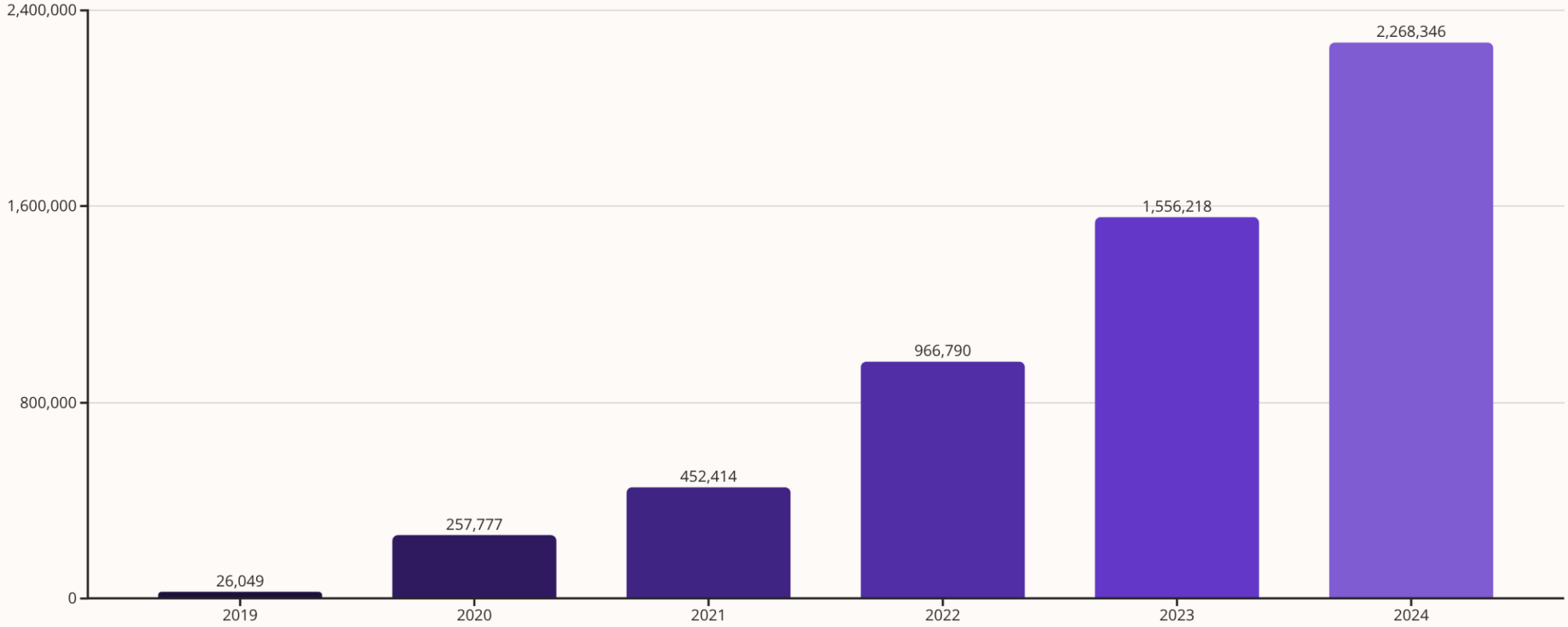
DoT's Digital Platforms for Security, Fraud Prevention & Consumer Protection

Presentation by
Satyam Singh,
Assistant DG (Security)
Mumbai LSA, Dept. of Telecommunications

Cybercrime Trends: Complaints on National Cybercrime Reporting Portal

Source: National Cybercrime Reporting portal (NCRP), MHA



The increase from 2022 to 2023 was 61%, and from 2023 to 2024 was 45.7%. For context, this translates to approximately ~7000 complaints per day as of May 2024.

Satyam Singh, ITS
About Speaker

1 **Indian Telecommunication Service (ITS)**

From Indian Telecommunication Service

2 **Assistant Director General**

In Department of Telecommunication

3 **Security Function**

Looks after Security Function of the Licensor

4 **Lawful Interception & Monitoring**

Experienced in Lawful interception and Monitoring

5 **Certified Lead Auditor**

ISO 27001:2022

6 **TEDx Speaker & Cycling Advocate**

Sharing insights and promoting a healthy lifestyle

7 **Previous Roles**

Ex- BEL and Ex- BHEL

The Mandate: A Collective Framework for Biometric Verification

The Telecommunications Act, 2023

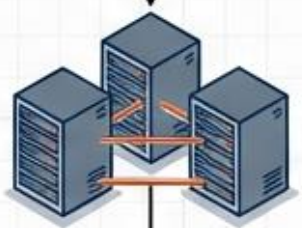
Draft Telecommunications (User Identification) Rules, 2025

RESPONSIBLE PARTIES

Authorised Entities (TSPs)

Option A: Individual

Option B: Collective



Strategic Opportunity: Shared Infrastructure Consortium

Live Photograph

Other Biological Attributes

BIVS (Biometric Identity Verification System)

