



PRESS RELEASE

23.01.2025

Directorate of Enforcement (ED), Hqrs. Office has provisionally attached Proceeds of Crime (PoC) in the form of 10 immovable properties worth **Rs. 20.69 Crore** (approx.) on 17.01.2025 generated out of various cybercrimes and laundered by cybercrime masterminds Punit Kumar @ Puneet Maheshwari @ John (resident of Moti Nagar, Delhi), and Ashish Kakkar @ Pablo (resident of Greater Kailash, Delhi).

These properties include 9 residential flats in New Delhi and a parcel of agricultural land in Rewari, Haryana held in the name of Deepti, w/o Punit Kumar; Ankur, brother of Punit Kumar; Prashant, cousin of Punit Kumar; Asha Kakkar, mother of Ashish Kakkar and in the name of Punit Kumar himself.

Multiple FIRs have been registered across India against cybercrime fraudsters involved in scams like online gaming fraud, multi-level marketing schemes, and investment scams. Following this, the ED initiated an investigation.

Some common fraud methods used are detailed below.

- **Investment Fraud:** Scammers lure people with promises of high returns through fake apps for share market investments. Initially, they show fake profits in the trading account to gain trust. Once convinced, victims are encouraged to invest larger sums, often in lakhs, with the promise of even higher returns. When victims request their money back, scammers demand additional payments as taxes or processing fees. This cycle continues until the victim stops paying, by which time their funds have been stolen.
- **Part-time Job Fraud:** Scammers post ads on platforms like Facebook, Instagram, and WhatsApp, offering part-time jobs. Victims register through a provided link and pay a small initial amount, like ₹100. After completing a task, they receive a slightly higher amount, such as ₹150, to build trust. Scammers then ask for more deposits, promising even higher payouts. However, when victims attempt to withdraw their earnings, they are told to complete more tasks and pay additional fees. This cycle continues until victims deposit large sums, often in lakhs, only to realize they have been scammed.
- **Online Shopping Fraud:** Scammers attract people with offers of very cheap products found via Google or social media platforms like Facebook and Instagram. Victims receive a purchase link on WhatsApp, register, and pay for the item. The fraudsters then demand additional payments, citing reasons such as customs duties or delivery charges. In the end, the victim loses their money and never receives the purchased item.
- **Fake Loan App Fraud:** Fraudulent loan apps offer small loans to people but charge extremely high interest rates. To recover payments, these apps resort to harassment, including calling the borrower's relatives and making threats of filing FIRs. This pressure forces borrowers to pay huge sums far exceeding the original loan amount.

Modus of money laundering

The investigation revealed that these scams operated through various fraudulent websites and apps (e.g. upbitro.com instead of original upbit.com, betting website www.taj777.com) created by companies based in small island nations like Curacao, Malta, and Cyprus.

These foreign companies and fake apps/websites are connected to bank accounts held in India for collection of POC from the public. The money was then routed through multiple bank accounts in four to five layers to disguise the transactions and hide the source and then transferred out of India under the false pretext of paying for imported goods or services. Those bank accounts of companies and firms which were used for layering crime proceeds are controlled by Ashish Kakkar, Punit Kumar, and their associates.

More than 200 companies were used for layering the POC and those companies were registered in the names of employees of Ashish Kakkar, Punit Kumar, and their associates, such as office boys, drivers, and sweepers. Their signatures were taken on documents and misused to operate the companies and bank accounts. These entities were created on the basis of forged documents in order to have complete control over all the banking transactions of the entities. Registered office premises were rented in the names of these dummy directors. Online verification revealed that the even stamp papers for the rent agreements were also forged.

Siphoning off the PoC through Circular trading

In order to siphon off the POC outside India, Ashish Kakkar and Punit Maheshwari misused Special Economic Zone (SEZ) facilities by obtaining GST registrations and SEZ permissions. They imported highly overvalued goods (overvalued by 5000 times) such as rose oil and solar panel machinery through SEZs like Mundra and Kandla from Dubai, Hong Kong, and China etc and made huge illegal outward foreign remittances abroad against import. Thereafter the same goods were re-exported (without any processing) but no remittance was received against the export. In these circular transactions, same goods were imported and then exported multiple times to siphon off the POC abroad. Ashish Kakkar and Punit Maheshwari ultimately siphoned off **Rs. 4,978 Crore** abroad, laundering the POC obtained from cyber fraud using these circular transactions.

Punit Kumar and Ashish Kakkar were arrested on 03.04.2024 and 02.03.2024 respectively. Further, searches were conducted at 17 places resulting in seizure of approx. 27.50 Kgs of Gold valued at Rs.19.08 Crore, cash amounting to Rs. 75 Lakh, jewelry, incriminating documents and electronic devices containing incriminating data from the premises of Ashish Kakkar, Punit Kumar and their associates.

Further investigation is under progress.