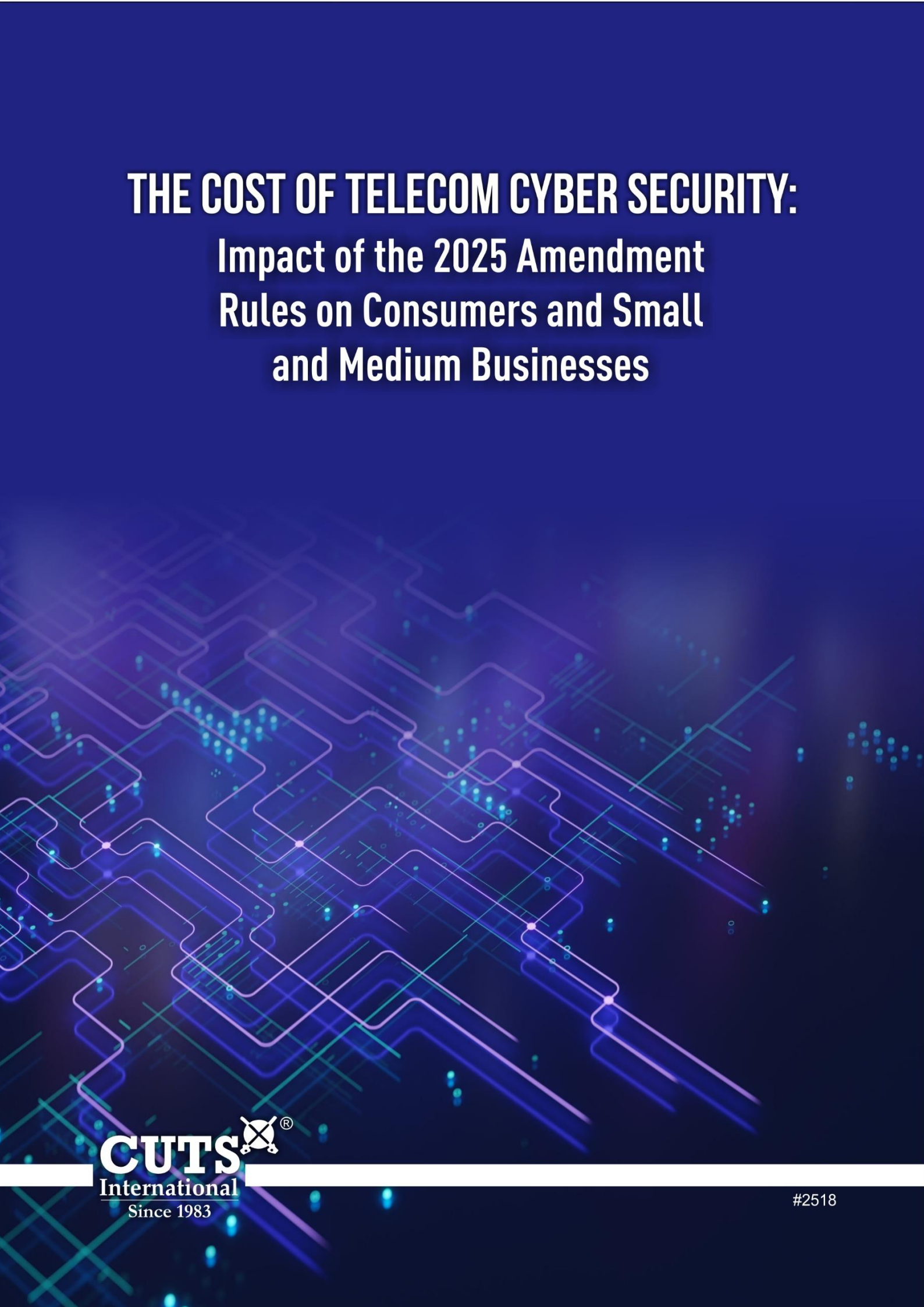
# THE COST OF TELECOM CYBER SECURITY:

## Impact of the 2025 Amendment Rules on Consumers and Small and Medium Businesses



CUTS International
Since 1983

#2518

# The Cost of Telecom Cyber Security

## *Impact of the 2025 Amendment Rules on Consumers and Small and Medium Businesses*

*Published by*

CUTS International
Since 1983

**CUTS International**
D-217, Bhaskar Marg, Bani Park, Jaipur 302016, India
Tel: +91.141.2282821, Fax: +91.141.2282485
Email: cuts1@cuts.org, Web site: www.cuts-international.org

**Author**: Krishaank Jugiani, Senior Research Associate, CUTS International. For any clarifications or further details, please feel free to contact him at: kju@cuts.org

**Acknowledgement**: The author is grateful for the support and guidance of Amol Kulkarni, Director (Research), CUTS International (amk@cuts.org)



#2518

# Contents

# Executive Summary

The Telecommunications (Telecom Cyber Security) Amendment Rules, 2025, mark a significant expansion of India's telecom cybersecurity framework. The Rules introduce two key mechanisms. One: the Mobile Number Validation (MNV) system for verifying telecom identifiers on digital platforms, and stronger controls for tracking devices via their International Mobile Equipment Identity numbers. The stated goal is to reduce identity theft, SIM fraud, and misuse of telecom identifiers. While the intent to strengthen cybersecurity is essential, the Rules raise concerns about cost, privacy, feasibility, and proportionality. Despite broad public consultation, most stakeholder suggestions were not accepted, and the Department of Telecommunications did not provide reasons for its decisions.

The Rules impose significant compliance obligations on digital platforms, including banks, fintech, e-commerce, and OTT services, requiring them to verify whether a mobile number corresponds to the registered user in the telecom operator's database, through the MNV platform. The final version removes fixed validation fees and instead links charges to the values specified on the portal. This creates uncertainty about costs, possible differential pricing, and approval procedures. For startups and smaller firms, this unpredictability could hinder budgeting, increase compliance expenses, and reduce competitiveness. Increased compliance burden could also stem from overlap with existing regimes such as CERT-In, RBI, the Data Protection Act, and the proposed Caller Name Presentation.

There are also risks of digital exclusion. Women, children, and other dependent users of shared devices, particularly from low-income segments, could lose access to digital services if strict verification is enforced. National surveys and studies show that personal device ownership remains uneven in India, especially among marginalised social groups. In these cases, mandatory name matching between user identity and SIM ownership can cause authentication failures and service disruptions. Such verification failures could translate into real-world exclusion from vital services — government benefits, digital banking, healthcare, and education platforms.

The Rules give the Government discretion over voluntary access to the MNV platform and allow revenue sharing with telecom operators, raising concerns about transparency and regulatory intent. They also expand government access to telecom identifier data without clear privacy safeguards.