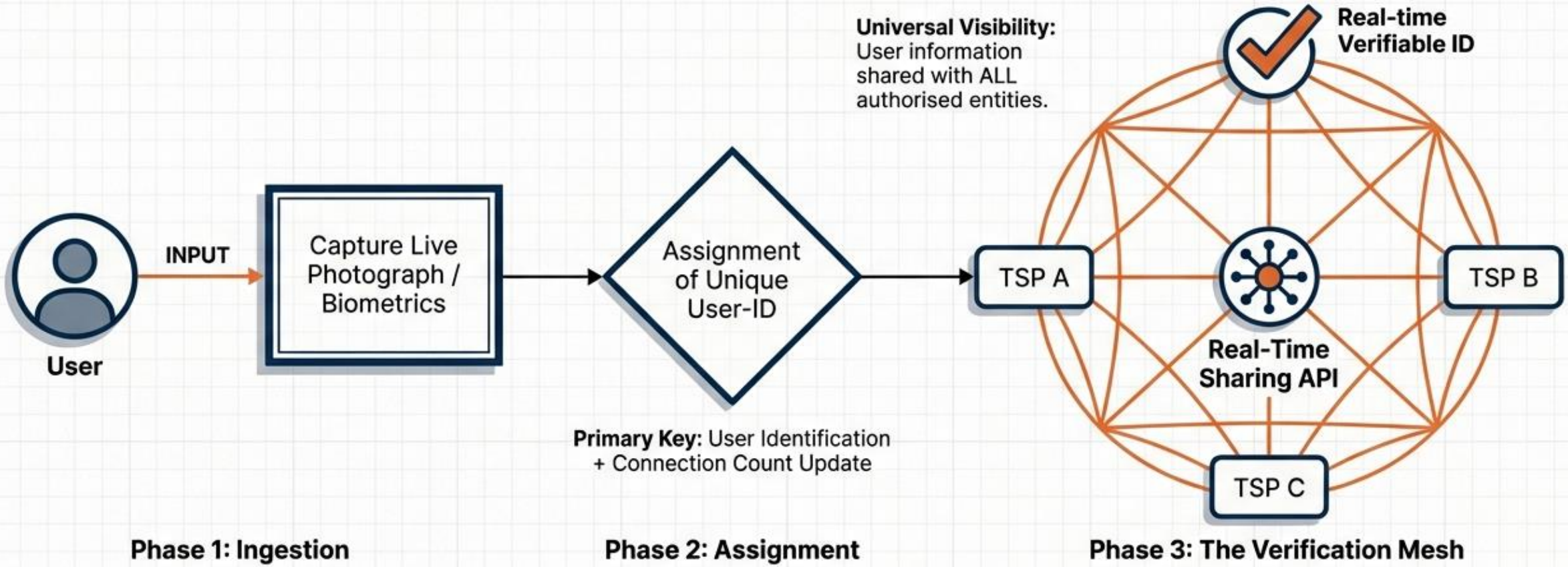
Scope of Responsibility

TSPs must establish, operate, maintain, and expand the system.

Regulatory Boundary

Operations must strictly comply with government directions, security standards, and data integrity requirements.

Operational Architecture: Data Flow & Inter-Entity Verification



PRIVACY & SECURITY LAYER: Ensuring data integrity and privacy in compliance with applicable laws and Central Government directions.

Policy Interventions: Prevention of Misuse of Telecom Resources

Draft Telecommunications (User Identification) Rules, 2025 under the Telecommunications Act, 2023:

- Under the Act, DoT has framed these Rules - published in Gazette for public consultation on 19.09.2025 – under finalization
- These rules:
  - ✓ provide a framework for the biometric based identification of users of notified telecommunication services
  - ✓ envisage to put in place “Biometric Identity Verification System” or “BIVS” means a system for biometric based identification of a user.
  - ✓ Rule 6 of the draft Rules: each authorised entity (i.e. TSP), individually or collectively with such other authorised entities, establish, operate, maintain and expand BIVS for biometric based identification of user, using live photograph or any other biological attributes of an individual as may be specified by the Central Government.
  - ✓ Each user - unique user-id in the BIVS – to be used by an authorised entity (TSP) for identification of the user and updating the number of connections.
  - ✓ User information maintained by an authorised entity in BIVS shall be shared with all other authorised entities -> to enable real-time verifiable biometric based identification of user

What is CNAP?

CNAP (Calling Name Presentation) is a network-level service mandated by India's Department of Telecommunications (DoT) that displays the caller's registered name during incoming calls.

> The caller name comes from the telecom operator's verified database, not from crowdsourcing

- Verified through KYC records
- No third-party app required
- Works at the network level

Why CNAP is Safer 🔐

Verified Identity

Names linked to official KYC

Reduces fake labels

No Contact Harvesting

Does not access your phonebook

Contacts not uploaded anywhere

Regulatory Oversight

Controlled by DoT

Subject to Indian data-protection laws

Works Without Internet

Network-based service

Works on feature phones and rural networks

Sanchar Saathi Initiative: Empowering Citizens, Breaking silos, real time collaboration with Stakeholders

