1. The Telecommunications (Telecom Cyber Security) Amendment Rules, 2025 – S & T

The Telecommunications (Telecom Cyber Security) Amendment Rules, 2025, were notified by the Department of Telecommunications

Key Amendments

1. Introduction of Telecommunication Identifier User Entities (TIUEs)

Definition - TIUEs are any business entities that use mobile numbers to identify, authenticate, or provide services to users — excluding licensed telecom operators (like Airtel, Jio, or BSNL).

Coverage - This new category brings digital platforms such as WhatsApp, PhonePe, Paytm, Swiggy, Zomato, Uber, and Ola within the purview of telecom cybersecurity regulation.

Compliance Duties - TIUEs must comply with government directives related to telecom security. They are required to respond to official data requests, including those from law enforcement or security agencies. They must verify customer identities using government-prescribed mechanisms. They are also obligated to suspend phone-linked accounts when directed by competent authorities.

2. Broad Scope of Regulation

The new rules expand the telecom regulatory net beyond traditional telecom service providers. All digital or app-based services that rely on mobile number authentication are now part of the telecom cybersecurity ecosystem. This ensures uniformity in accountability and traceability across communication, financial, and delivery platforms. It effectively closes a long-standing regulatory gap where non-telecom apps could use mobile numbers without telecom-grade verification safeguards.

3. Mobile Number Verification (MNV) System

Centralized Verification Gateway - The government has introduced a new Mobile Number Verification(MNV) system to check and validate user numbers.

Function - The MNV system verifies whether a number provided by a user corresponds to a legitimate, active telecom subscriber.

Implementation - Mandatory for TIUEs during user onboarding or KYC (Know Your Customer) verification. Enables platforms to authenticate whether a mobile number has been used for fraudulent or criminal activities.

Database Checks - Mandatory database checks before buying or selling used mobile devices to prevent circulation of stolen or tampered phones.

4. Empowering Immediate Government Action

Immediate Suspension Powers - Authorities can now act instantly, without prior notice, when it is deemed necessary for reasons of "public interest" or national security.

Wide Application - This enables rapid intervention across multiple services—telecom, messaging, fintech, and mobility apps—simultaneously.

Purpose - Designed to stop ongoing cyberattacks, financial frauds, or misinformation campaigns before they spread further.

5. Suspension of Accounts Linked Across Services

Linked Suspension - Authorities can issue a single order to suspend a user's access across multiple apps or telecom networks simultaneously.

Joint Compliance - Both telecom operators (e.g., Jio, Airtel) and digital platforms (e.g., Paytm, WhatsApp, Zomato) are legally bound to comply.

Impact - This prevents offenders from continuing fraudulent activities by switching between different platforms.

6. Regulation of Used Mobile Phone Market

IMEI-Based Verification - Before buying or selling a used mobile device, both parties must check the International Mobile Equipment Identity (IMEI) number against a government database.

Blacklisted Devices - The database will include IMEIs that are stolen, tampered, cloned, or restricted for

fraud. Selling or purchasing such blacklisted devices is strictly prohibited.

Enforcement Purpose - Reduces circulation of illegal devices in the grey market. Disrupts the network of criminals using stolen phones for cyber and financial crimes.

7. Establishment of a Government Verification Gateway

Centralized Platform - Apps and services can integrate with a government verification gateway to authenticate users' mobile numbers.

Modes of Integration -

Voluntary integration for self-regulating platforms.

Mandatory integration when directed by government or regulatory agencies.

Agency Access - Government agencies will have direct, assured access to verification data when required for investigations. The gateway cross-checks numbers with databases maintained by telecom operators (Airtel, Jio, Vi, BSNL, etc.).

Objective - Ensures accurate verification, strengthens digital trust, and prevents misuse of fake or temporary numbers.

Need For the Amendments

1. Rising Cybercrime Incidents

Data from I4C (Indian Cyber Crime Coordination Centre) - Over 7.4 lakh cybercrime cases were reported in the first four months of 2024 alone. Approximately 85% of these cases involved online financial frauds such as fake investment schemes, digital payment scams, and phishing operations.

Reason - Many of these crimes are executed using stolen, cloned, or fake mobile numbers which are difficult to trace.

2. Surge in Financial and Investment Frauds

Investment Scams - Over 83,000 cases in early 2024 involved fraudulent investment or trading offers spread via WhatsApp and Telegram groups. Fraudsters often impersonate legitimate brokers or advisors using spoofed mobile numbers.

Money Mule Accounts - Fraudsters use stolen identities and SIM cards to open fake digital bank accounts or wallets. These accounts act as intermediaries to launder fraudulently obtained money.

3. Exploitation of Mobile-Based Identity Systems

Criminals frequently exploit the mobile number as a digital identity in India's interconnected ecosystem (banking, e-commerce, UPI payments, etc.). They use cloned SIM cards, forged KYC documents, or spoofed caller IDs to gain access to sensitive systems. The new verification framework seeks to close these identity loopholes through real-time subscriber validation.

4. Rise of Stolen Phone Market

A thriving grey market for stolen and tampered phones fuels cybercrime by providing anonymous communication devices. Such phones often carry altered IMEIs to evade law enforcement tracking. Mandatory IMEI verification aims to cut off the supply chain that supports identity theft and online scams.

5. Ensuring Traceability and Accountability

As apps and platforms increasingly act as communication intermediaries, holding them to telecom-level security standards ensures -

1. Traceability of communications in case of fraud or cyber incidents.
2. Uniform data verification standards across digital platforms.
3. Better coordination between telecom and digital regulators for national cybersecurity management.

6. Building a Safer Digital Ecosystem

These rules strengthen the Digital Public Infrastructure (DPI) by improving trust and reliability in mobile-based services. They also align with India's broader strategy for a secure and resilient digital economy, protecting both users and businesses from cyber threats.

Source - https - //www.hindustantimes.com/india-news/govt-enforces-regulations-for-telecom-cyber-security-101761246752343.html