To address these challenges, the Rules should be harmonised with existing legal and regulatory frameworks to avoid duplication. A risk-based, proportionate approach should guide compliance requirements, particularly for startups and MSMEs. Transparent and equitable pricing models, clear due-process safeguards for suspension or revocation, and pilot testing before nationwide rollout are essential. The government should also conduct Regulatory and Privacy Impact Assessments to ensure that policymaking is informed and evidence-based. Such a coordinated framework would strengthen cybersecurity while also safeguarding digital inclusion, innovation, and stakeholder confidence.

# 1 Introduction

The Department of Telecommunications (DoT) notified the Telecommunications (Telecom Cyber Security) Amendment Rules, 2025 (herein referred to as 'the Amendment Rules' or 'the Rules') on October 22, 2025.[1]

The final Rules have been published with only marginal modifications from the draft version.[2] Indicating that the government has largely retained its originally proposed regulatory design. During the consultation process on the Draft Amendment Rules, several stakeholders, including industry bodies, civil society organisations, and policy research groups, submitted detailed comments and alternative design suggestions.[3]

These submissions raised concerns about proportionality, overlap with existing cybersecurity regulations, and the risk of unintended user exclusion. Despite the wide range of feedback, the final Rules reflect only minor textual changes, and the DoT has not publicly provided a statement of reasons for proceeding with its proposed version. As a sound rule-making practice, the DoT should have published its reasons for proceeding with the proposed version of the Rules despite extensive stakeholder feedback and alternative design suggestions submitted during the consultation process.

Rule 7A(1) of the Amendment Rules states that the objective is to strengthen telecom cybersecurity and prevent security incidents, addressing the growing cybersecurity risks in India's telecom ecosystem. The DoT is empowered to direct Telecom Identifier User Entities (TIUEs) to use the Mobile Number Verification (MNV) platform to confirm whether a number corresponds to the registered user in the telecom operator's database. These will include all entities that use telecom identifiers, such as streaming platforms, fintech apps, food delivery apps, gaming apps, payment apps, insurance companies, edtech apps, OTTs, ride-hailing services, physical retail outlets, and banks.

1 https://egazette.gov.in/WriteReadData/2025/267074.pdf

2 https://dot.gov.in/sites/default/files/Gazette%20Notification%20Draft%20Telecom%20Cyber%20Security%20Amendment%20Rules.pdf?download=1

3 See: https://cuts-ccier.org/pdf/comments-on-the-draft-telecommunications-amendment-rules-2025.pdf; https://internetfreedom.in/iffs-submission-to-the-dot-on-the-proposed-amendments-to-the-interception-rules-the-cyber-security-rules/; https://sahamati.org.in/wp-content/uploads/2025/07/250723_Sahamati_Feedback_-Draft-Amendments-to-Telecom-Cyber-Rules-2024_MNV-platform.docx.pdf; https://www.linkedin.com/posts/kautilya-society-nluo_legislative-comments-on-the-draft-telecom-activity-7357445055692857344-_GXX; https://thedialogue.co/wp-content/uploads/2025/07/Written-Comments-Draft-Telecom-Cybersecurity-Amendment-Rules.pdf

The Central Government or its designated agency will create and operate the platform, which will forward validation requests to telecom operators and receive their responses to authenticate telecom identifiers such as mobile numbers. Participation in this system is mandatory for telecom operators and authorised entities as defined under Section 3 of the Act. These include any person who intends to provide telecommunications services, establish, operate, maintain, or expand a telecommunications network, or possess radio equipment, and who responds to validation requests from approved users.

Rule 3 of the Amendment Rules expands the government's data access powers. It authorises the DoT to request data on telecom identifiers used by TIUEs, and requires TIUEs to furnish such data "in the form and manner specified on the portal." This effectively brings platforms that use telecom identifiers, such as mobile apps, fintech platforms, OTTs, or retailers, within a broader compliance framework for data provision and information sharing with the government. The Rule also clarifies that both telecom entities and TIUEs are obligated to respond to such data requests, thereby expanding the scope of entities subject to direct regulatory oversight.

In addition to obligations concerning telecom identifiers, the Amendment Rules expand the regulatory framework to cover telecommunication equipment bearing International Mobile Equipment Identity (IMEI) numbers. The idea is to prevent the misuse of tampered or duplicated IMEIs for identity theft, cloned devices, and other telecom-related cybercrimes. Under Rule 8(4A) of the final Rule, the Central Government may issue directions to manufacturers of telecommunication equipment to ensure that no IMEI already in use in India's telecom networks is reassigned to newly manufactured or imported devices.

Further, the sub-rules (6) to (8) empower the Government, or an authorised agency, to maintain a centralised database of IMEIs that are tampered with or restricted, and require manufacturers, importers, and even dealers of used devices to check this database before sale or purchase. Access to this database will be available on payment of the fees specified on the portal. These entities must ensure that they do not deal in any telecommunications equipment whose IMEI number appears on the restricted list.

For reference, the draft Amendment Rules proposed a similar framework, with specific operational differences. It had included explicit directions to manufacturers to "provide assistance as required in relation to tampered telecommunication equipment or IMEI number" and a fixed access fee of ten rupees per IMEI for sellers and purchasers of used equipment.

However, in the final Rules, these provisions were refined—dropping the fixed ₹10 fee in favour of a dynamic fee specified on the MNV portal and clarifying the Government's power to issue directions "from a date as specified on the portal." The final text also introduced an additional compliance obligation (Rule 8(8)), requiring all manufacturers and importers of IMEI-bearing equipment to comply with any future directions issued by the Central Government for the implementation of these rules.

In addition, TIUEs are required to disclose to the DoT how they utilise telecom identifiers and to comply with the government's prescribed cybersecurity standards. They must also suspend use of any mobile number upon instruction from the DoT. If the DoT detects the misuse of a telecom identifier, it may order telecom operators and TIUEs to block or deactivate the number immediately in the public interest, without prior notice, while recording its reasons in writing. The Rules mandate two categories of entities to request validation from the MNV platform:

1. A TIUE, either *suo moto* or upon direction from the Central or State Government or an authorised agency; and
2. The Central or State Government or its authorised agencies themselves.

TIUEs may place validation requests upon payment of fees, as specified on the MNV platform. Where a TIUE seeks to use the MNV platform voluntarily, the decision to permit such access rests with the Central Government. The Rules further provide that the fees charged for using the platform shall be shared between the Government or its authorised agency and the telecom licensee or authorised entity providing validation services.

