

FINANCIAL FRAUD RISK INDICATOR – ECONOMY

NEWS: Recently, the **Department of Telecommunications (DoT)** has launched the **Financial Fraud Risk Indicator (FRI)** as part of the **Digital Intelligence Platform (DIP)** to safeguard financial systems and telecom infrastructure.

WHAT'S IN THE NEWS?

About Financial Fraud Risk Indicator (FRI)

- **What is FRI?**

The Financial Fraud Risk Indicator (FRI) is a digital, risk-based analytical tool developed to assess and classify mobile phone numbers based on their likelihood of being used in financial frauds or cybercrimes.

- **Purpose of FRI:**

It aims to act as an early warning system by alerting financial institutions, payment platforms, and law enforcement agencies about potentially risky mobile numbers before a transaction is processed.

- **Risk Classification:**

The FRI system assigns each mobile number into one of three risk categories—**Medium Risk**, **High Risk**, or **Very High Risk**—based on how likely it is to be associated with fraud-related activities.

- **Data Sources Used in Risk Assessment:**

FRI uses multiple trusted data sources to generate its risk score, including:

- The **National Cybercrime Reporting Portal** managed by the Indian Cyber Crime Coordination Centre (I4C), which records complaints and FIRs related to cybercrimes.
- The **Chakshu platform** under the Department of Telecommunications (DoT), which allows the public to report suspicious calls and SMSs.
- Data and alerts shared by **banks, fintech firms, and financial service providers**, which help identify fraud-prone mobile numbers based on transaction histories and suspicious patterns.

- **How it Works:**

Once a mobile number is flagged by any of the data sources, it undergoes a detailed, multi-layered analysis that considers various behavioral, transactional, and historical fraud indicators.

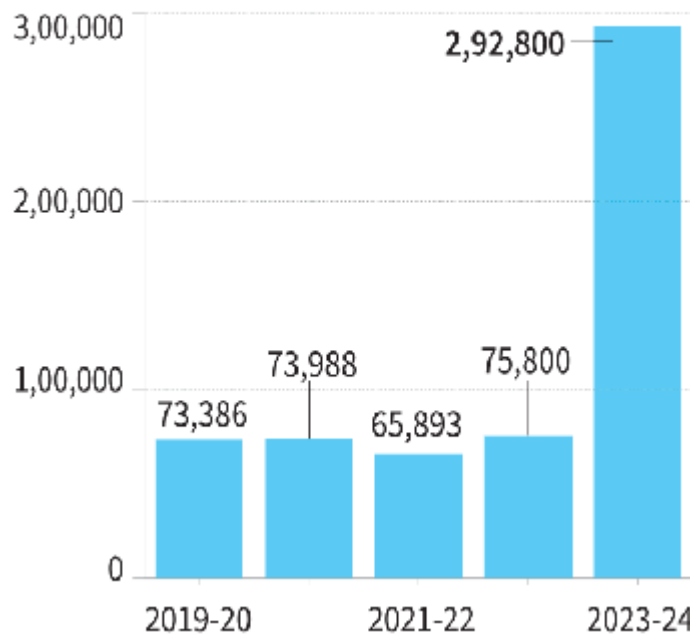
The FRI score is then calculated and **shared instantly in real-time** with stakeholders such as banks and UPI platforms for proactive fraud prevention.

- **Adoption by UPI Platforms:**

Leading UPI-based digital payment platforms such as **PhonePe, Paytm, and Google Pay** have now started to **integrate FRI alerts** into their payment infrastructure.

This helps them to **identify high-risk users** and either stop or flag suspicious transactions before any financial damage occurs.

Cyber frauds across the years in banking transactions



Cyber Fraud Scenario in India

- **Rising Threat:**

Cyber financial frauds have witnessed a **sharp increase in India**, with the proliferation of digital payments, e-wallets, and online banking systems. The digital push has expanded access to finance, but it has also made users more vulnerable to cyber threats.

- **Types of Cyber Financial Fraud:**

Some common forms of cyber financial fraud include:

- **Hacking:** Unauthorized access to a user's financial or personal data.
- **Phishing:** Fraudulent attempts (usually via emails or fake websites) to trick individuals into revealing sensitive information like OTPs or passwords.
- **SIM Swapping:** Gaining control of a user's phone number to intercept OTPs and gain unauthorized access to bank accounts.
- **Identity Theft:** Using someone else's identity to commit fraud.
- **Cyber Espionage:** Theft of financial or business secrets through digital means.
- **Cyberbullying & Blackmailing:** Sometimes used as leverage to extract money or personal information.

- **Data on Financial Losses:**

There has been a **substantial rise in the financial losses** due to such cyber frauds in the banking sector, as reflected in the annual data released by enforcement agencies and the Reserve Bank of India (RBI).

Government Initiatives Against Cyber Financial Fraud

a) Legal Frameworks and Acts

- **Information Technology Act, 2000:**

The IT Act is the **primary legislation in India** to deal with cybercrimes, electronic records, digital signatures, and the liability of intermediaries like telecom companies and digital platforms.

- **Bhartiya Nyaya Sanhita, 2023:**

As part of the criminal law reforms, this new legislation updates India's criminal justice system and introduces **specific provisions related to digital frauds and cybercrime**, making punishments more effective and technology-relevant.

- **Protection of Children from Sexual Offences (POCSO) Act, 2012:**

While primarily focused on protecting children, it includes provisions to **combat online child sexual exploitation and grooming**, which can sometimes be financially motivated.

b) Institutional Mechanisms and Tools

- **Indian Cyber Crime Coordination Centre (I4C):**

Established by the Ministry of Home Affairs, I4C is a **nodal agency** that works with state police forces, banks, and IT firms to **coordinate cybercrime responses and investigations** across India.

- **National Cyber Crime Reporting Portal:**

Citizens can lodge complaints related to cybercrime directly via this **online portal** (www.cybercrime.gov.in), which has significantly improved public access to grievance redressal mechanisms.

- **Citizen Financial Cyber Fraud Reporting and Management System:**

This platform allows victims to **report fraudulent financial transactions quickly**, leading to swift blocking of bank accounts and recovery of funds.

The system has successfully **helped recover over ₹1,200 crore** in defrauded amounts so far.

- **RBI's 'MuleHunter' Tool:**

This is an **Artificial Intelligence (AI) based tool** developed by the Reserve Bank of India to **track and detect 'money mule' accounts**—i.e., accounts used to transfer or hide the proceeds of digital frauds.

Banks and NBFCs have been advised to use MuleHunter for better fraud detection.

- **Blocking of Fraudulent SIMs and Devices:**

The government has deactivated over **3.2 lakh SIM cards** and blocked more than **49,000 IMEIs** (unique identifiers of mobile devices) that were being used in cyber fraud operations.

c) Citizen-Centric Measures and Campaigns

- **Chakshu Facility on Sanchar Saathi Portal:**

The **Chakshu platform**, under the **DoT's Sanchar Saathi initiative**, enables mobile users to report any suspicious calls, fraud attempts, or fake messages.

It aims to **disrupt fraud networks** by cutting off their communication channels.

- **e-Zero FIR Initiative (under I4C):**

Victims can now **file FIRs online**, irrespective of their physical location or the jurisdiction of the police station.

This **removes delays** caused by jurisdictional conflicts and helps initiate faster action.

- **Cyber Awareness Campaigns:**

The government actively promotes **cyber hygiene and fraud awareness** through various mediums:

- **Social media campaigns** like #CyberSafeIndia.
- **Radio jingles and short films** in regional languages.
- **Workshops in schools and colleges** to educate youth about secure digital behavior.

Source: <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2130249>