The Indian EXPRESS
JOURNALISM OF COURAGE

OTPs, FASTag, food orders: How digital breadcrumbs are reshaping policing in India

Apps and services designed for convenience have become instruments for tracking individuals in an age where nearly every transaction, message and delivery request leaves behind an electronic fingerprint.

Written by Soumyarendra Barik Follow
New Delhi | Updated: December 24, 2025 06:31 AM IST
5 min read

Kanpur Police arrested Ravindra Soni from Dehradun on November 30

The Indian man who ran the alleged Rs 1,000-crore BlueChip Group con from Dubai was captured in Dehradun last month after around a year on the run. What brought him down was not an old-fashioned police stakeout but a food delivery order.

Ravindra Soni's arrest is one of the most recent examples of law enforcement's increasing reliance on the digital residue of everyday life — one-time passwords, food-delivery logs, e-commerce histories — to trace elusive suspects and dismantle sophisticated criminal networks.

Apps and services designed for convenience have become instruments for tracking individuals in an age where nearly every transaction, message and delivery request leaves behind an electronic fingerprint.

What was the BlueChip con

Soni arrived in Dubai in 2010 after completing his MBA in Delhi. In 2021, he set up the BlueChip Group for trading in forex and commodities such as gold, oil and metals. The group attracted investors from a number of countries including India, UAE, Malaysia, Canada and Japan.

Three years later, investigators found out that Soni was running an elaborate scam and that his company had vanished with millions that people had invested.
After a year on the run from authorities in Dubai, Soni was traced back to India last month. On November 30, police nabbed him in Dehradun as he stood at his doorstep to receive **what he thought was a food order**.

As the investigation progressed, police discovered that Soni had allegedly defrauded numerous investors through multiple investment companies, including BlueChip. They estimated that the scale of the fraud could be as high as Rs 1,000 crore.

How digital residue is becoming key evidence

The BlueChip Group case is not an isolated one. Last May, **in a Rs 5,300-crore GST fraud case**, investigators pieced together a web of fake companies and forged tax credits by analysing data that most people would consider trivial. One-time passwords (OTPs) generated by delivery apps like Swiggy and Zomato, and text alerts from FASTag toll transponders, became central tools in triangulating the movements of suspects who constantly switched phones, SIM cards and hotel identities to evade detection.

The people behind the scam would keep changing their mobile numbers, keeping them switched off most of the time, switching them on only to receive OTPs from delivery apps. This helped police track them down. FASTag was also tapped to track the high-end luxury cars used by these people on the Delhi-Noida-Lucknow route.

This October, while trailing a **Rs 22 lakh cyber fraud**, the Delhi Police dismantled a network of digital fraudsters with the arrest of seven people, following a nine-day operation spanning 1,800 kilometres across four states, by connecting dots across multiple commonly used apps. WhatsApp data revealed the accounts were operating from Malaysia, while digital footprints from delivery platforms like Flipkart, Swiggy, and Zomato helped trace the accused despite frequent location changes.

The fine print in online applications' privacy policy typically has a clause which allows them to share users' personal data with law enforcement agencies. For instance, Zomato's policy states that it may share a user's data with the police when it is necessary to investigate, prevent or take action regarding possible illegal activities or to comply with legal processes.

This shift towards digital evidence is not confined to financial crime. In the United States, prosecutors building a case against the accused instigator of the devastating 2025 Palisades Fire in California cited interactions with ChatGPT — including prompts about sparking fires and AI-generated imagery of dystopian infernos — as part of the evidentiary mosaic linking the suspect to the blaze that consumed more than 23,000 acres and destroyed thousands of homes.

Regulatory changes to tackle crime

According to a government press release from October, the surge in cybersecurity incidents from 10.29 lakh in 2022 to 22.68 lakh in 2024 reflects the growing scale and complexity of digital threats in India. At the same time, the financial toll is becoming more pronounced, with cyber frauds amounting to Rs 36.45 lakh reported on the National Cyber Crime Reporting Portal (NCRP) as of February 2025.

The Department of Telecommunications' (DoT's) recent directive to enforce SIM-to-device binding for messaging platforms reflects a broader shift in how authorities view digital identifiers in law enforcement.

The DoT directed companies such as WhatsApp, Telegram and Signal to ensure that their services are "continuously" linked to the SIM card used to register with them. The department said they must disallow access if the device does not contain a SIM card.

The Centre is drawing powers from the Telecommunication Cybersecurity Amendment Rules, 2025, that were notified in October, to introduce the concept of Telecommunication Identifier User Entity (TIUE) under the scope of telecom regulations. As per the rules, a TIUE (who is not

a licensee like telecom operators) uses telecommunication identifiers — such as mobile numbers — to identify its users.

This essentially means that apps that require a user's phone number to onboard, or register them, can be classified as a TIUE.

While for now, the SIM binding directive has been sent to messaging services, experts believe that the broad definition of a TIUE could also cover food delivery platforms such as Swiggy or Zomato since they too utilise mobile numbers to create user accounts.

Soumyarendra Barik Follow