Web portal available at : www.sancharsaathi.gov.in

BLOCK YOUR LOST / STOLEN MOBILE HANDSET

45.87 lakh
mobiles blocked

28.46 lakh
mobiles traced

KNOW MOBILE CONNECTIONS IN YOUR NAME

322.74 lakh
requests received

297.10 lakh
requests resolved

CHAKSHU - REPORT SUSPECTED FRAUD COMMUNICATION

7.97 lakh
inputs received

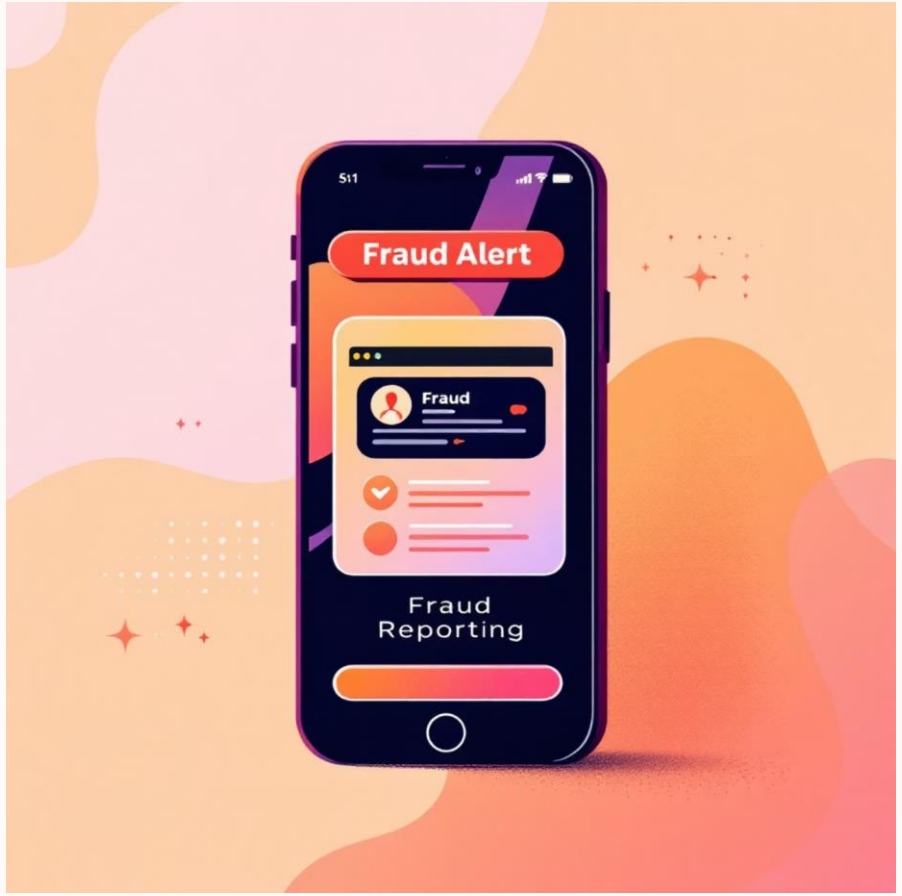
45.40 lakh
action taken

Citizen Centric Services

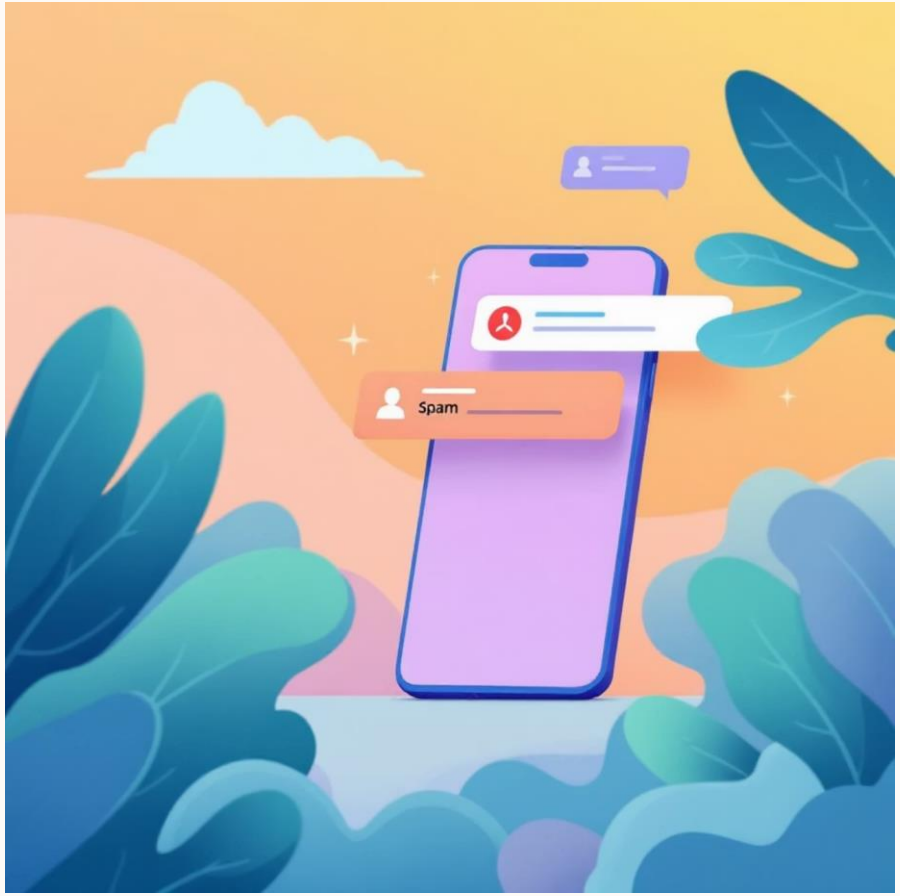
- CHAKSHU - REPORT SUSPECTED FRAUD COMMUNICATION / UCC (SPAM) / SUSPECTED WEB LINKS
- BLOCK YOUR LOST / STOLEN MOBILE HANDSET
- KNOW MOBILE CONNECTIONS IN YOUR NAME
- KNOW GENUINENESS OF YOUR MOBILE HANDSET
- REPORT INCOMING INTERNATIONAL CALL WITH INDIAN NUMBER
- KNOW YOUR WIRELINE INTERNET SERVICE PROVIDER
- Beta TRUSTED CONTACT DETAILS

चक्षु - Report Suspected Fraud & Unsolicited Commercial Communication

Report Suspected Fraud Communication (Received within last 30 days)



Report Unsolicited Commercial Communication (UCC) / Spam (Report within 7 days for action)



चक्षु - Report Suspected Fraud & Unsolicited Commercial Communication

Report Suspected Fraud Communication
(Received within last 30 days)

Chakshu facilitates citizens to report the suspected fraud communications with the intention of defrauding telecom service users for cyber-crime, financial frauds, non-bonafide purpose like impersonation or any other misuse through Call, SMS or WhatsApp.

Few examples of suspected fraud communications are communication related to Bank Account / Payment Wallet / SIM / Gas connection / Electricity connection / KYC update / expiry / deactivation, impersonation as Government official / relative, sextortion related etc.

Note: If you have already lost money due to financial fraud or are a victim of cyber-crime, please report at cyber crime helpline number 1930 or website https://www.cybercrime.gov.in. Chakshu facility does not handle financial fraud or cyber-crime cases.

