

# SPOTLIGHT



# Betting on casinos, crypto

Recovering money swindled from victims in cybercrime cases is already a Herculean task. **Chetan B.C.** reports on the recent trends in Karnataka, which show how cybercriminal networks are colluding with other networks like casinos, online betting apps and cryptocurrency exchanges to launder money, and in many instances, also converting black money to white, complicating the money trails further and posing severe challenges to law enforcement agencies

**A**bout two months ago, Manjunath (name changed), a cab driver from Hyderabad, had the shock of his life when he received summons from the Bengaluru South East Division Cyber Crime Police asking him to appear for questioning in a cyber crime case. “Your response is required regarding a money transaction to your account. Appear before the investigator at the Bengaluru Southeast CEN Police Station,” the summons read.

Manjunath rushed to Bengaluru as he had received the letter late and had already missed the deadline. The police, meanwhile, were preparing to send a team to Hyderabad, but eventually detained Manjunath in Shanthinagar after tracking his location.

“His account had received money transferred by a resident of South Bengaluru, who had been duped by a cyberfraudster in a courier fraud,” the investigator handling the case told *The Hindu*.

A courier fraud or a FedEx fraud is one where cyberfraudsters claiming to call from Customs or one of the law enforcement agencies claiming they had intercepted a courier in their name with contraband, subject them to ‘interrogation’ on video, seek their bank details and siphon off money, or sometimes subject gullible citizens to even “digital arrest”.

Manjunath was summoned as the

**Banks should enforce stricter Know Your Customer protocols and conduct thorough checks while opening accounts**

money siphoned off from the victim in South Bengaluru had landed in his account. However, further investigation revealed that Manjunath's landlord in Hyderabad, one Eshwar, had "borrowed" his account for a transaction to avoid "tax issues", and that is how the money siphoned off from the Bengaluru-based cyber crime victim landed in Manjunath's account.

The police then began pursuing Eshwar, a businessman and a casino enthusiast, suspecting him to be part of a cyber fraudsters' gang. But he was also not.

Investigations found that Eshwar had visited a casino in Sri Lanka after which the transaction was initiated. "During his visit, Eshwar stopped gambling midway and returned to India. He surrendered all the casino chips he had purchased using real money and asked for a refund," the investigator explained. To receive the refund, Eshwar requested Manjunath's bank account details and provided it to the casino. The police connected the dots and concluded that the Sri Lankan casino had links with cyber fraudsters operating in India. The refund was made through proceeds of cyber crime.

## Money laundering networks

This is not an isolated case. Senior police officials say such links between cyber criminal networks and various networks, including hawala, crypto currencies, casinos, online betting apps and the likes, are increasingly common. This indicates how several networks are converging to launder illicit money and in many instances also converting black money to white money.

This has posed serious challenges to law enforcement agencies, as the money trail has become more complex, spread over not just multiple States in the country, but also overseas. As an indication of this, the Directorate of Enforcement (ED), the specialist federal agency to check money laundering and violations of foreign exchange rules, has been joining several cyber crime investigations across the country.

This has complicated an already herculean task of recovering swindled money from cyber crime victims.

Crypto exchanges are secure and transactions are hard to trace, even though technically it is possible. But we cannot freeze a crypto wallet, as current laws do not allow it.

## A SENIOR CID OFFICER

agents representing foreign casinos operate in India. When cybercriminals need to transfer money to their overseas counterparts, they pay casino agents in India using money mules or proceeds from cyber crime. The foreign casino agents then disburse equivalent funds to the fraudsters' partners abroad. Likewise, whenever casinos have to pay someone, like in the above case, there are instances where they have used cyber crime networks to pay them.

## Online betting apps

Recently, the ED summoned over 25 celebrities in connection with a money laundering case registered under the Prevention of Money Laundering Act (PMLA), 2002, related to online gaming platforms.

Pronab Mohanty, Director-General of Police (DGP) and head of the newly formed Cyber Command Unit (CCU), confirmed that several cyber crime investigations have unearthed links to money laundering through online betting platforms. "In many cases, the stolen money was laundered through online betting and cryptocurrency," Mr. Mohanty told *The Hindu*.

Betting applications provide virtual coins or chips in exchange for real money. Winners are paid in cash or through accounts that are untraceable to them by these platforms. Since these gaming apps do not use their nodal accounts to pay winners, there is no proof that a payment was made to a particular user. Such payments are outsourced to cybercriminal networks, who pay winners using proceeds of cybercrimes, often transferring money from victims to the accounts who need to be paid. These cybercriminal networks are reimbursed

with an additional cut later through other means, often abroad and in white. Meanwhile, the money collected from other players by the betting app is legitimate, effectively converting black money into white, an officer explained.

According to the officer, many of these betting apps are unverified. “PlayStore won’t permit such apps. They are floated online and advertised via social media and Telegram channels,” the officer said, advising users to avoid unverified apps and not to install them via APK files.

## The crypto route

Cryptocurrencies are another often chosen avenue to launder proceeds of cyber crimes.