The DoT aims to prevent escalating telecom-related cyber threats, such as identity theft, SIM-swap fraud, and IMEI misuse.[4] The idea is to combat the misuse of dormant, stolen, fraudulently acquired, unused, forgotten, or otherwise misused telecom identifiers (phone numbers, SIMs, IMEIs) that could lead to security incidents, including identity theft and fraud, as well as other security incidents in the telecom ecosystem.[5]

Evidence underscores both the scale and urgency of the issue. In 2023, daily SIM-swap frauds were reported in every city, and criminals routinely exploited mobile number porting to steal OTPs.[6] Many entities, including companies, have lost crores of rupees in SIM-swap cases, highlighting the massive scale of the issue.[7] Such figures clearly

[4] https://www.mondaq.com/india/telecoms-mobile-cable-communications/1651616/draft-amendments-to-the-telecom-cybersecurity-rules-strengthening-cybersecurity-or-regulatory-overreach
[5] https://www.storyboard18.com/how-it-works/centre-tightens-telecom-cybersecurity-rules-mandates-mobile-number-validation-for-all-service-platforms-71896.htm
[6] https://www.protectt.ai/sim_binding_solution_protect_sim_swap_frauds
[7] https://perfios.ai/blogs/a-real-story-on-how-sim-swap-fraud-cost-a-company-millions/

demonstrate a systemic and widespread nature of the problem, which the Amendment Rules aim to address.

However, while the stated intent is to enhance telecommunications security, the final text raises several structural and operational concerns, particularly regarding cost implications, data protection, and the proportionality of the regulatory design. In this regard, this white paper assesses the impact of the Amendment Rules on users and small and medium businesses. It draws on the Regulatory Impact Assessment previously undertaken for the Draft Amendment Rules, but revises the discussion to include a more detailed analysis.[8]

The paper evaluates the potential impact of these Rules on small and medium businesses, consumers, and the broader digital economy. It concludes with a set of policy recommendations to ensure that the Rules do not impose disproportionate costs on users and businesses and to support digital inclusion.

[8] https://cuts-ccier.org/pdf/comments-on-the-draft-telecommunications-amendment-rules-2025.pdf

# 2 Consumers at the Crossroads: Security Gains or Service Barriers?

The Amendment Rules can have far-reaching implications for consumers, particularly for digitally marginalised groups, affecting how consumers access services, share data, and bear indirect costs. The mechanism could disrupt the current ease of access to digital services by introducing additional layers of identity verification and device authentication. While the Amendment Rules aim to enhance telecom security, they do not account for India's complex realities of mobile ownership, shared phone use, and digital literacy gaps.

As a result, millions of users, including women, older adults, children, low-income families, and rural residents, may be excluded from essential digital services or burdened by new financial and procedural requirements. These exclusion risks do not occur in isolation. They are closely linked to the economic and privacy challenges that the Amendment Rules may introduce. As access barriers rise, users may also face higher verification costs and greater exposure to personal data.

India's digital access has been premised on mobile-first connectivity, with over 1.14 billion active mobile connection users.[9] However, mobile ownership is not synonymous with mobile usage. In India, many families share a single mobile number, and children use their parents' number for essential activities, including educational apps. Approximately 85.5 percent of households possess at least one smartphone.[10] In many households, economic constraints mean that only one smartphone is purchased and shared among all members, and most Indian women use shared devices.[11]

Dependent or secondary users, like women, children, and the elderly, create accounts in their own names because services such as school apps, scholarship portals, healthcare portals, government welfare schemes, or social media profiles require personal details tied to the actual user. Similarly, there may be instances in which, for bank accounts or financial services used by senior citizens, female members, or children of the household, the mobile number of a male household member is registered. This means that even when the mobile number is listed in a father's or

[9] https://dot.gov.in/sites/default/files/Annual%20Report%20English%20Dot%202024.pdf
[10] https://www.communicationstoday.co.in/85-5-indian-households-posses-at-least-one-smartphone-mospi-survey/
[11] https://ifmrlead.org/whose-phone-is-it-anyway-women-users-india/

spouse's name, women, children, or elderly family members frequently register accounts in their own names.

This structural reality may create a significant challenge under the Amendment Rules. Since the MNV system requires the name associated with a user account to match the telecom identifier information maintained by authorised entities, a mismatch between the user's actual name and the registered owner's details could trigger an authentication failure. In such cases, women, children, or elderly family members using shared or family-owned phones may be unable to verify their identities. Consequently, their access to critical services such as digital education platforms, health portals, government welfare schemes, financial accounts, or communication apps could be interrupted or denied altogether.

Children as Dependent Users

A survey on social media usage among children found that 52 percent of parents reported their children use their own accounts, while only 31 percent said their children use their parents' accounts. This demonstrates that children, even when using a parent's phone, often set up personal accounts with their own names,[12] particularly for school platforms, exams, and learning apps. In fact, most of the 165 million children aged 5-14 years who use mobile phones do so on a shared basis, contributing an estimated 149 million to the count of non-owning users.

Among children aged 14-16, the share owning a smartphone increased from 19 percent to 31 percent over the year.[13] While access to smartphones at home is nearly universal among children, individual ownership remains significantly lower, underscoring continued reliance on shared devices. This ownership gap is critical because educational support and independent learning increasingly rely on personal accounts. It also underscores why young users often need to register accounts with their own details, even when the mobile number is not in their name.

Moreover, while parental oversight is crucial, this should not override the functional need for identity-aligned registration. Digitally literate youth must be able to manage their own credentials.[14] In recognition of these realities, policy guidelines should thoughtfully carve out exceptions for education and training platforms primarily serving young users. MNV requirements could be relaxed or replaced with institution-linked or lightweight, youth-appropriate verification alternatives. Requiring validation against the parent's SIM details in such cases could block access, even though the child is the rightful user of the account.

[12] Balancing Consent and Customisation
[13] ASER Annual Status of Education Report (Rural) 2024
[14] Economic Analysis Of Verifiable Parental Consent Mechanisms

Youth and Smartphone Ownership Trends

In 2018, nearly 90 percent of rural households owned simple mobile phones, whereas only 36 percent owned smartphones. By 2022, smartphone penetration rose to over 74 percent, and this year it has further grown to 84 percent. The National Sample Survey's 2025 Telecom report corroborates this picture. In rural areas, 80.7 percent of males and 48.4 percent of females aged between 15-29 years owned a phone. Of these, around 79.2 percent of males and 75.6 percent of females own a smartphone. Similarly, in urban areas, 90 percent of males and 71.8 percent of females aged 15 and above owned a phone. Of these, 89.4 percent of males and 86.2 percent of females owned a smart hone.[15]

In absolute terms, these gaps translate into significant numbers. Across the 1.42 lakh individuals surveyed, roughly 18,000 rural youth and over 8,000 urban youth in this age group remain without personal smartphones. These are not small margins as they raise serious concerns for digital access and identity-linked services. In contexts where phone-based verification is the norm, and where individuals may resort to using ID documents of family members or others to meet KYC requirements, the very premise of secure, person-specific authentication is undermined. Ownership matters because it determines who controls access, but it does not erase usage. Many women and girls who rely on shared devices nonetheless use them for independent purposes such as banking, telemedicine, or learning.[16]

Further, from the recently released Indian Telecom Services Performance Indicator Report, by the Telecom Regulatory Authority of India, it can be seen that while internet penetration is steadily rising, with over 100 crore internet subscribers by June 2025, the gap between connectivity and personal ownership of devices remains striking.[17]

Of these subscribers, 95.81 crore rely on wireless connections. However, these figures do not disaggregate the number of users who personally own their own phones or other devices, so the precise gap between access and personal device ownership remains undetermined. But it is safe to say that while households and shared users are counted in the surge of internet adoption, actual phone ownership is less widespread, particularly among women, children, and rural populations. This mismatch underscores that growing internet subscriptions do not automatically translate into personal digital agency, making strict name-matching requirements even more exclusionary for dependent users who participate online without owning the SIM card or device.