Know More | Continue reporting →

Report Unsolicited Commercial Communication (UCC) / Spam
(Report within 7 days for action)

Chakshu facilitates citizens to report UCC or spam received through Voice Call or SMS which is not as per the consent given by recipient to sender or as per registered preference (s). UCC / Spam are dealt as per The Telecom Commercial Communication Customer Preference Regulation (TCCCPR), 2018 regulations of Telecom Regulatory Authority of India (TRAI). Visit https://trai.gov.in/what-spam-or-ucc for more details.

Any complaint made within 7 days of receiving UCC / Spam are considered valid complaints and further investigation is done by the telecom service providers and may lead to action against sender. The complaints made beyond 7 days of receiving UCC / Spam are considered reports. These reports may not lead to action against the sender at first hand but would aid in finding such spammers proactively.

Know More | Continue reporting →

चक्षु - Report Suspected Fraud Communication

Medium of Suspected Fraud Communication

Please select how you received the communication*

Medium
Select Medium

Suspected Fraud Communication Details

All * marked fields are mandatory.

Select Suspected Fraud Communication Category

Category
Select Category

Attach a screenshot

Choose an image file (upto 1MB in size) | Choose Files

Date and Time of the suspected fraud communication*

Select date of communication

Select time of communication in 12-hour (HH:MM AM/PM) format

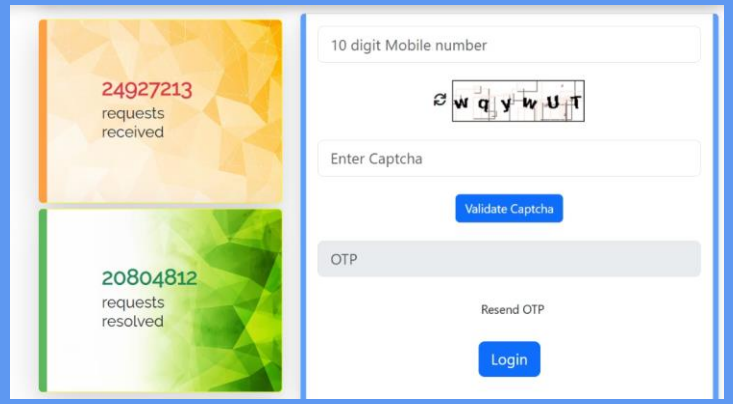
Enter complaint details*

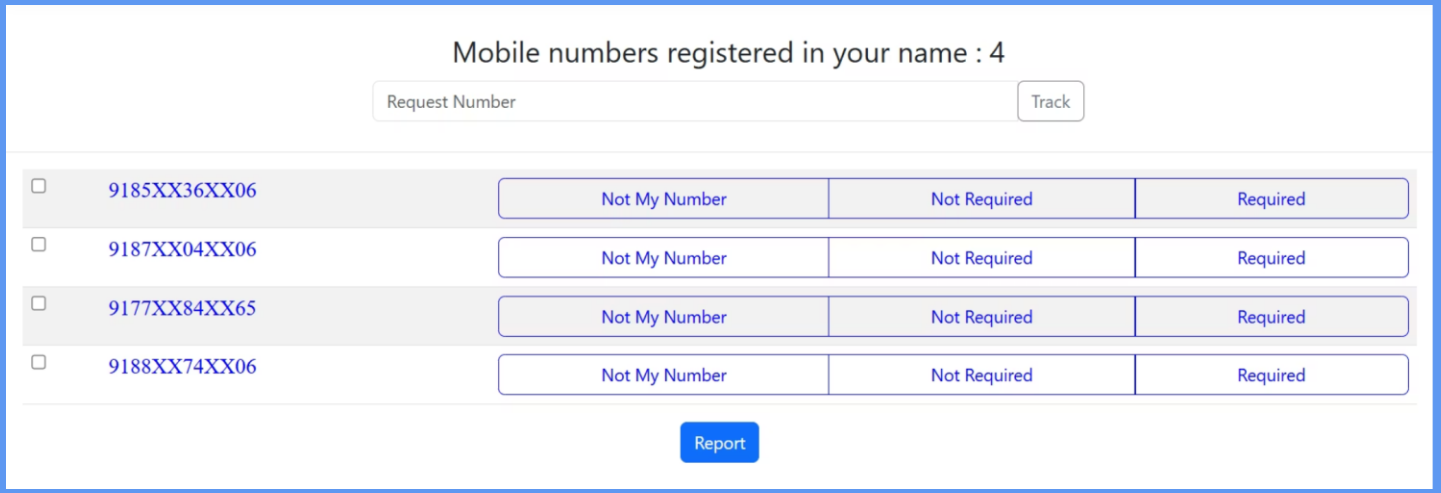
Complaint details (minimum 30 valid characters required)

500 characters remaining

Know Mobile Connections in Your Name

Know the number of connections issued in your name by logging in using your mobile number


24927213
requests
received
20804812
requests
resolved
10 digit Mobile number
Enter Captcha
Validate Captcha
OTP
Resend OTP
Login


Mobile numbers registered in your name : 4
Request Number
Track
9185XX36XX06
9187XX04XX06
9177XX84XX65
9188XX74XX06
Not My Number
Not Required
Required
Report

