. 261 crore) between July 2025 and September 2026.

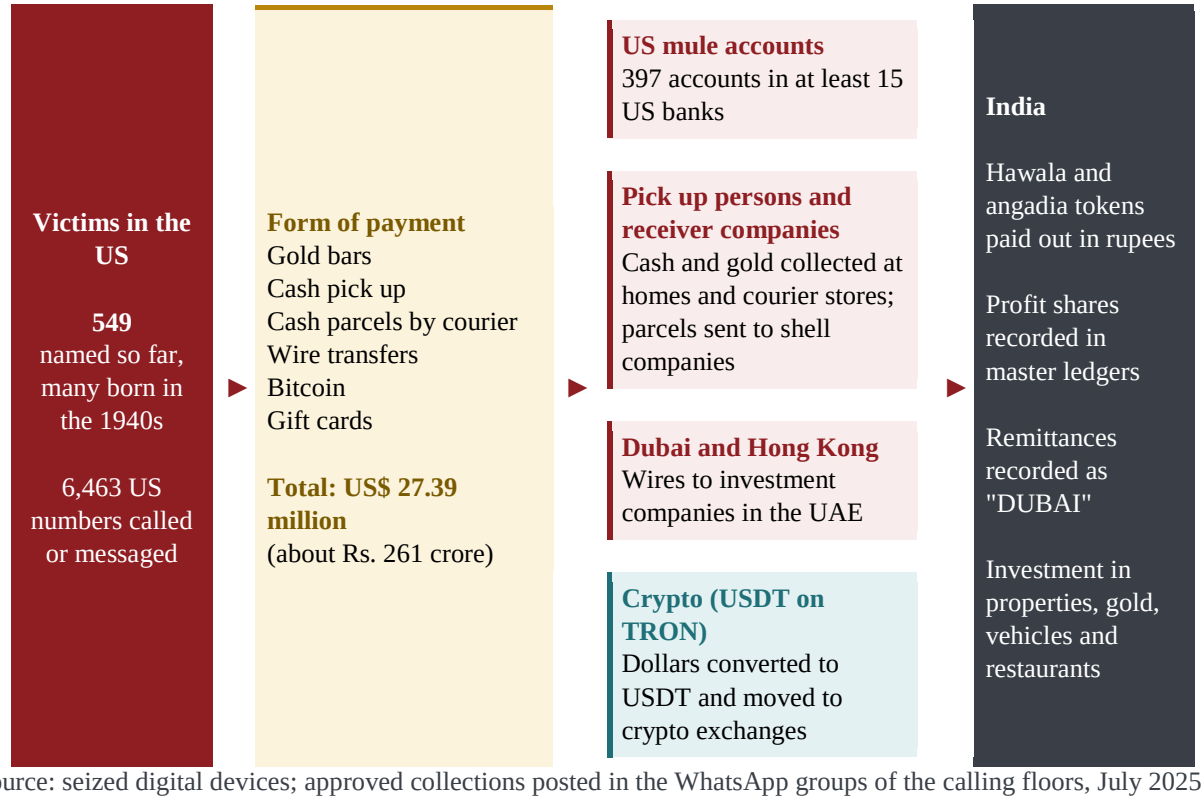
Source: seized digital devices; figures as recorded in the digital evidence.

The digital evidence shows that the syndicate committed **impersonation of US federal officers, cheating by personation, forgery of US government documents and court orders, identity theft and takeover of victims' bank accounts,** mostly against elderly US residents, many of them born in the 1940s. Forged documents recovered include US Department of Justice 'Notice of Seizure & Lien on Financial Accounts', US Treasury 'Assurance Letters', 'Asset Forfeiture' notices, a fake order of a US Court of Appeals and fake legal notices of the Federal Trade Commission and the US Supreme Court. **At least 11 forged identity cards and badges** in the names of 'Special Agents' and officials of the Drug Enforcement Administration, Department of Justice, Federal Trade Commission and Department of the Treasury werealso found in the phone galleries of devices.

The operation spanned **several countries**. Calls were placed from India to residents of the **United States** using lead lists of about 20 lakh persons, US telephone numbers and auto dialler servers hosted in **Germany and Finland**.

Investigation has revealed that proceeds were collected in the **US** and routed through accounts of companies in the **United Arab Emirates (Dubai)** and **Hong Kong**, and through crypto-assets, before reaching **India** through hawala and angadia channels.