[15] Comprehensive Modular Survey: Telecom, 2025 NSS 80th Round (January - March, 2025)
[16] No phone of their own: How Indian women have to share mobiles | India News
[17] India's internet subscribers cross 100 crore, up 3.48 percent in March-June 2025 quarter. Check details | Mint

Women Mobile Non-Owners

Data and surveys consistently show that a significant portion of India's connected population are secondary users who create and manage their own accounts on shared devices. As per the recent Global Findex survey report 2025, even when mobile phones are distributed to women under a govt programme in India, nearly 40 percent of women had lost control over their devices within a month after distribution, despite 98 percent of women having received the phones, highlighting the gendered dimensions of device access and control.[18]

According to national surveys, around 76.3 percent of rural women aged 15 and above use mobile phones, but just 48.4 percent own one–which means roughly one in four female users does not have personal ownership of the device they operate.[19]

In a survey, among women, roughly 80 percent reported using a phone, but only about half owned one—suggesting that around 215 million women are likely secondary users. Further, a study on migrant workers in Bihar highlights how many women, mainly from marginalised and low-income groups, rely on shared family phones rather than owning their own devices.[20]

The findings are tabulated below.

| Category | Men (%) | Women (%) |
|---|---|---|
| Mobile phone ownership | 91 | 73 |
| SIM card ownership in one's own name | 83 | 64 |

The reliance on shared devices intersects with class, caste, and geography. Data from 2024 shows that 67 percent of shared device users are from rural areas, 66 percent are under the age of 19, and 59 percent are female. Among rural shared device users, 58 percent are under the age of 19, and 76 percent of these users are female. 62 percent are from NCCS CDE categories, that is, to the lower socio-economic segments as classified by the New Consumer Classification System (NCCS), which categorises households based on the education and occupation of the chief earner. This means that the last shared device users come from comparatively disadvantaged economic

[18] https://www.worldbank.org/en/publication/globalfindex

[19] https://www.livemint.com/economy/upi-usage-india-rural-women-digital-access-mobile-phone-ownership-rural-women-digital-divide-india-rural-internet-usage-11749021032545.html

[20] Historical inequalities and the unequal access to digital communications

segments and may have limited access to individual digital devices due to financial constraints.[21]

These women face a heightened risk of digital exclusion. Any mismatches between the SIM owner's and user's names could disrupt access to essential platforms, including banking, education, health, and welfare services. For millions of women who use a family member's number to access digital accounts or government schemes, this could mean being locked out of systems central to their financial and social empowerment. In effect, the Rules risk reinforcing gendered and socio-economic gaps in connectivity, undermining the very goals of digital inclusion that India's telecom and e-governance initiatives seek to advance.

Mobile Non-Owners Who Have to Register for State-Sponsored Benefits

Many women, particularly from marginalised castes and lower-income households, do not own the devices they use but rely on shared family phones. When these women sign up for digital services, whether for government schemes, for example, the Mahila Samman Savings Certificate, health platforms, or social media, they typically have to provide their own details rather than the SIM owner's.

For instance, in Rajasthan, the MAA Yojana requires women to register using their own mobile numbers to avail health benefits.[22] Similarly, the Jan Aadhaar scheme in Rajasthan treats women as heads of their families and requires them to provide personal details, including mobile numbers, for registration.[23]

Among elderly Indians, who face higher barriers to digital access, nearly 28 million phone users are estimated to depend on family-owned devices.[24] There may be several such schemes, both at the central level and across states, that follow this design.

Such users could face disruptions in accessing these state-sponsored benefits if the mobile number registered for these schemes does not match the telecom subscriber's name. Any discrepancies in names during the process could result in a denial or suspension of benefits. This would disproportionately impact women-led welfare programmes and senior citizen entitlements, effectively penalising legitimate dependent users.

Rural Mobile Non-Owners

The situation is especially pronounced in rural areas, where the share of internet users who rely on shared devices is higher than in urban areas. Data indicate that in many households, primarily rural or low-income, only one member owns a mobile phone,

[21] Internet in India 2024
[22] MAA Yojana
[23] Frequently asked questions related to Jan Aadhaar
[24] https://www.dataforindia.com/comm-tech/

while others share it.[25] This is especially true for women, children, and elderly family members,[26] Many of whom rely on their father's, husband's, or son's phone to access services such as digital payments, online learning, and food delivery.

Indeed, in India, having a family member with a phone number is the most common reason adults without accounts cite for not having their own, underscoring the prevalence of shared or proxy access to digital services. In fact, rural shared-device users have experienced a 24 percent increase since 2024, reflecting a widening gap in individual digital ownership.[27]

To illustrate, while more than 95 percent of Indian households possess at least one mobile or landline, individual-level ownership remains uneven. Among women aged 15 and above in rural areas, a staggering 51.6 percent still do not own a mobile phone outright. In urban areas, approximately 28.2 percent of women aged 15 and above do not own a mobile phone.[28] This stark contrast highlights how, despite widespread device availability, proper personal access to connectivity remains elusive for many in rural India.

For context, while Aadhaar coverage has reached nearly universal levels,[29] individual phone ownership, especially among women and marginalised groups, remains significantly lower. Data reliability is also an issue: only 1.15 crore Aadhaar numbers were deactivated over 14 years, despite more than 15 crore recorded deaths during the same period.[30] These gaps point to the need for a more nuanced approach to mobile numbers identities as well. In total, nearly 400 million Indians—primarily women, children, and older adults—may be using phones they do not personally own, underscoring a critical dimension.

Under the proposed MNV system, if a user logs in using their name but the SIM is registered to another person—such as a father, spouse, or son (in the case of seniors)—the mismatch will likely result in verification failure and denial of service. Thus, the Amendment Rules risk severing digital access for millions of "secondary users" who are legitimate but not legal subscribers.

