



Press Release
07.10.2026

Directorate of Enforcement (ED), Guwahati Zonal Office-I, has issued a Provisional Attachment Order under the Prevention of Money Laundering Act (PMLA), 2002, provisionally attaching balances aggregating to **Rs. 2.12 Crore** (approx.) lying in 43 bank accounts held with Axis Bank, Bank of India, Federal Bank, IndusInd Bank, Punjab National Bank and State Bank of India, in a case of a cyber fraud committed by way of "digital arrest" of a senior citizen of Guwahati.

ED investigation was initiated on the basis of FIR registered by the Cyber Police Station, CID, Assam, Guwahati, under various sections of the Bharatiya Nyaya Sanhita, 2023 and the Information Technology Act, 2000, against unknown cyber fraudsters.

Investigation has revealed that between September and December 2025, cyber fraudsters impersonating officials of TRAI, Mumbai Crime Branch and the CBI contacted the senior citizen, a resident of Guwahati, falsely convinced that a bank account opened with his Aadhar was involved in money laundering, and placed him under a so-called "digital arrest" through WhatsApp video calls. He was shown fabricated court proceedings and a fake "Digital Arrest Warrant", made to mark his presence every two hours, and threatened with detention under the National Security Act if he disclosed the matter to anyone. Under the pretext of an "RBI inspection" of his family's funds and, later, a fake "bail bond", the victim was coerced into transferring a total of Rs. 2.13 Crore (approx.) in 19 transactions into bank accounts dictated by the fraudsters, for which he liquidated fixed deposits, mutual funds and shares and took loans against his pension account and insurance policies.

Further investigation has revealed that the extorted amount was credited to first-layer "mule" accounts and was immediately split and routed through multiple layers of bank accounts held by individuals, firms and companies across the country. The funds were thereafter withdrawn in cash, converted into digital currency, transferred to payment gateways or moved onward to other accounts, in a deliberate and systematic manner to conceal the trail. The transactions in these accounts were found to be wholly inconsistent with the declared profiles of the account holders, indicating an organised network of mule accounts operated by the cyber fraud syndicate.

By tracing the money trail, ED identified 43 bank accounts through which the proceeds of crime were routed and in which balances were still available. These balances, representing proceeds of crime or the value thereof, have been provisionally attached under Section 5(1) of the PMLA, 2002, so as to prevent their dissipation.

Further investigation is under progress.