Ahead of the Fraud Network

Mule account hubs, exposed through VKYC Onboarding data, before they make news

Executive Summary

India's digital onboarding boom has widened the door for fraud. Current systems have done real work, saving ₹9,055 crore and freezing 26.48 lakh mule accounts, but they act only after the damage is done. Fraud rings move too fast for that.

We studied our Video-KYC data, done for leading financial institutions. We analysed the rejection data and mapped fraud and mule account networks across districts.

Here's what we found:

VKYC data as an early signal for mule hotspots:

VKYC rejection data flagged emerging mule and fraud hotspots 2 weeks to 2 months ahead of police or media detection, with our forecasts preceding law-enforcement action or news in 33% of regions.

Page 3,4

A pattern that holds up:

We've seen this pattern, VKYC data flagging districts before they hit official radar, hold across 6 quarters of data. **What stands out: fraud rings don't disappear when enforcement catches up, they relocate.** This whitepaper walks through 2 real examples.

Page 5,6

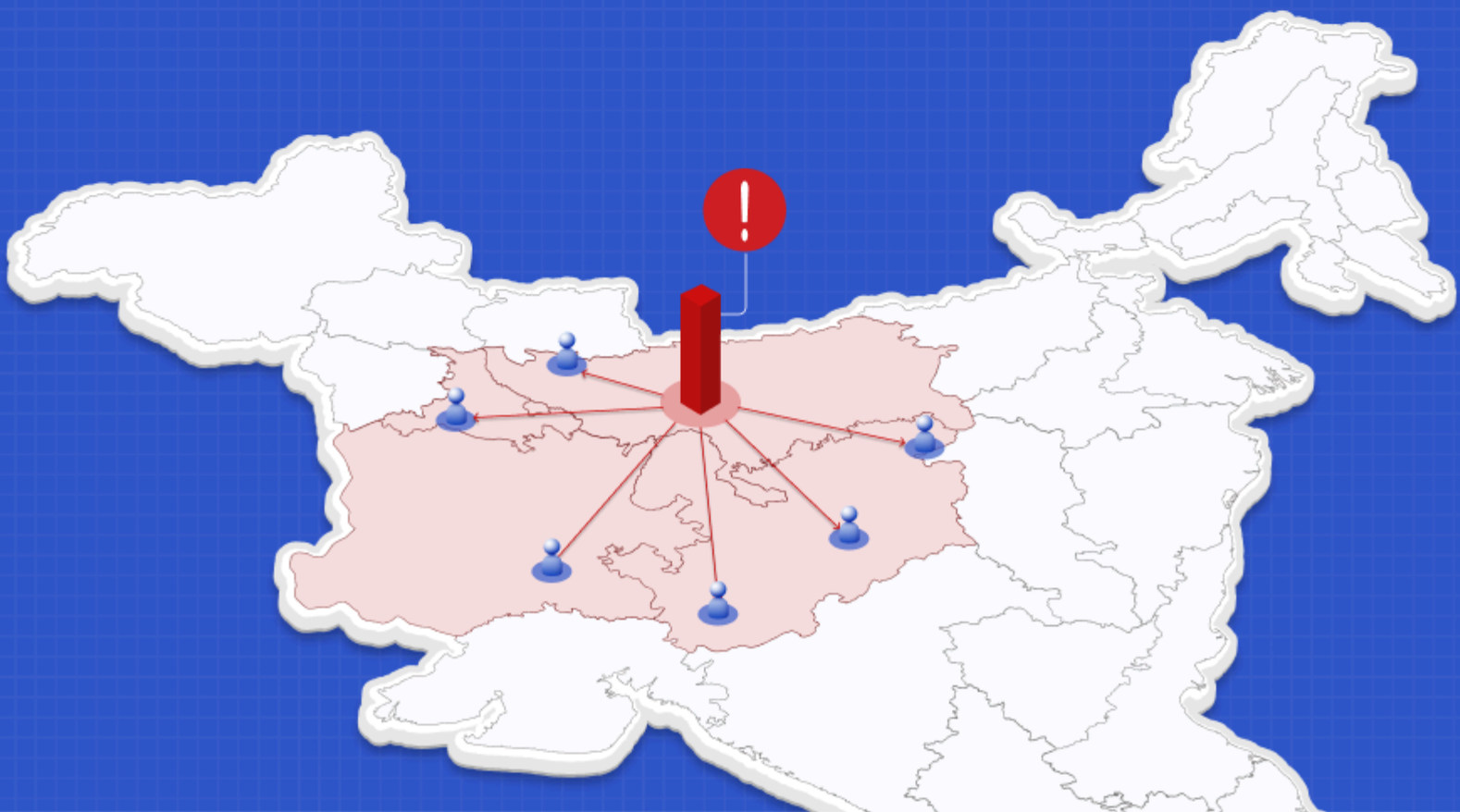
Districts flying under the radar:

From FY27 Q1 VKYC rejection data, we've identified several districts showing rising fraud activity that haven't hit government or police radar yet. **This whitepaper lists the top 10 that need immediate attention.**

Page 7

What's next

This is the first in a quarterly series. IDfy will keep sharing these signals so risk teams can stay ahead of the next wave.



VKYC as an Early Signal

01

Using V-KYC rejection data, we spotted around 16 district-level fraud hotspots every quarter in FY26. Of these, 85-90% were later confirmed, through law enforcement action, or news reports.

Featuring two such examples, Varanasi and Malappuram, flagged early and later confirmed as fraud hotspots by law enforcement.

Varanasi, Uttar Pradesh

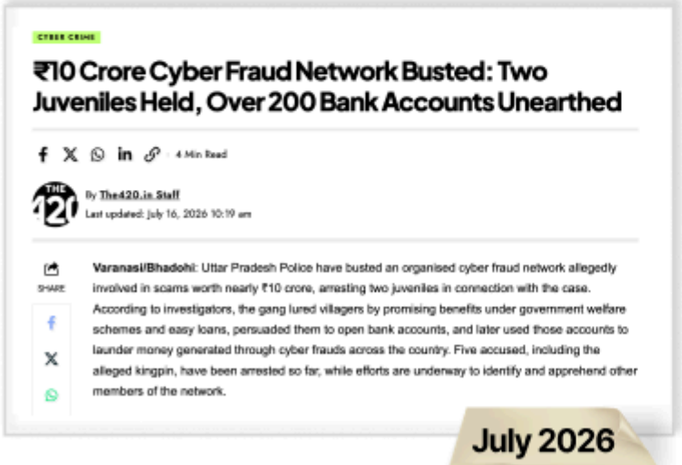
First Flagged in

May 2026
Rejection Rate

11.88%

Lead: 1 month

About a month after we identified Varanasi as the epicentre, Operation Mule Strike and related law enforcement crackdowns made national and local headlines.



CYBER CRIME

₹10 Crore Cyber Fraud Network Busted: Two Juveniles Held, Over 200 Bank Accounts Unearthed

4 Min Read

By The420.in Staff
Last updated: July 16, 2026 10:19 am

SHARE

Varanasi/Bhadohi: Uttar Pradesh Police have busted an organised cyber fraud network allegedly involved in scams worth nearly ₹10 crore, arresting two juveniles in connection with the case. According to investigators, the gang lured villagers by promising benefits under government welfare schemes and easy loans, persuaded them to open bank accounts, and later used those accounts to launder money generated through cyber frauds across the country. Five accused, including the alleged kingpin, have been arrested so far, while efforts are underway to identify and apprehend other members of the network.

July 2026

News / City News / Varanasi News / 5 Arrested For Running Interstate Mule Account Cyber Fra...

Trending | Haryana Murder | Dehradun Bridge Collapses | CJP Protest | Mair Beera | Cockroach Janta Party

5 arrested for running interstate mule account cyber fraud racket

Rajeev Dikshit / Jul 30, 2026, 00:12 IST

Preferred on Google | Comments | Share | AA

TOI

Varanasi: The cyber crime police arrested five members of an interstate cyber fraud racket that allegedly lured economically weak people into opening bank accounts in their names and used them as mule accounts for cyber criminals.

DCP (Crime) Neetu Kadian said on Wednesday that the accused were identified as Adarsh Chaube of Mirzapur, Ashish Yadav of Azamgarh, Sujal Singh of Muzaffarnagar, Piyush Singh of Mau and Yuvraj Verma of Varanasi.

July 2026

https://the420.in/varanasi-bhadohi-police-mule-account-fraud-network/

https://www.jagran.com/uttar-pradesh/varanasi-city-operation-mule-strike-in-varanasi-case-registered-against-six-account-holders-for-cyber-fraud-arrests-made-40279245.html

https://timesofindia.indiatimes.com/city/varanasi/5-arrested-for-running-interstate-mule-account-cyber-fraud-racket/articleshow/132720576.cms

https://www.jagran.com/uttar-pradesh/varanasi-city-varanasi-police-arrests-3-in-1798-cr-cyber-fraud-across-13-states-40322728.html utm_source=chatgpt.com

VKYC as an Early Signal

02

First Flagged in

May 2026
Rejection Rate **6.29%**

Lead: 1 Quarter

Operation Cy-Hunt: 30 arrests in 12 hours, 44,088 mule accounts blocked — confirming the epicentre months later.