Risks of Shifting to Alternate Modes of Verification, like Emails

Further exclusion may occur if TIUEs migrate to email-based authentication to avoid MNV charges. But email adoption in India is neither universal nor uniform, and such

[25] *Ibid*
[26] Supra Note 11
[27] Internet in India 2024
[28] Supra Note 15
[29] 99.9 percent of adults in India have an Aadhaar number and 'use it at least once a month', says UIDAI – Firstpost
[30] Crores of dead people live as Aadhaar ghosts; UIDAI trying to find tech solution - India Today

a shift may also create new safety and security risks, as email accounts are more vulnerable to phishing and credential theft than SIM-based verification, especially among first-time or low-literacy users. As discussed above, a significant portion of the digitally connected population lacks an active email address or the skills to operate one. For such users, the shift from mobile to email as the primary verification method may result in loss of access to services.

In sum, although the Rules aspire to improve telecom cyber resilience, they could inadvertently compromise accessibility, affordability, and trust—the very foundations of consumer participation in India's digital ecosystem.

*Regulatory Uncertainty and Operational Risks:* Beyond access challenges, the Amendment Rules may also pose new issues for consumers, particularly low-income users. The final Rules introduce an additional layer of uncertainty. The government may decide whether to permit voluntary (*suo motu*) use of the MNV platform, thereby preventing even willing TIUEs from accessing MNV when needed. This discretion could create inconsistency and unpredictability in service continuity, with potential implications for the consumer experience and business planning.

Furthermore, there are operational challenges related to response time and system reliability. If the MNV platform's validation request turnaround time is slow, or if network latency or congestion causes delays, users may experience timeouts or failed transactions. In high-volume consumer apps such as fintech, mobility, and food delivery, even short disruptions can lead to abandoned transactions, payment failures, and potential security risks, as frustrated users may retry or switch between platforms mid-process. Thus, even if validation requests are fewer than projected, the combined effect of approval requirements, uncertain access, and delayed responses could still impose a high hidden cost. This may erode trust in digital platforms and deter continued use, particularly among low-income and time-sensitive users.

*Cost Burdens and Economic Impact:* While access challenges may affect who can use digital services, cost implications may determine who can continue to use them. If service providers pass on the cost of compliance to consumers, even in part, users face higher service prices. A platform such as Uber, Zomato, or PhonePe, which processes millions of authentications per month, may incorporate these into its pricing structures, thereby subtly increasing access costs across urban and rural markets.

Even a seemingly nominal fee can compound quickly for end-users. For instance, if each login incurs a charge of ₹1.50 (as proposed in the Draft of the Rules) and a typical user logs in at least three times per day across different platforms, the daily cost would be ₹4.50, amounting to roughly ₹135 per month. If a typical user logs in five times per day across different platforms, the daily cost is ₹7.50, totalling to ₹225 per month. For

users logging in more frequently, such as seven times per day, the monthly expense increases to ₹315.

This figure is comparable to the price of a basic subscription plan for a digital service– whether educational, financial, or skill-building.[31] At scale, the economic impact becomes even more pronounced. With over 800 million mobile phone users in India, and assuming just 400 million interact with services offered by TIUEs, even if 10 percent of them (40 million users) are subject to verification costs of ₹135 per month, the total consumer costs could add up to ₹540 crore per month--or over ₹6,480 crore annually. For many, this cost competes with essentials.

For context, data from the Periodic Labour Force Survey (PLFS) 2023-24[32] reveals that the bottom 10 percent of earners in India have a monthly income of just ₹3,900. A validation-related cost of ₹135 per month would amount to nearly 3.5 percent of their total revenue — and could rise to over 10 percent in high-use or voluntary verification cases. In effect, this verification cost could represent a significant opportunity cost, particularly for low-income users who may be forced to reduce their usage or cancel subscriptions to other platforms that offer tangible value.

*Privacy, Data Protection, and Trust Deficits:* Beyond access and affordability, the Amendment Rules also raise deep concerns about consumer privacy and data protection. From the consumer's perspective, the expanded data-sharing requirements under Rule 3 pose significant risks to privacy and digital security. As TIUEs collect, store, and transmit personal information, the likelihood of data breaches or unauthorised access grows. This could expose sensitive identity information to malicious actors. Consumers may face increased risks of identity theft, fraud, or misuse of their personal data without their consent or knowledge. Consequently, the Amendment Rules risk exacerbating the problems identified in the intended objectives rather than resolving them.

Stakeholders have pointed to a lack of adequate safeguards, including clearly defined procedures, explicit consent protocols, and strict limitations on the use and sharing of personal data collected through verification platforms. Without these safeguards, there is a risk of conflict with the privacy principles enshrined in the Digital Personal Data Protection Act, particularly with respect to consent, purpose limitation, and data minimisation.[33]

The complexity of these data flows, and the involvement of multiple intermediaries, also reduces transparency, making it harder for consumers to know who holds their

[31] https://www.proskills.in/pricing
[32] https://www.competitiveness.in/wp-content/uploads/2025/04/Report_Labour_markets_Income_Inequality_in_India_Web_version.pdf
[33] https://www.youtube.com/watch?v=MzHNeeYSPbQ

information and how it is used. This erosion of control over personal data undermines trust in digital platforms and identity systems, discouraging users, particularly vulnerable groups such as women, the elderly, and low-income individuals, from fully engaging with digital services.

Additionally, fear of repeated verification and privacy violations may lead consumers to limit their use of essential services, such as digital payments, telemedicine, or online education, thereby deepening existing digital divides. Without robust privacy protections and precise accountability mechanisms, consumers may bear the brunt of systemic risks stemming from mandatory data sharing. Together, these factors may deepen existing digital inequalities—making it harder for already marginalised consumers to remain connected, afford services, and trust digital platforms.

# 3 Compliance, Costs, and Complexity for Businesses

While the Amendment Rules retain the broad compliance architecture proposed in the draft version, a key difference lies in how the cost of validation is treated. The final text omits specific fee figures, and instead the Rules state that the charges for use of the MNV platform will be "as specified therein", i.e., determined on the platform itself. This shift preserves flexibility for the government but leaves stakeholders unclear about pricing models and cost-recovery mechanisms. The absence of a defined structure also creates uncertainty for TIUEs, who cannot predict whether charges will vary by sector, transaction volume, or entity type. This also increases the risk of differential or preferential treatment in pricing or access decisions, which could disadvantage smaller platforms or startups operating on thin margins.

Without a clear framework for cost allocation or proportionality, compliance could become disproportionately burdensome for entities with high user volumes or low per-transaction revenues.

To assess potential financial implications, we can refer to the draft Rules, which proposed ₹1.50 per validation for government-directed requests. These provide a valuable basis for understanding the magnitude of potential costs across sectors. Even at the modest per-transaction levels, the total outlay becomes significant when scaled to the user volumes of digital platforms. For example, Zomato, with approximately 30.7 million weekly active users nationwide,[34] would have around 4.39 million daily active users.

Assuming 10 percent will require validation, which means 439,000 daily validation requests. At a rate of ₹1.5 per verification, this yields ₹658,500 per day, corresponding to ₹240.35 million (₹24.035 crores) annually. At higher compliance thresholds of 20 percent and 30 percent, these costs would increase proportionally to ₹480.71 million (₹48.07 crores) and ₹721.06 million (₹72.10 crores), respectively.