A senior CID officer described how some foot soldiers open wallets on crypto currency exchanges and deposit stolen funds. In return, they receive cryptocurrency equivalent to the amount deposited, which they then transfer to ringmasters abroad.

In other instances, the fraudsters transfer stolen funds into a specific mule account that appears legitimate and holds proper documentation. Using those credentials, they send a large sum of defrauded money to a crypto currency exchange and receive the corresponding cryptocurrency.

“Crypto exchanges are secure and transactions are hard to trace, even though technically it is possible. But we cannot freeze a crypto wallet, as current laws do not allow it. In cases where fraudsters use their own secure wallets not linked to any exchange, it becomes virtually impossible to trace or track subsequent transactions,” the officer said.

Even when the police identify the wallet receiving the stolen funds, they are unable to determine its ownership due to encryption and anonymity.

However, this kind of money laundering is possible due to gaps in our banking system, say cyber crime investigators. Investigators frequently blame the banking system for allowing fraudsters to get away with siphoned funds. According to them, such laundering can be curbed only through a broader and streamlined banking system.

“Banks should enforce stricter Know Your Customer (KYC) protocols and conduct thorough checks while opening accounts. These checks are currently lacking, leading to the creation of lakhs of mule accounts,” said a CID officer. According to data from the Indian Cyber Crime Coordination Centre (I4C), a federal agency coordinating cyber crime investigations in the country, nearly 4,000 mule accounts are created in India every day. Creation of every mule account is a testament to gaps in the banking regulations, officers argue.

Not just that, as per Reserve Bank of India regulations, banks are mandated to monitor suspicious transactions and flag them. However, this rarely happens. These shortcomings are indirectly aiding cyber criminals.

Moreover, banks are slow to respond when police seek information. Data accessed by *The Hindu* shows that major private-sector banks in the State took up to 30 days to reply to police queries in 2024, when the golden hour to freeze an account to prevent the swindled money, proceeds of cyber crimes is around two hours. The Bengaluru City Police's Cybercrime Information Report (CIR) helpline has been a pioneer in this real time intervention. However, it depends on victims reporting crimes to the helpline within the golden hour and the banks also responding and acting with alacrity in the same time window.

In addition, victims face larger problems because of the existence of mule accounts. For example, a fraudster scamming a victim in Karnataka may use mule accounts based in another State to make police investigations more difficult. Likewise, the money withdrawal would occur in a third State, further complicating the trail. "A foot soldier in the third State would withdraw the stolen funds and deposit them with a local money laundering agent. The agent's counterpart in Karnataka would then pay the original fraudster," the officer explained.

**CLASSIFIEDS MART**

**TO ADVERTISE VISIT**  
**[www.thehinduads.com](http://www.thehinduads.com)**  
Contact your nearest Authorised space sellers

## LEGAL NOTICE

[illegible]

**IN THE COURT OF THE  
HON'BLE ADDITIONAL  
SENIOR CIVIL JUDGE: KADAPA  
I.P.No.40 of 2025**

**Nagarapu Naveen Kumar,  
S/o,Nagarapu Narasimulu, aged 29  
years, Hindu, R/A, D.No.2/281-3,  
Nehru Nagar, Chinna Chowk, YSR  
Kadapa District**

**...Petitioner**

**Vs.**

**1) FIBE.O/A., D.No.404, The  
Chambers, Near Ganapathi Mandir  
Chowk, Viman Nagar Road, PVNE,  
Maharashtra.**

**2) CASHE, O/A., 5th Floor, Paville  
House, Off Veer Savark Marg,  
Prabhadhur, Mumbai, Maharashtra.**

**... Respondent No.19 & 21**

**GENERAL PUBLIC NOTICE &  
RESPONDENTS**

The above named petitioner filed the above I.P., Praying the Hon'ble Court to declare him as an indigent person and also for other reliefs. If either respondents or any persons are having objections to appear before the above named court on 02-09-2025 either personally or through their authorized counsel, Failing which the matter will be decided as ex parte.

**By Order of the Court /**


**Sd/- ANDE SUBRAMANYAM, Advocate  
Kadapa Town & District,  
Andhra Pradesh State, India.**

**ANNAMACHARYA INSTITUTE OF TECHNOLOGY & SCIENCES**  
(AUTONOMOUS) Rajampet - 516126, Annamayya Dist., A.P.

**TENDER NOTICE**

Sealed Quotations are invited from reputed companies / suppliers for the supply of equipment, tools and consumables for the establishment of AICTE IDEA Lab at AITS, Rajampet. For details please visit our website: [www.aitsrajampet.ac.in](http://www.aitsrajampet.ac.in) and navigate to the Incubation Center tab. Email: [aitsap@yahoo.co.in](mailto:aitsap@yahoo.co.in) / by post to above address. **Last date: 25-08-2025.**