Large amount of money received in bank in Malappuram withdrawn within minutes; 27 people arrested in Operation Cy-Hunt

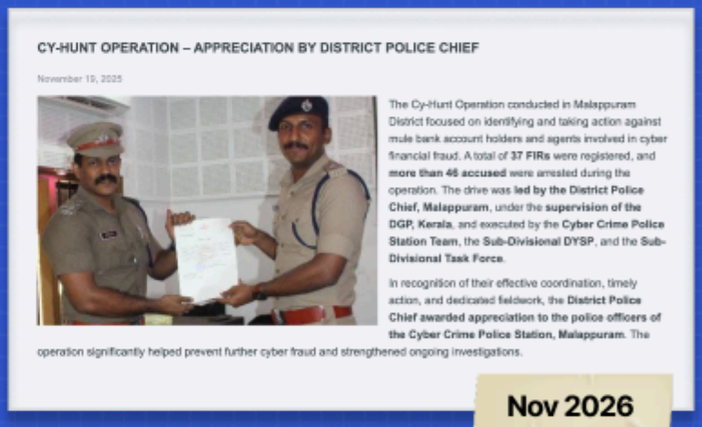
Published by: Nandu Krishnan | news18-malayalam
Last Updated: March 5, 2026 9:46 PM IST

The Psy-Hunt operation was carried out after a three-month investigation focused on various bank accounts.

27 people have been arrested in Operation Cy-Hunt, a cyber-financial crime operation conducted in Malappuram district. The Cy-Hunt operation was conducted after a three-month investigation focusing on various bank accounts.

Symbolic image

Mar 2026



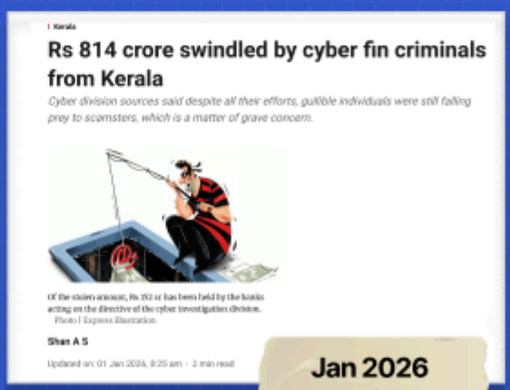
CY-HUNT OPERATION – APPRECIATION BY DISTRICT POLICE CHIEF

November 10, 2025

The Cy-Hunt Operation conducted in Malappuram District focused on identifying and taking action against mule bank account holders and agents involved in cyber financial fraud. A total of **37 FIRs** were registered, and **more than 46 accused** were arrested during the operation. The drive was **led by the District Police Chief, Malappuram**, under the **supervision of the DGP, Kerala**, and executed by the **Cyber Crime Police Station Team**, the **Sub-Divisional DYSP**, and the **Sub-Divisional Task Force**.

In recognition of their effective coordination, timely action, and dedicated fieldwork, the **District Police Chief awarded appreciation to the police officers of the Cyber Crime Police Station, Malappuram**. The operation significantly helped prevent further cyber fraud and strengthened ongoing investigations.

Nov 2026



Kerala

Rs 814 crore swindled by cyber fin criminals from Kerala

Cyber division sources said despite all their efforts, gullible individuals were still falling prey to scamsters, which is a matter of grave concern.

Of the stolen amount, Rs 352 cr has been held by the banks acting on the directive of the cyber investigation division.
Photo | Express Illustration

Shan A S

Updated on: 01 Jan 2026, 8:25 am · 2 min read

Jan 2026

https://ps.keralapolice.gov.in/malappuramcyberps-ps/good-works/Cy-Hunt-Operation-Appreciation-3542?utm_source=chatgpt.com

https://www.newindianexpress.com/states/kerala/2026/Jan/01/rs-814-crore-swindled-by-cyber-fin-criminals-from-kerala?

https://malayalam.news18.com/news/crime/27-arrested-frommalappuram-district-in-operation-cy-hunt-against-mule-accounts-and-cyber-fraud-nkn-ws-kl-764843.html

A Pattern That Holds Up

03

Fraud rings keep moving. We track where.