Uber India, with 33.6 million monthly active users, would have approximately 1.12 million daily active users.[35] Assuming 10 percent require validation, that's 112,000

[34] https://www.moneycontrol.com/news/business/startup/blinkit-s-weekly-user-base-of-over-30-million-within-striking-distance-of-zomato-widens-lead-over-instamart-and-zepto-clsa-13099185.html

[35] https://www.equentis.com/blog/14-cabs-31-autorickshaws-56-bike-taxis-is-rapido-set-to-outpace-ola-uber/

daily validation requests and at a rate of ₹1.5 per verification, this translates to ₹168,000 per day, or ₹61.32 (₹6.13 crores) million annually. At compliance thresholds of 20 percent and 30 percent, these costs would increase to ₹122.64 million (₹12.26 crores) and ₹183.96 million (₹18.4 crores) per year, respectively.

PhonePe has 600 million registered users,[36] and 281.96 million transactions daily in June 2025.[37] At 10 percent validations (around 28 million), it could face ₹15,330 million annually (₹1,533 Cr). For 20 percent and 30 percent validations, the corresponding annual amounts are ₹30,660 million (₹3,366 Cr) and ₹45,990 million (₹4,599 Cr), respectively.

Furthermore, more than 30,000 small and medium-sized retail brands serve nearly 1.15 billion Indians.[38] It is estimated that among these MSMEs, 51 percent handle fewer than 1,000 orders per month, 25 percent manage 1,000-10,000, and 6.6 percent process over 10,000.[39] This corresponds to more than 82 million orders per month.

Furthermore, consumers use their mobile numbers for such orders to track them and facilitate communication. If MNV validations are mandated, even at 10 percent compliance, these businesses would collectively need to validate 8.25 million orders per month, costing ₹1.24 crore per month, or ₹14.85 crore annually, at ₹1.5 per validation. At 30 percent compliance, the cost could surge to over ₹44 crore a year - a significant burden for small businesses.

The failure rate of Indian startups is exceptionally high. About 90 percent of startups fail within the first five years, with regulatory compliance cited as a critical contributing factor, accounting for about 10-20 percent of operational expenses for startups, significantly eroding capital available for innovation and scaling.[40]

The requirements for MNV and IMEI verifications would lead startups to divert a significant portion of early-stage capital to compliance. Moreover, the absence of transparent cost structures or access guarantees within the MNV framework could disadvantage smaller players, who may be unable to negotiate preferential pricing or service-level agreements with the platform. This asymmetry may result in slower request processing, higher latency, or even transaction dropouts during peak hours, each of which can severely undermine user trust and service reliability. For startups

[36] https://www.phonepe.com/press/phonepe-crosses-600-million-registered-users/
[37] https://www.rbi.org.in/Scripts/Statistics.aspx
[38] https://www.financialexpress.com/business/sme-msme-eodb-over-30000-small-medium-brands-in-retail-catering-to-80-of-indias-population-cait-2494199/
[39] https://cxotoday.com/press-release/get-the-msme-perspective-msme-highlight-their-biggest-pain-points-and-preferences-reveals-borzo-data/
[40] https://www.linkedin.com/pulse/why-indian-startups-fail-due-non-legalregulatory-kappillil-anilkumar-ziapc and https://bfsi.economictimes.indiatimes.com/news/fintech/how-much-do-indian-fintechs-spend-on-compliance/110858284

operating in high-frequency sectors such as fintech, e-commerce, or mobility, these disruptions can directly translate into lost users and revenue.

Furthermore, many startups use SIM binding, an OTP-free authentication method that enhances secure access. These entities might also be caught in this compliance, and the solution will become less feasible, thereby increasing security threats and reducing innovation.[41]

If the regulator limits obligations to big TIUEs, it might be assumed that those players can internalise costs. However, this imposes significant opportunity costs. First, the opportunity cost–even when large TIUEs absorb these expenses and divert the funds towards compliance. This might consume funds earmarked for innovation, research and development, service quality improvements, or access enhancements. These firms may reduce innovation-related investments as compliance burdens increase, thereby reducing their collaborations with or support for startups.

Second, there are waterbed effects too. When large TIUEs internalise costs, these indirect burdens can often cascade into other areas. TIUEs provide adjacent digital services, including cloud hosting, data storage, and advertising platforms.[42] and are highly likely to raise their pricing structures to offset rising compliance costs. This price escalation inevitably ripples through the digital value chain, significantly increasing operational costs for downstream service providers and small and medium-sized businesses, including startups, that rely on these platforms.

By removing the fixed rates and linking fees to what will be "specified on the platform," the final rules introduce pricing uncertainty. Businesses cannot yet model annual compliance budgets, nor can they predict whether differential pricing (e.g., by size, sector, or validation purpose) will be permitted. For startups and emerging TIUEs, this uncertainty complicates financial planning and deters early integration efforts, as per-request costs can fluctuate over time or vary across agencies. Large enterprises, while better equipped to absorb compliance costs, still face the challenge of integrating real-time validation mechanisms across user-facing systems, requiring sustained investment in technical infrastructure, API orchestration, and data governance frameworks.

Moreover, the Rules allow fees collected from each validation to be shared between the Government or its authorised agency and the telecom licensee. This raises concerns about regulatory intent. Since a cybersecurity safeguard is designed to generate revenue, the arrangement risks transforming a compliance measure into a fiscal

[41] https://economictimes.indiatimes.com/markets/options/sim-binding-in-trading-apps-how-otp-less-login-enhances-secure-trading-access/articleshow/121288349.cms

[42] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328

instrument. Importantly, the validation requirement stems from gaps in the enforcement of existing KYC and SIM issuance rules, placing the financial and operational burden of earlier implementation failures on end users and businesses. This approach, rather than strengthening cyber resilience, may inadvertently blur the line between regulatory cost recovery and commercialisation, creating the risk of uneven treatment among TIUEs.

Beyond direct per-query fees, the Amendment Rules can impose substantial operational burdens on TIUEs that extend well beyond per-query verification fees. Managing the MNV system will require API integration, real-time monitoring of verification requests, handling failures, managing disputes, and coordinating with platforms. For small and mid-sized firms, this translates into hiring or reallocating staff, including compliance officers and technical personnel. These are recurring operational expenses that divert resources from core product development, innovation, or service delivery to compliance and potentially unproductive uses – especially for startups or lean firms operating on tight margins.

This is also distinct from the time spent understanding the mechanism, addressing verification failures, and ensuring compliance with evolving regulatory protocols. For startups, these obligations divert scarce human resources away from core product development and innovation. Even if parts of the process can be automated, doing so requires upfront investment, ongoing human oversight, and continuous system upgrades, which could further strain limited early-stage capacities.