**Contact : 9100235810. PRINCIPAL**

 **KERALA BANK**  
Kerala State Co-operative Bank

PB.No.6515,  
COBANK TOWERS,  
VIKAS BHAVAN,P.O, PALAYAM,  
THIRUVANANTHAPURAM, PIN-695033

**TENDER NOTICE**

The Kerala State Co-operative Bank invites competitive quotations in E-tender mode from reputed printers for printing and supply of Cheque Books and Demand Drafts. E-tender documents containing specification, terms & conditions etc. can be obtained from e-tenders website of Kerala State Govt. ([www.etenders.kerala.gov.in](http://www.etenders.kerala.gov.in)). **Tender ID: 2025\_KSCB\_784837.1**. Details are also available in the Bank's website: [www.keralabank.com.in](http://www.keralabank.com.in). The Tender Document Download Start Date is 11/08/2025 at 05.55 pm and last date of submission of E-tender is on 19/09/2025 at 6.00 pm

Thiruvananthapuram,  
12/08/2025

(Sd/-) Chief Executive Officer

**कार्यालय अधीक्षण अभियन्ता, सार्वजनिक निर्माण विभाग, वृत्त टोंक**  
 क्रमांक: 1361-65 दिनांक : 31-07-2025


**निविदा सूचना संख्या: 06/2025-26**

राजस्थान के राज्यपाल महोदय की ओर से श्री.आई.आई.एफ. प्रोजेक्ट के अन्तर्गत संगम टोंक के अधीन वृत्त टोंक के विभिन्न सरकारी निर्माण कार्य हेतु श्रेणीम सुधार अभियाना एच.एल.ए. संविध सार्वजनिक निर्माण विभाग राजस्थान जयपुर के उच्च कारा पत्र क्रमांक 12912510 दिनांक 28.03.2025 के अनुसार संगम टोंक की अवधि लिए राजस्थान श्रेणी में सार्वजनिक निर्माण विभाग राजस्थान एच.एल.ए. संविध संगम टोंक के अन्तर्गत विभिन्न कार्य हेतु श्रेणीम सुधार अभियाना एच.एल.ए. संविध तत्वा द्वारा सरकार के अधीक्षक सार्वजनिक/केन्द्रीय लोक निर्माण विभाग/डाक एवं दूर संचार विभाग/रेल्वे इन्स्टीट्यूट एवं पंजीकृत संसदें, जहाँ की राजस्थान सरकार के उपयुक्त श्रेणी संसदें/को के समकक्ष हों, से कराया हेतु ई. टेंडरिंग के माध्यम से निविदाएं पत्र में 2 निर्माण कार्य हेतु जिनकी कुल राशि 12229.65 लाख है, प्राप्ति की जावेगी। निविदा से सम्बन्धित विवरण देब साईट <http://diipr.rajasthan.gov.in> एवं <http://eproc.rajasthan.gov.in> व <http://sppp.rajasthan.gov.in> पर देखा जा सकता है। कार्यकार UBN संख्या निम्नानुसार है।

**NIB code:** PWD2526A2343  
 1. PWD2526WLOB08598  
 2. PWD2526WLOB08599


(एच.एल. मीना)  
 अधीक्षण अभियन्ता स.नि.वि. वृत्त टोंक

**DIPR/C/11167/2025**

THE  HINDU

**Surcharge:**

**Ahmedabad – Rs. 5.00**

  
THE HINDU


## Your feedback will keep us Cleaner, Sharper and Bolder

Call our toll-free number


**1800 102 1878**

Or write to us at

**customercare@thehindu.co.in**




Scan the  
QR code to  
register your  
feedback


THE  HINDU

the hindu **businessline.**

**FRONTLINE**

**SPORTSTAR**

THE  **young world**

THE  **HINDU**



**ଓଡ଼ିଶା ବିଦ୍ୟୁତ୍ ଶକ୍ତି  
ସଂଚାରଣ ନିଗମ ଲିଡ଼**  
( ଓଡ଼ିଶା ସରକାରଙ୍କ ଦ୍ୱାରା ପ୍ରସ୍ତୁତ )



**ODISHA POWER TRANSMISSION  
CORPORATION LIMITED**  
(A Government of Odisha Undertaking)

Regd. Office: OPTCL Tech Tower, Jagathi, Sahed Nagar, Bhubaneswar-751007

---

**EXPRESSION OF INTEREST (EOI)  
FOR AI-BASED INSPECTION AND MAINTENANCE OF  
TRANSMISSION LINES OF OPTCL**

---

**EOI NO.-01 /25-26**

**Dated: 12.08.2025**

On behalf of OPTCL, Director (Operation) invites Expression Of Interest (EOI) from interested firms for providing AI-Based Inspection and Maintenance of Transmission Lines of OPTCL. The detailed requirement of OPTCL for the above is available in OPTCL website (**[www.optcl.co.in](http://www.optcl.co.in)**) along with EOI in elaborated manner and technical requirement.

**Sd/-  
DIRECTOR (OPERATION)**

**HIPR-28/2025-26**

**©/optcl.odisha    ©/optcl\_odisha**