When enforcement clamps down in one district, fraud doesn't stop, it just moves. Using VKYC data from our work with leading financial institutions, we studied 15 months across ~130 districts and found three clear patterns.

1. Risk spikes last one month, then shifts

Fraud hot spots rarely stays put. In 81% of cases, a district's risk spike lasts just one month. Only 6.5% last three months or more.

Note: *this tracks how long a district stays risky, not how long a fraud ring survives*

2. When one district cools down, the one next door heats up

Fraudulent activities in a district doesn't disappear, it shifts nearby. 39% of the time, the next hotspot is in the same state. On average, it moves about 190 km away.

Note: *this shows a geographic pattern. We can't confirm if it's the same fraud network moving*

3. Old hotspots come back, usually within a quarter

A district going quiet doesn't mean it's fixed. Flagged districts often reignite around 3 months later. This quarter alone, 11 active hotspots had already been flagged earlier in FY26.

Note: *this shows the location stays vulnerable, not that the same operators returned.*

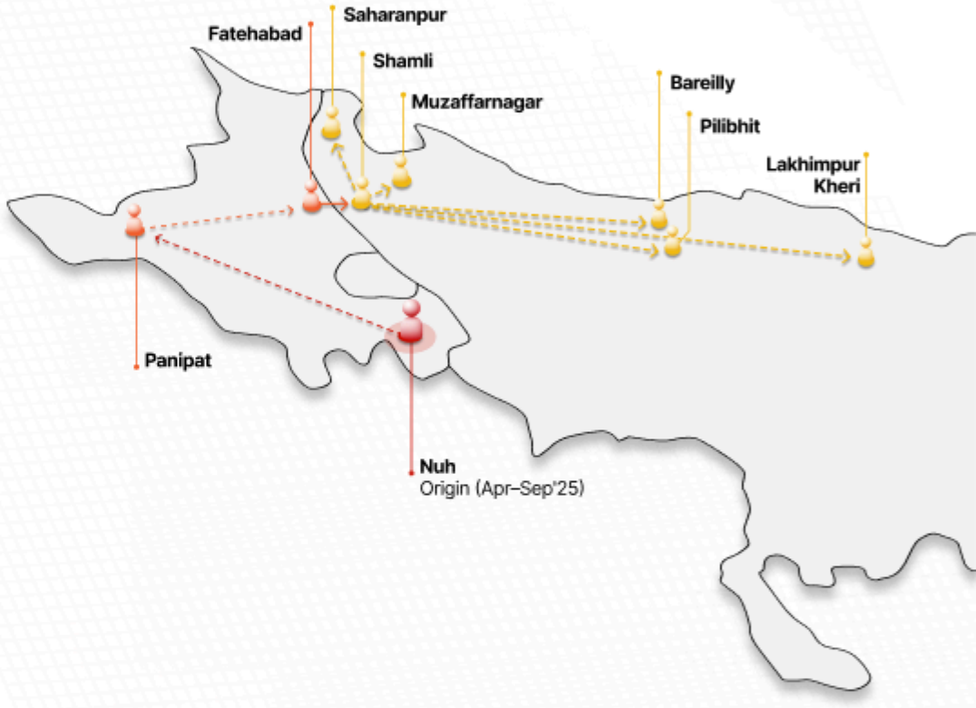
A Pattern That Holds Up

04

These patterns play out in real cases. Here are two examples, out of many we've tracked: **Nuh, Haryana and Surat, Gujarat,** showing fraud clusters moving across districts and state borders, later confirmed by law enforcement.