Figure 2: Movement of the proceeds of crime



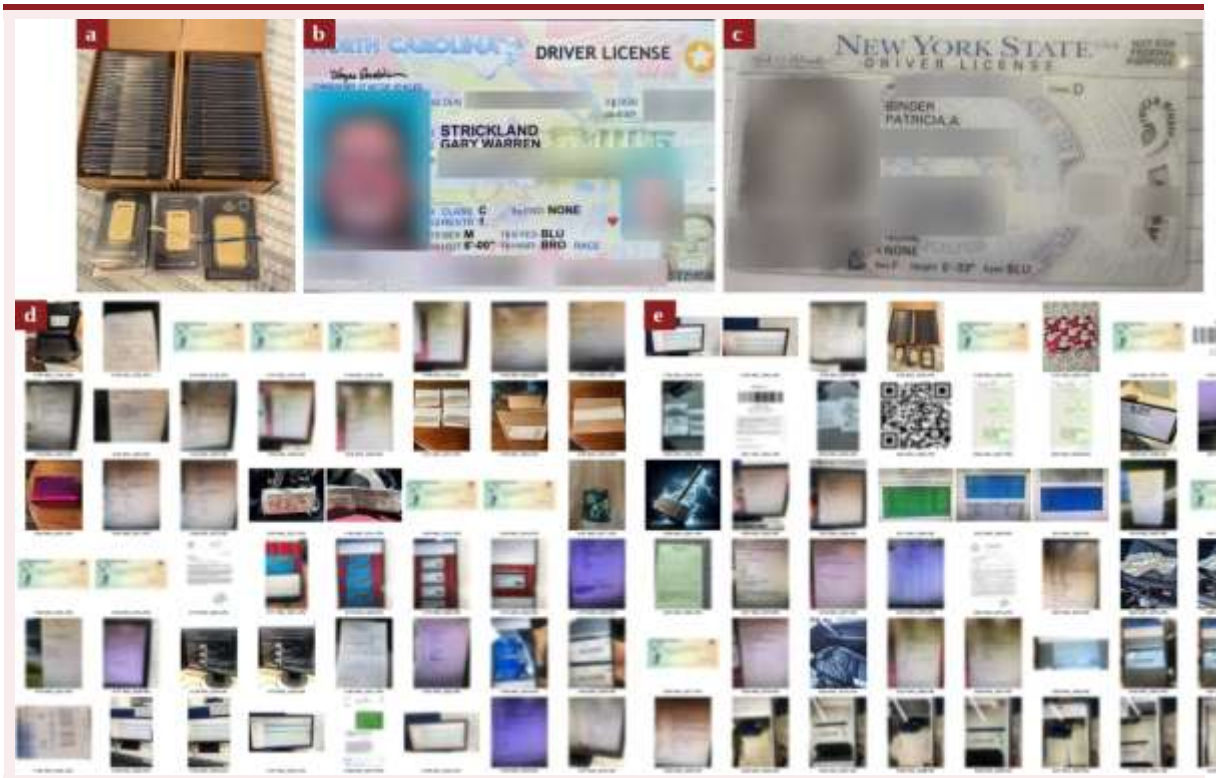
Source: seized digital devices; approved collections posted in the WhatsApp groups of the calling floors, July 2025 to September 2026.

Investigation under PMLA has revealed that Pranav Pithadia was the owner and manager of the Patiala calling floors

(fake call centre), employing 242 staff including 110 dialers, who received the payment approvals and settlements and directed movement of the illegal earned proceeds through US mule accounts and Dubai accounts.HarshilNayanbhaiRaval maintained the master accounts of the operation at fake call centres, recording the profits out of the earning of fake call centres, partners' shares and remittances of PoC to Dubai, and invested the proceeds in properties. Jaswant Singh coordinated cash pick-ups from victims in the US through pick-up teams and parcels, routing the cash to the network for conversion into Indian Rupees through tokens and hawala. Chetan Munjal, a 25% partner of M/s Rabditta Corporates, which runs the Kala Ghoda restaurants which received proceeds of crime of Rs. 23.19 lakh, provided the protection to the call centre and received the funds (out of PoC) for the said call centres.