Block your lost / stolen mobile handset

Block and Trace your lost or stolen mobile handset

Lodge a police complaint

So that the case can be tagged to the police station

Get one of the SIMs reissued

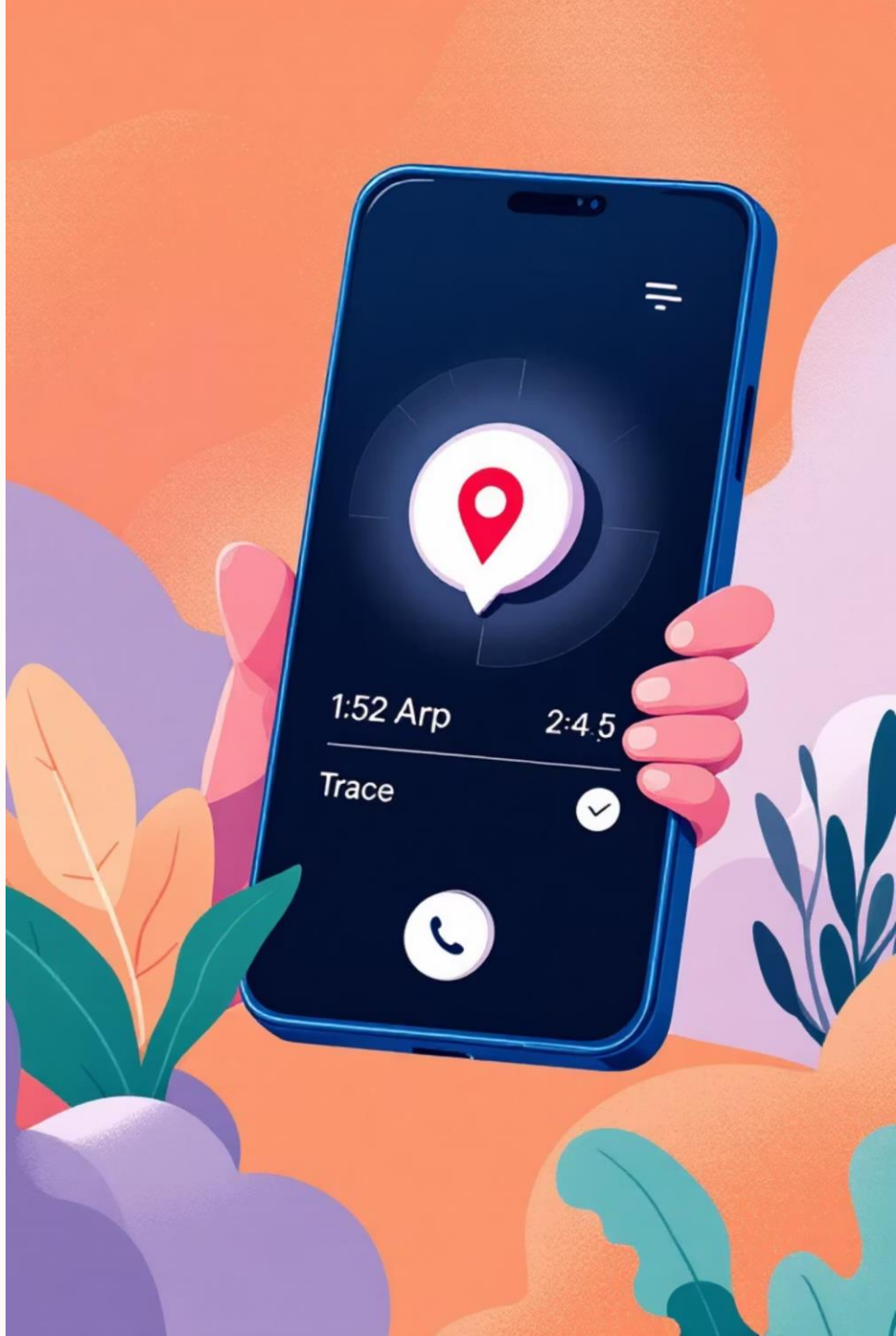
So as to validate the authenticity of your request

Approach the police station

Once you receive the traceability report

Unblock the phone

After the recovery.



Know Genuineness of Your Mobile Handset

Verify the authenticity of your mobile device and IMEI number through our official channels.

Use *#06# for getting IMEI Number

Alternate Verification Options

In addition to the online portal, you can verify your mobile device's genuineness and IMEI details using the following method:

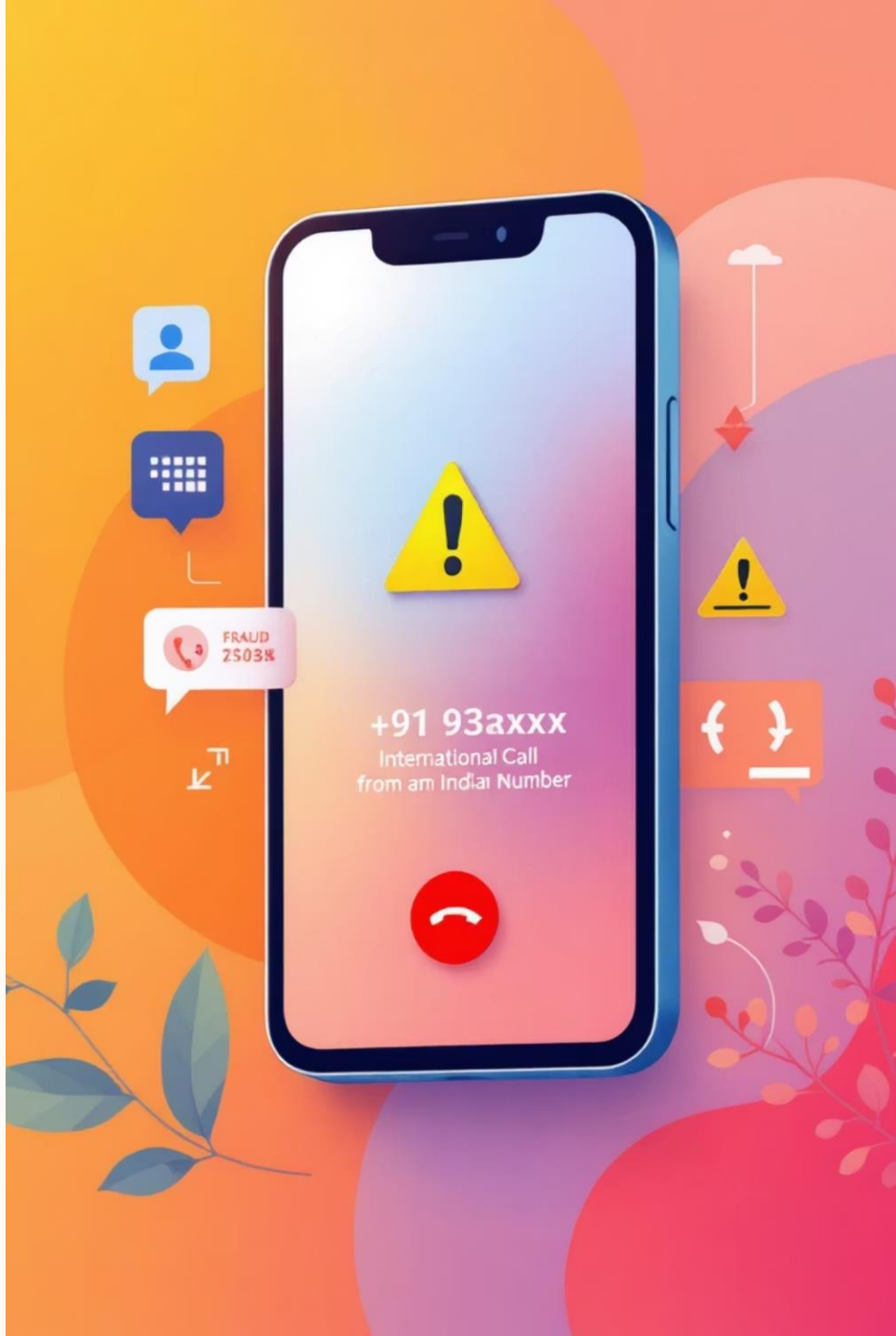
SMS Verification

owing Details found based on provided IMEI number '357611731993

शीर्षक	टिप्पणी
Brand Name	Motorola
Model Name	XT2303-2
Manufacturer	Motorola Mobility LLC, a Lenovo Company
Marketing Name	London23
Device Type	Smartphone

Report Incoming International Call With Indian Number

Alternatively, you can report on 1963/1800110420



Find Wireline Internet Service Providers (ISPs)

Search by PIN Code

Search by Address

Search by ISP Name

Trusted Contact Details

Search by Name | Search by Website | Search by Email | Search by Contact Number

Bank / Financial Institution Name IIFL Samasta Finance Limited Search

Show 10 entries

#	Bank / FI Name	View Details
1	IIFL Samasta Finance Limited	

Showing 1 to 1 of 1 entries (filtered from 231 total entries)

Previous 1 Next

Showing Complete Details for State Bank of India

#	Bank / FI Name	Website	Email ID	Official Number	Toll Free Number	Whatsapp Number	Other Customer Care Number
1	State Bank of India	https://sbi.bank.in	customercare@sbi.co.in contactcentre@sbi.co.in noreplyprmdlr@alerts.sbi.co.in nodalofficer.aadhaarseeding@sbi.co.in socialreply@sbi.co.in customercare.homeloans@sbi.co.in noreplyprm@alerts.sbi.co.in gm.customer@sbi.co.in	1600203027 1600014123 1600304197 1600208011 1600320334 1409262238 1409269093 1409247713 1409170004 1600210017 1409295382 1600117012 1600320336	18008888 1800111109 18004253800 1800112017 18004259760 1800112211 18002100 18008900 1800110018 18001234 1800112018 1800111103 1800110009	91-9022690226	080-26599990 9449112211

Close

Previous 1 Next

Impact of Jan Bhagidari

Chakshu - Report Suspected Fraud Communication

7.97lakh
Inputs

39.58 lakh+
Numbers disconnected

2.27 lakh+
Handsets/IMEIs blocked

Know Mobile Connections in Your Name

2.98 crore +
Numbers disconnected

Block Your Lost/Stolen Mobile Handset

8.5 lakh Handsets recovered worth Rs2000 Crores

Know Genuineness of Your Mobile Handset

40 lakh +
Successful response

Mumbai Police recover 1,650 lost and stolen mobiles worth Rs 2 crore from Uttar Pradesh

Updated on: 10 January,2026 07:32 PM IST | Mumbai
Samiullah Khan | samiullah.khan@mid-day.com

Share: FOLLOW ON Google News

Text AA AA Join Us

During a state-wise review of complaints registered on the Central Equipment Identity Register (CEIR) portal, police observed that a significant number of missing devices were being traced to Uttar Pradesh

Mumbai Police's operation successfully recovered 1,650 mobile phones, collectively valued around Rs 2 crore.

