Press Release
02.11.2024

Directorate of Enforcement (ED), Hqrs. Office has filed a Prosecution Complaint (PC) on 10/10/2024 before Hon'ble Special Court (PMLA), Bengaluru against 8 accused persons (all arrested by ED) namely Charan Raj C, Kiran S K, Shahi Kumar M, Sachin M, Tamilarasan, Prakash R, Ajith R and Aravindan and 24 related companies in a cybercrime case involving Proceeds of cybercrimes to the tune of **Rs 159 Crore**. All 8 arrested accused are currently under Judicial Custody.The Hon'ble Special Court, Bengaluru has taken cognizance of PC on **29.10.2024.**

ED initiated investigation on the basis of various FIRs registered by multiple Law Enforcement Agencies (LEA) across India. These FIRs allege that some unknown cyber fraudsters enticed innocent individuals into their trap by luring them with schemes involving fake IPO allotments and stock market investments through fraudulent apps, promising high returns. Furthermore, some victims were manipulated under the guise of a fake arrest by Customs and the CBI, ultimately making them transfer huge funds to various shell companies under fake "fund regularization process".

ED investigationrevealed hugenetwork of cyber scams in India, involving fake stock market investments and digital arrest schemes executed primarily through social media platforms like Facebook, Instagram, WhatsApp, and Telegram. Known as "pig-butchering" scams, stock market investment scams entice victims with promises of high returns, using fake websites and misleading WhatsApp groups that appear connected to reputable financial firms. Scammers establish credibility through fake ads and fabricated success stories, ultimately leading victims to invest significant amounts.

Additionally, digital arrest scams involve fraudsters posing as law enforcement officials, intimidating victims into transferring their savings by fabricating scenarios that suggest illegal involvement of the victim.

ED investigation revealed that the scam involves a complex scheme to defraud victims and launder illicit proceeds. Fraudsters obtained hundreds of SIM cards which wereeither linked to the bank accounts of shell companies or were utilized to create WhatsApp accounts. The anonymity afforded by these untraceable SIMs allow scammers to defraud victims with a reduced risk of immediate detection.

ED investigation revealed that scammers have created 24shell companies in various states such as Tamil Nadu, Karnataka, etc.to facilitate the acquisition and laundering of proceeds from cybercrimes. These shell companies, registered mainly at the addresses of coworking spaces (where no actual business presence exists), have used fake bank statements in filings before Registrar of Companies as proof of commencement of business of these companies. In addition to these shell companies, scammers have operated through mule accountsto transfer and conceal Proceeds of Crime (POC) generated from Cybercrimes. The proceeds are ultimately converted into cryptocurrency and transferred abroad.

Numerous companies were incorporated solely for the purpose of layering the POC generated from cyber fraud. Common Directors appear across multiple companies, yet many Directors claimed they were unaware of their roles and were merely figureheads. ED investigation has further revealed that the bank statements used for incorporation of companies were fake.This web of shell companies has enabled the cybercriminals to obscure their identities and disguise the true beneficiaries of these POC.

ED investigation further revealed that certain individuals residing outside India (Hongkong and Thailand) orchestrated a sophisticated cyber fraud and money laundering operation, with the active assistance of their associates located in India to target numerous victims. These overseas scammers have coordinated with individuals in India to create digital signatures, establish shell companies, and serve as dummy Directors to open bank accounts, using fake documents sent via WhatsApp. One of the accused persons, Charan Raj C played a key role in this scheme by recruiting individuals for directorships and managing bank account openings.Shashi Kumar M(accused) has assisted in incorporating several shell companies which became instrumental in collecting and integrating proceeds of crime into the banking system.

During the investigation, a search at the residence ofCharan Raj C led to the seizure of numerous documents and items including a diary with a shell company stamp, handwritten notes detailing bank account openings, cheques and banking documents, identification documents of dummy Directors, and various company-related documents that reveal a network of shell companies involved in investment cyber-frauds.

ED investigation into various companies associated with accused, Kiran S K, Sachin M, and Tamilarasan has revealed extensive involvement in fraudulent activities and money laundering. Kiran S K, linked to several shell companies, had connections with bank accounts of multiple shell entities created by overseas scammers, who submitted fake documents to incorporate these companies. Sachin M, a Director in several firms, admitted to assisting overseas scammers in recruiting dummy Directors and facilitating bank accounts, being well aware of their illegality. WhatsApp communications indicated that he was actively involved in this operation.

Tamilarasan played a significant role in facilitating these activities, collaborating with both Indian and overseas scammers. He assisted in opening bank accounts for shell companies, including Cyberforest TechnologiesPvt Ltd, and knowingly continued these operations despite of knowledge of their connection to cybercrime. Incriminating evidence, such as chequebooks and communication records, further supported the conclusion that these individuals participated in a syndicate that laundered proceeds from cyber frauds across India.

ED investigation reveals use of WhatsApp groups to manage fraudulent banking transactions linked to shell companies involved in cybercrimes across India. Key individuals, including accused persons, coordinated the receipt and sharing of OTPs to authorize transactions. Several companies, including Cyberforest Technology Pvt Ltd and Dreamnova Technologies Pvt Ltd, were used as fronts for layering proceeds of crime to obscure their origins. Directors like Aravindan and Prakash knowingly facilitated these transactions, opening and managing accounts used in frauds.

ED investigation revealed POC totalling Rs.159.70 Crore in illicit funds moved through various accounts, with cryptocurrency used to further conceal and transfer the money abroad.

ED has also frozen proceeds of cybercrime to the tune of Rs. 2.81 Crore in bank account of M/s. Cyberforest Technology Private Limited (accused company in the Prosecution Complaint) under the provisions of Prevention of Money Laundering Act, 2002.

So far, 17 searches have been conducted under PMLA, 2002 at various premises which led to seizure of various incriminating material including various mobile phones, cheque books, company stamps, debit cards, and other digital devices.

Further investigation is underprogress.