The WhatsApp groups of the calling floors record **927 'approved' collections of about US$ 27.39 million (about Rs. 261 crore)** between July 2025 and September 2026, received from victims as gold, cash pick-ups, cash parcels sent through courier, wire transfers, Bitcoin and gift cards. The seized devices further record **397 US bank accounts held in at least 15 US banks**, including Wells Fargo (313 accounts), SSB Bank, Bank of America, Thread Bank, Column N.A. and Lead Bank, into which victims were made to wire or deposit money. These accounts were held by recruited money mules, by victims whose accounts had been taken over, or in stolen or synthetic identities; in four cases the online banking log-in details of the victims were also found.

Figure 3: Gold, identity documents and camera roll of a seized phone



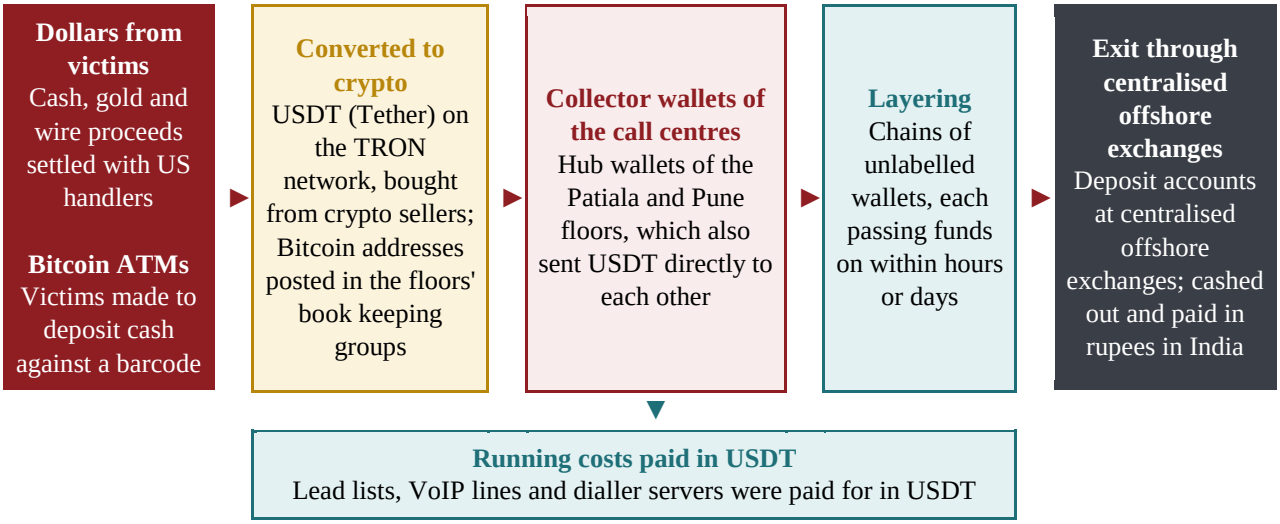
(a) **Boxes of gold bars** photographed on a seized phone; (b) and (c) **US driving licences of victims**, key details blurred; (d) and (e) **contact sheets of the camera roll of a seized phone** showing gold, parcels, US Treasury cheques, gift cards and victim records, personal details blurred

Photographs recovered from the seized digital devices.

The devices also hold the **Social Security Numbers (SSN) of 140 US nationals** (complete numbers in 4 cases and the last four digits in 136), along with their dates of birth, addresses and bank details, photographs of US driving licences and **92 images of identity documents**, which were used to profile victims, to collect cash parcels at courier stores in the names of other persons, and to front US companies used as receivers of the parcels and wires. The persons whose identities were misused are being identified.

Crypto-assets were a major channel for moving the proceeds. Collections were converted into **USDT (Tether) on the TRON network** and into **Bitcoin**, and victims were also made to deposit cash at Bitcoin ATMs. The consolidated analysis of the digital evidence seized during the search has so far identified **549 US nationals** as victims and targets of the syndicate, whose names and particulars were found recorded on the seized devices. Besides, **6,463 US telephone numbers** were called or messaged from the seized phones.

Figure 4: Crypto route of the proceeds



Source: wallet addresses found on the seized devices; public TRON blockchain records.

ED investigation is continuing to identify further Proceeds of Crime, trace the money trail, and ascertain the involvement of other persons/entities in the offence of money laundering.

Further investigation is under progress.