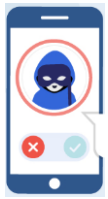
Threat landscape

Cyber frauds in India

Last 5 years
60 lakh complaints,
₹52,000 crores lost

Misuse of telecom resources

SIMs



Spoofed calls

SIM Box

SIP/PRI

Sanchar Saathi

A citizen centric initiative

23 crore+
Portal Visitors

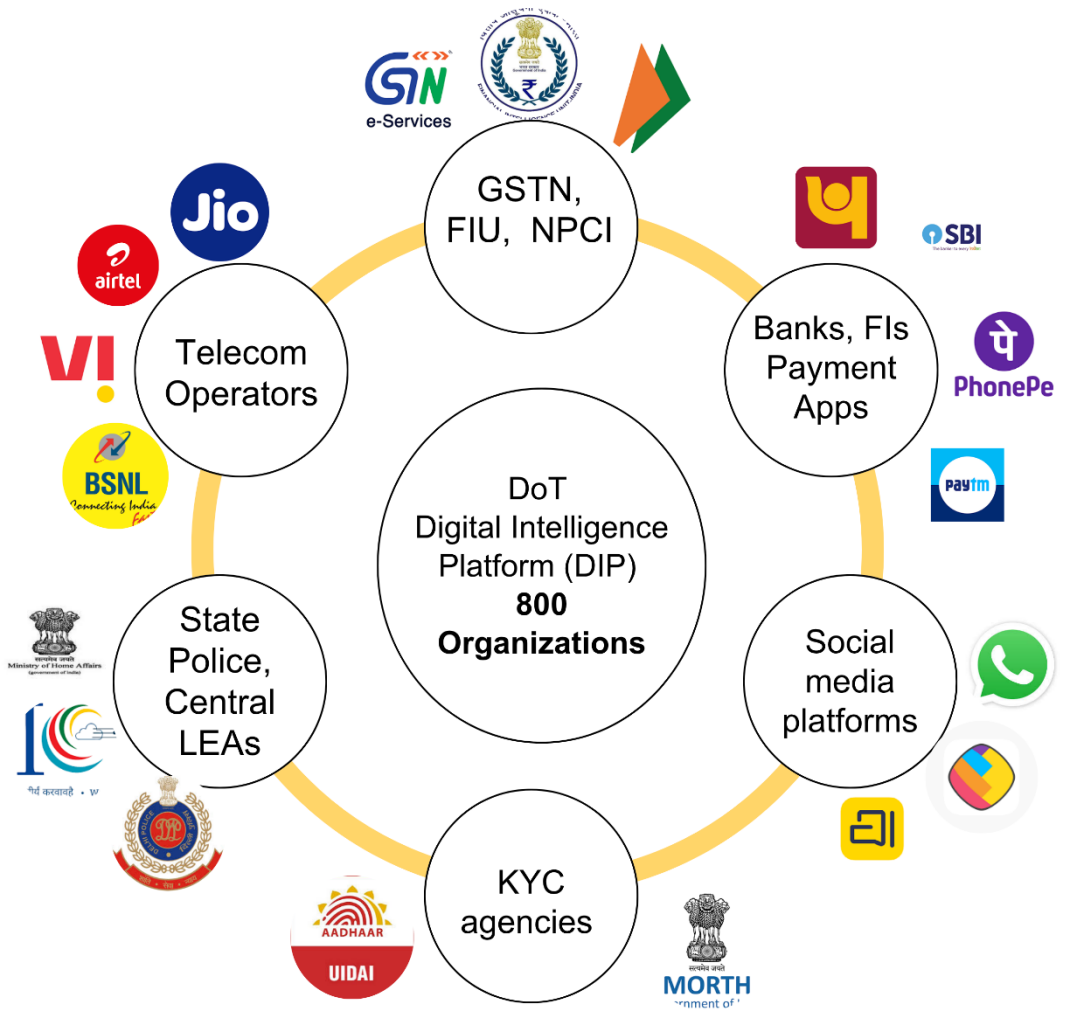
1.7 crore+
App Downloads

BHASHINI
23
Languages

DoT Digital Intelligence Platform (DIP)

Problem Statement

- **Mobile Number** – seeded for availing most digital services – banking, e-gov, e-commerce etc.
- Finite Numbering Resource - Re-allotted after 90 days of disconnection
- No information about disconnected numbers to user entities – keeps sending service, transactions SMSs to new customer – inconvenience as well as data privacy issues.
- Sensitive information susceptible for misuse cybercrime and financial frauds



Enabling synergy Telecom ● Finance ● LEAs to curb cyber frauds

Initiative#1- Mobile Number Revocation List (MNRL) at DIP

Problem Statement

Mobile Number
Availing digital services- banking, e-gov etc.

Finite Numbering Resources
Re-alloted after 90 days of disconnection

No information sharing
To User organization, keep sending SMS, Inconvenience and Data privacy issues

Solution

MNRL
List of disconnected number with date, reason, TSP etc.

Automated Sharing
Through DIP

Dynamic List
Live for 90 days, automated removal

Advisory by RBI to its regulated entities

- Use MNRL, clean their database.
- Enhanced Due diligence, Delinking from account / profile