The requirement will also demand significant investment in digital infrastructure. Firms will have to build and maintain secure API integrations, ensure latency and transaction integrity, develop real-time dashboards for query monitoring, and maintain audit trails. These technical requirements are capital-intensive. Moreover, firms will need to budget for ongoing updates, platform alignment, and periodic security enhancements. These costs are particularly burdensome for smaller players who lack economies of scale or in-house engineering bandwidth.

Collectively, these factors suggest that the Amendment Rules, though well-intentioned, could impose high compliance costs with limited demonstrable benefit, potentially constraining innovation and competitiveness within the digital ecosystem. Moreover, the rule-making process itself raises concerns. Conducting a public consultation only to disregard substantial stakeholder feedback sends a discouraging signal about regulatory predictability and responsiveness.

# 4 The Ripple Effect: Impact on India's Digital Economy

The Amendment Rules may threaten India's digital economic ambitions by introducing structural inefficiencies and exclusionary costs. These include financial and operational burdens on these entities, compounded at scale, that distort competition, undermine the growth and dynamism of telecom markets, and limit consumer access. For instance, in 2022-23, India's digital economy accounted for 11.74 percent of the GDP (₹31.64 lakh crore or US$402bn)[43] and is expected to rise to 13.42 percent by 2024-25.[44] Assuming the growth rate slows by 10 percent due to increased costs, compliance friction, uncertainty, unpredictability, unfair conduct, and restricted market access, this could have resulted in a loss of more than ₹2.5 lakh crore in economic activity by FY2025 alone.

The impact would be more severe for startups and new entrants. For instance, by 2025, more than 159,000 startups have been recognised under the Startup India initiative.[45] In 2023, the number was 117,254.[46] The corresponding figure for direct jobs is 1.7 million. If this momentum is reduced by even 10 percent, approximately 4,000-5,000 potential startups may be excluded from the market, risking the loss of nearly 150,000-200,000 direct jobs and a significantly higher indirect employment impact through service networks and vendor linkages.

This deceleration in entrepreneurial growth is closely tied to consumer access and digital adoption dynamics. During the same period (March 2023 to march 2025), the wireless (mobile) subscriber base grew from 1,143.93 million[47] to 1,163.76 million,[48] registering a net addition of 19.8 million users. This corresponds to a total growth of approximately 1.73 percent over the two years. A 10 percent decline in new user additions would result in roughly 2 million fewer consumers gaining access to mobile and internet services over two years. The introduction of additional costs for device resale and MNV verification will disproportionately affect first-time users, who often rely on affordable second-hand smartphones. These users, predominantly from rural and aspirational districts, are susceptible to price increases.

43 https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2097125
44 https://indbiz.gov.in/indias-digital-economy-to-outpace-national-growth-by-2030/
45 https://www.orfonline.org/research/reflections-on-the-first-decade-of-startup-india
46 https://www.pib.gov.in/PressReleasePage.aspx?PRID=2002100
47 https://www.trai.gov.in/sites/default/files/2024-09/16th.pdf
48 https://www.trai.gov.in/sites/default/files/2025-05/PR_No.35of2025_0.pdf

For India, which is still attempting to bridge the digital divide, especially in rural and aspirational districts, this slowdown would disproportionately affect first-time users, who often rely on low-cost services. In effect, this would deepen digital exclusion among those at the very edge of inclusion.

When combined, the costs of both MNV validation fees constitute a persistent microtax on digital access. For lean startups and smaller TIUEs, these fees erode margins and viability by diverting scarce resources away from innovation, product development, and customer service improvements. Ultimately, this cumulative burden threatens to stifle competition, reduce consumer choice, and slow India's progress toward a more inclusive digital economy.

This challenge becomes even more significant when considering that limited consumer access and heightened compliance costs may also disincentivise new service providers. The rapid expansion of India's startup landscape has also introduced a phenomenon often referred to as "startup dwarfism," in which many small startups struggle to scale effectively. This risk will deepen due to the financial and operational burden imposed by the Amendment Rules. Many new entrants to the startup ecosystem may feel disincentivised and demotivated by the upcoming compliance burden.

This trend is at risk of deepening due to the financial and operational burdens imposed by the Amendment Rules. The cumulative effect of compliance risks diverts scarce resources from core product development, market expansion, and research & development, hindering nascent ventures' ability to achieve sustainable growth and compete effectively in the broader market.

# 5 Potential Implementation Challenges with the MNV System

However, we need to analyse how the MNV platform will operate. For instance, the Amendment Rules only describe the MNV platform, and that it will be used for "validation as to whether the telecommunication identifiers as specified by their customers or users, correspond to the users as available in the database of an authorised entity or licensee".

Users who do not match the provided data may be disconnected or suspended. Yet it is unclear how frequently records will be updated or how disputes (e.g., subscriber-username mismatches) will be resolved. This makes it unclear whether the platform will respond with "valid/invalid" or provide more nuanced data. But more importantly, how will it handle edge cases in which the identity has been previously compromised or stolen?[49]

Moreover, fraudsters have repeatedly demonstrated the ability to obtain subscriber identities and bypass validation systems. Court and STF investigations have found criminal networks using fake or stolen Aadhaar credentials to activate SIM cards and then leveraging those SIMs for fraud or resale, without triggering detection.[50]

If the identity attributes (SIM subscriber, Aadhaar, alternate number, photographs) are stale or forged, and verification does not include robust live or liveness checks, the MNV platform will merely replicate existing fraud rather than prevent it.[51] Most such frauds stem from upstream vulnerabilities, such as weak KYC processes, gaps in telecom identifier issuance, or insufficient verification.[52]

The Rules may not adequately address issues such as SIM misuse, data leaks of customer details through cyber breaches, and misreporting and reissuance of SIMs for fraud.[53] A fraudster using a stolen or SIM-swapped number, but paired with the legitimate subscriber name, would still pass validation.

[49] https://www.insightfultake.com/details/indias-cybersecurity-gamble-can-mobile-number-verification-stop-digital-fraud?utm_source=chatgpt.com
[50] https://the420.in/up-stf-busts-illegal-sim-card-gang-prayagraj/
[51] https://www.insightfultake.com/details/indias-cybersecurity-gamble-can-mobile-number-verification-stop-digital-fraud?utm_source=chatgpt.com
[52] https://telecom.economictimes.indiatimes.com/news/industry/cbi-cracks-down-on-pos-generating-ghost-sim-for-cybercriminals/121245390
[53] https://timesofindia.indiatimes.com/city/delhi/sim-swap-fraud-over-100-customers-duped/articleshow/92421686.cms

Operationally, the system also faces monumental logistical challenges. With over 1.1 billion active mobile connections,[54] The platform will need to manage, refresh, and respond to massive real-time queries. Maintaining latency, accuracy, and data integrity at this scale is itself a security vulnerability. It may create a honeypot for fraudsters, as any compromise of the verification API or mobile identity database could trigger systemic disruption or mass deregistration.[55]

Further, the validation process introduces added dependence on government discretion. TIUEs using the MNV platform voluntarily must first obtain approval from the Central Government. This could create administrative delays and unpredictability in service continuity. The lack of transparency in how approvals will be granted or withheld can generate uncertainty and uneven treatment among TIUEs, notably smaller or newer entrants that may not yet have established regulatory interfaces. This additional administrative step compounds the broader operational unpredictability of the MNV framework, heightening compliance risk and deterring early adoption by responsible players who would otherwise support its intended cybersecurity objectives.