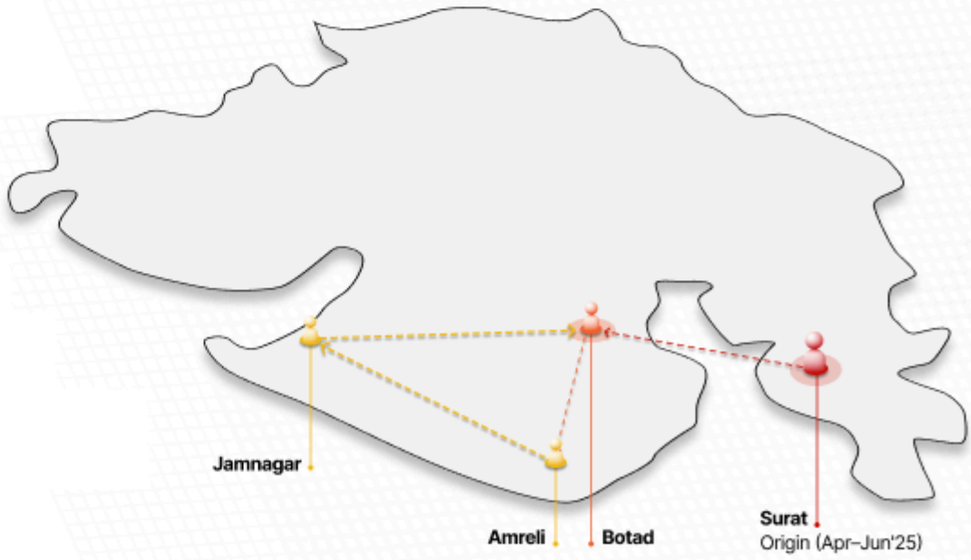
First Movement

Fraud activity remained concentrated in Nuh through late 2025 before progressively expanding within Haryana and subsequently spilling over into adjoining districts of Western Uttar Pradesh during March–June 2026.



Second Movement

The Gujarat cluster originated in Surat and progressively expanded north-westward through Botad before extending to Amreli and Jamnagar, indicating gradual regional diffusion rather than abrupt relocation.