4 crore+
MNRL shared in last 90 days

30 lakh+
Accounts Frozen or debit/ credit restricted

Initiative#2- Financial Fraud Risk Indicator(FRI) at DIP

Suspected number

Minimum 15 days
Life cycle of Number flagged in Reverification

5 days
Outgoing barred

5 days
Incoming barred

5 days
Disconnected

Mobile Number disconnected failing reverification

MNRL

Generated after min 15 days

Flagged to entities for taking action

- Banks/ FIs
- Social Media Platforms
- Central LEAs
- I4C, MHA
- State Police

Same day when flagged for reverification

Financial Fraud Risk Indicator(FRI) Generation Module

- Very High Risk Numbers
- High Risk Numbers
- Medium Risk Numbers

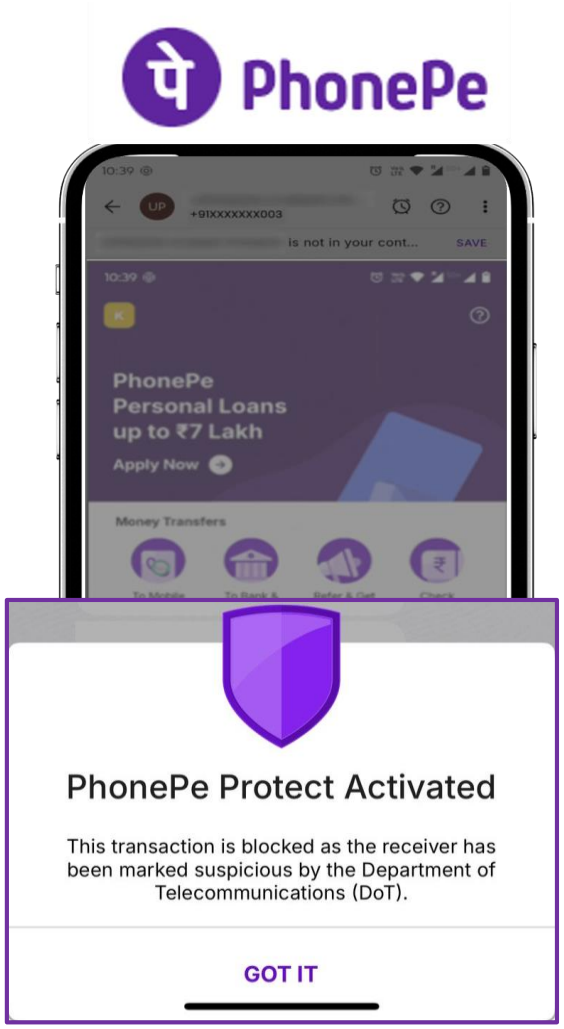
Generated within 24 hrs

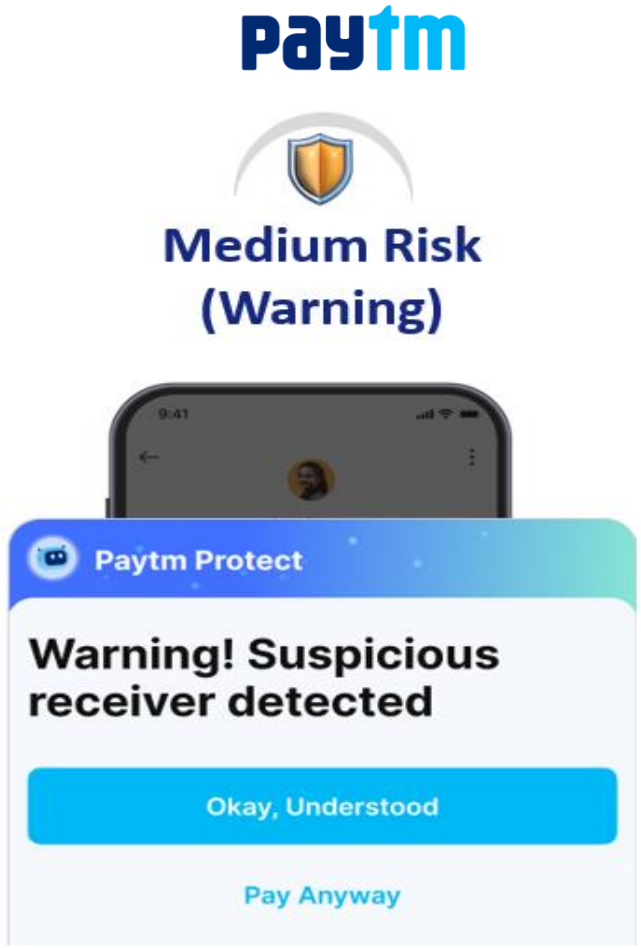
समय ही सार है- Time is the essence

Proactive & Preventive

RBI advisories to banks & Payment Service Operators (PSO) for integration of FRI with their respective systems and adopt necessary real-time response protocols (like alerts, transaction delays, warnings, transaction decline etc.)

Advisory by RBI to regulated entities Real-time response protocols (alerts, transaction delays, warnings, transaction decline etc.)





₹1000 Crore+ saved

90 Lakhs Transactions declined/ alerts generated

PROTECTED BY FRI DEPARTMENT OF TELECOMMUNICATIONS

10 Lakhs+ Accounts / wallets frozen

23 Lakhs+ Debit / credit restriction

National level Impact

Solution#3- Mobile Number Validation System (MNVS)

- To enable **validation** by **TSPs** for the **ownership** of mobile number.
- **POC** - A **POC** for MNV undertaken with **GSTN** & **Punjab National Bank**.
- **Decentralized architecture** without Central data collection and data sharing**.**
- **Telecom Cyber Security Amendment Rules 2025** published on 22.10.2025.

Request
63937*****
Mohit Kumar
Male
20-09-2005

Mobile KYC
63937*****
Jitendra Kumar
Male
02-02-1998

Response
Image: **1%**, Name: **0%**
Gender: **Matched**, DOB: **Not Matched**

Secure API Connectivity, Encrypted Data flow

Secure API Connectivity, Encrypted Data flow

Seeker (Bank)

MNV platform

TSP

Solution#4- Central International Outroamer Register(CIOR)

- Before CIOR:
  - *Many fraudsters made international calls seem like local Indian numbers using manipulated caller IDs. This trick encouraged people to trust the call and often led to* ***financial scams, impersonation, or cybercrime****.*

- CIOR acts like a **central list/registry** that telecom networks use in real time:
  - When an incoming international call shows an Indian number, the system checks whether that number is a legitimate outbound roamer (i.e., an Indian subscriber actually roaming abroad).
  - If it *isn't legitimate*, it can be flagged and blocked so the call doesn't reach your phone.

Policy Interventions: Prevention of Misuse of Telecom Resources

Recent KYC Reforms

- KYC - Digital format only.
- No Paper KYC
- Mandatory end user KYC of business connections
- GPS capturing of PoS device
- eKYC - fingers, iris and face based

Point of Sales - Instructions

- Unique PoS ID across all TSPs
- Mandatory registration of PoS
- Written agreement including area of operation
- Rs. 10 lakh penalty per instance of sale by unregistered PoS
- Blacklisting within 24 hrs. across all TSPs if involved in forgery

The Telecommunications Act, 2023:

- Biometric verification mandatory (Section 3)
- Protection and cyber security of telecom network & services (Section 22)
- Protection of Users (Section 28)
- Online grievance redressal mechanism (Section 28)
- Duty of Users (Section 29)
- Impersonation: Imprisonment upto 3 years, fine upto Rs 50 lakhs (Section 42)

Sanchar Saathi Initiative: Empowering Citizens, Breaking silos, real time collaboration with Stakeholders

Thank You