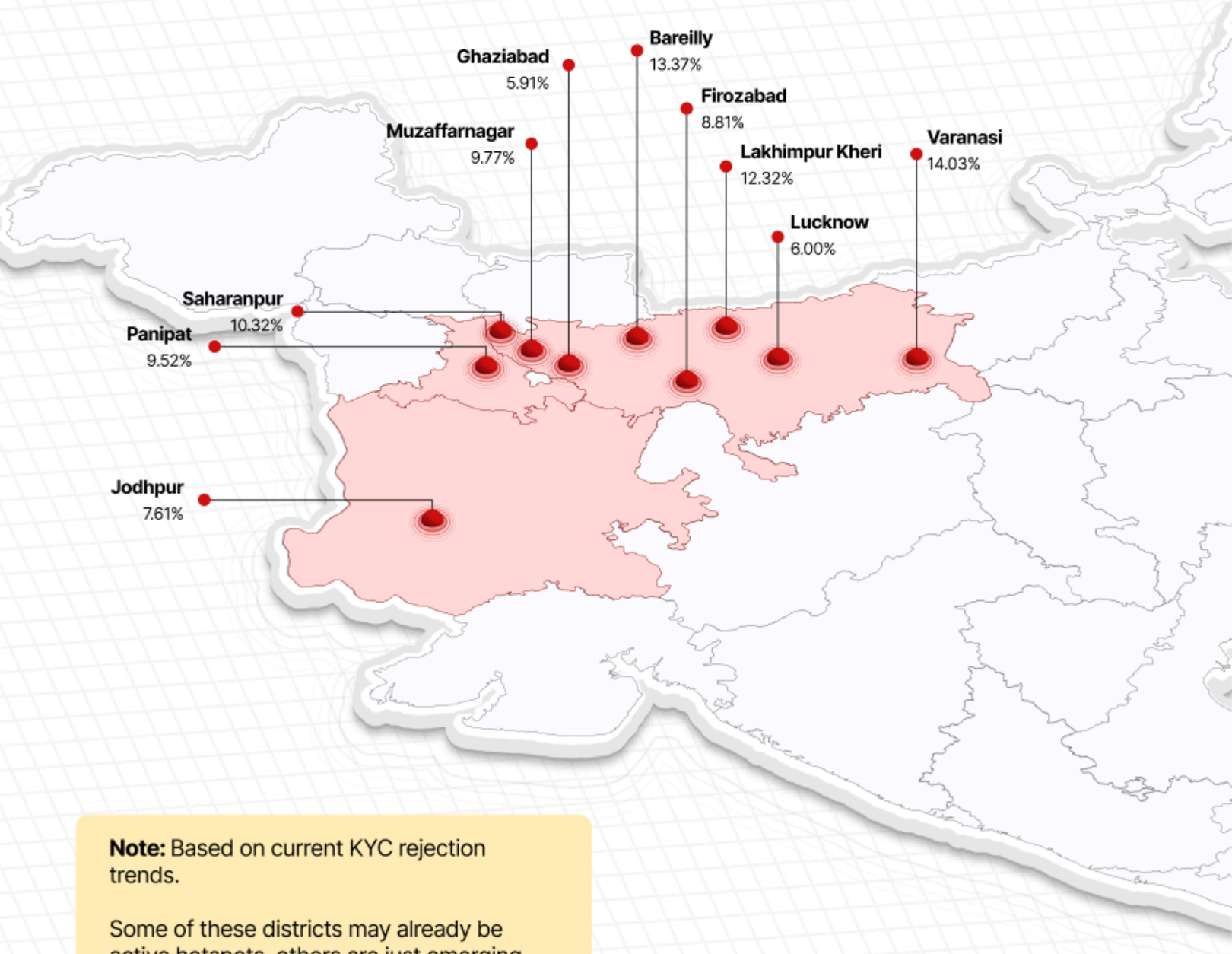


Action for regulators and regulated entities: Flag high-risk districts while they are active and pre-alert neighboring districts to prepare for the potential emergence of the next fraud cluster.

Upcoming Districts Where Fraud Rings Are Gaining Ground

10 districts could be showing a silent rise in fraud activity, and none of them are on the enforcement radar yet.

These are early signs of the next big fraud clusters. **Risk leaders and regulators need to act now, before it scales**



Note: Based on current KYC rejection trends.

Some of these districts may already be active hotspots, others are just emerging, either way, they need attention now.

Annexure

Data Source

We base this report on V-KYC onboarding telemetry captured between April 2025 and June 2026.
For every district, we track monthly V-KYC attempts against total rejections to map localized risk patterns.

Rejections occur when automated systems or live agents flag impersonation, document tampering, third-party prompting, or suspicious user behavior.

The dataset is limited to domestic operations and excludes foreign location entries from the raw feed before analysis.

Methodology: How Districts Are Flagged

A district is flagged in a given month only after it passes two independent tests, and then it is ranked against other qualifying districts.

Test 1
Statistical Validity Floor

Small sample sizes distort risk data. In low-volume districts, a single random rejection artificially spikes the failure rate.

So we calculate a dynamic sample size floor every month to eliminate this noise:

Minimum calls required = max($5 \div p_0$, $5 \div (1 - p_0)$)
where p_0 is that month's national average rejection rate.

This formula ensures statistical validity by requiring at least 5 expected instances of the rarer outcome. As national rejection rates shift monthly, this threshold adjusts with them—typically landing between 108 and 143 calls per month.

We tested this against a stricter threshold requiring 10 expected instances. The results were identical, confirming that our choice of cutoff does not alter the findings.

Test 2
Minimum Fraud Volume Floor

Test 1 confirms a rejection rate is statistically real, but it does not confirm the fraud volume is large enough to matter.

We apply a second floor: a district must record at least 30 rejected calls in a month to qualify for ranking.

This ensures every flagged district represents a real concentration of fraud, not just a high percentage on a small sample.

Ranking: Z-Score

Once a district passes both volume floors, we rank it by Z-score.

A Z-score measures how many standard deviations a district's rejection rate sits from the national mean. It separates actual risk from noise.

We deliberately avoid raw rates and raw volumes because:

- Raw rejection rates over-index on small districts prone to noisy swings.
- Raw call volumes over-index on India's largest cities, whether fraud is actually concentrated there or not.

Testing showed that ranking by raw volume fails to track genuine fraud concentration. The Z-score balances rate and volume without distorting the picture. The top 16 districts by Z-score each month form the final flagged list.

Regional Accuracy

- **Confirmed Locations:** Law enforcement and media mentions verified the majority of our flagged districts. We manually audited and corrected data glitches, such as place names matching individual names, before finalizing counts. In fact, onboarding telemetry identified 33% more active fraud locations than official daily reporting.

Signal Lead Time

Onboarding telemetry catches fraud at entry, before downstream complaints or enforcement action takes place.

- **Leading Signal:** In verified cases, the signal flagged high-risk districts months before any public reporting emerged—in one instance, gaining up to a two-month proactive advantage.
- **Lagging Signal:** In other cases, news reports broke before the signal's monthly cadence caught up.

Both outcomes are documented directly. Onboarding data provides a proven early-warning signal across many districts, even if that early lead is not universal.

Seeing similar trends in your onboarding metrics or a completely different story?

We'd love to compare notes.

About IDfy

IDfy is Asia's leading trust stack, delivering identity verification, risk intelligence, and data privacy governance for banks, financial services, retail, logistics, and mobility enterprises. Processing over 70 million verifications monthly across 500+ enterprise institutions, IDfy's infrastructure intercepted over 20 million potential fraudulent onboardings in Fiscal Year 2026 alone.