Furthermore, it may not be easy to develop a clear, logical rationale for distinguishing between large and small TIUEs. Will the basis of differentiation be total users, active users, revenue generated by TIUEs, profit made by TIUEs, the utility of unique mobile numbers for logging in and communication by TIUEs, fraud attempts against TIUEs, or measures implemented by TIUEs to address scam, spam, and fraud callers?

Some TIUEs with large user bases may not be profitable, and it may not be reasonable to expect them to internalise the cost of telecom cybersecurity. At the same time, some niche TIUEs with smaller active user bases may be profitable. The guidance provided by the DPDP Act on the Significant Data Fiduciary may be of little use in this case. Ultimately, these accumulated costs can translate into increased prices for end consumers.

[54] https://www.trai.gov.in/sites/default/files/2025-06/PR_No.51of2025_0.pdf
[55] https://www.insightfultake.com/details/indias-cybersecurity-gamble-can-mobile-number-verification-stop-digital-fraud?utm_source=chatgpt.com

# 6 Risks of Arbitrary Suspension and Revocation

The Amendment Rules also expand the government's power to suspend or revoke the use of telecom identifiers. Under the substituted Rule 5(6), the Central Government may, "in the public interest," order the temporary suspension of a telecommunication identifier by both the telecom entity and the TIUE, without prior notice, if it considers immediate action necessary. While the provision requires that reasons be recorded in writing, it does not mandate prior disclosure, notice to affected entities, or a mechanism for review.

Such broad discretion, exercised without procedural safeguards, risks arbitrary or disproportionate disruption of services. The suspension of identifiers used for communication, financial transactions, or digital authentication can instantly cut users off from essential services and expose businesses to operational losses. Furthermore, where identifiers have already undergone regulated KYC verification, automatic suspension based on an MNV mismatch may penalise both compliant entities and innocent users for systemic or technical errors rather than malfeasance. In the absence of a transparent review or appeal process, these provisions raise rule-of-law concerns and create uncertainty in business continuity and consumer access.

# 7 Concerns with Existing KYC Processes and the Need for Strengthened Safeguards

It is essential to understand the current landscape of telecom fraud and the government's ongoing efforts to address it. Examining existing measures provides context for assessing whether the MNV platform and other regulatory interventions can effectively mitigate persistent vulnerabilities.

There have been efforts to curb such incidents. In 2023, of the 1.14 billion active mobile connections in India, over 6.6 million were flagged as suspicious, resulting in 5.2 million disconnections and the blocking of over 67,000 telecom dealers. Moreover, nearly 1,700 FIRs have been filed against dealers involved in fraudulent KYC practices.[56] 2024 data show that 7.3 million connections obtained via forged documents were also identified in mid-year.[57]

In response, authorities have stepped up their efforts. Till October 2024, using AI-driven systems, 1.77 crore mobile connections acquired through fraudulent or forged documents had been identified and deactivated. Furthermore, 45 lakh spoofed international calls have been blocked from infiltrating India's telecom network.[58] Consequently, several initiatives already exist to address the problem.

The framing of the Amendment Rules remains too narrow, given the broader threat environment. The core issue lies not solely in the misuse of telecom identifiers but in the porous and inconsistent identity-verification processes underlying telecom KYC (Know Your Customer) and customer verification. While the DoT mandates subscriber registration through e-KYC, digital KYC (d-KYC), or paper-based KYC (p-KYC), the actual implementation of these procedures remains weak and fragmented. KYC details are collected by TSPs (Telecom Service Providers) through self-declarations from subscribers. TSPs must conduct mandatory KYC checks on users before issuing SIM cards. KYC information is basic user information, including full name, photograph, Date of Birth, and address, collected and verified against official documents such as

[56] https://www.hindustantimes.com/india-news/union-government-announces-overhaul-of-kyc-norms-for-mobile-phone-connections-to-crack-down-on-cyber-fraud-industry-101692296237181.html

[57] https://www.business-standard.com/industry/news/7-3-million-connections-obtained-on-fake-documents-shut-down-dot-124080701465_1.html

[58] https://timesofindia.indiatimes.com/technology/tech-news/govt-has-deactivated-1-7-crore-mobile-connections-blocked-45-lakh-scam-calls-so-far/articleshow/113946754.cms

Aadhaar, driving licence, PAN card, and passport. Such information may not be completely accurate, and there is a risk of information mismatch. Moreover, manual verification of KYC information is error-prone.[59] Furthermore, the forging of such official documents to obtain SIMs is not uncommon.

A joint study by the ISB Institute of Data Science and the Telangana Cyber Security Bureau found that telecom SIM subscription fraud continues to thrive, with identity verification failures at the core of the problem.[60]

The study, based on analyses of over 1,600 Customer Acquisition Forms (CAFs), public complaints, and real-time data, found that nearly 91.76 percent of d-KYC users submitted their Aadhaar as proof of identity. However, in 89.11 percent of these cases, the alternate number provided during onboarding was not linked to the submitted Aadhaar, rendering the OTP-based verification process largely ineffective.

While this highlights a specific Aadhaar-based vulnerability, the broader issue was that Point-of-Sale (PoS) agents failed to verify identity documents (such as Aadhaar, voter ID, and driving licences) with the issuing authorities across all KYC types. There was no real-time cross-verification of photographs from ID documents against live images captured at the time of SIM issuance, allowing fraudsters to complete onboarding with mismatched or forged credentials.[61]

Significantly, these vulnerabilities were not limited to d-KYC. Even e-KYC procedures, which involve biometric submissions, were undermined by the lack of real-time verification by PoS agents, thereby enabling identity theft and subscription fraud through stolen or spoofed credentials. These findings emerged from Telangana, a state with one of the highest per capita incomes,[62] and a rural literacy rate of 66.54 percent[63] — implying that the problem could be significantly worse in other states, where compliance and verification oversight, digital literacy, and enforcement capacity may be weaker. Hence, the national scale of flawed KYC-driven fraud may be far greater. In terms of security, the BSNL breach in July 2024 alone exposed 278 GB of sensitive telecom data.[64]

Furthermore, the data collected through KYC–often via self-declaration- is not routinely updated or re-verified, which turns it into a static and unreliable dataset over time. RTI responses indicate that the TRAI neither maintains nor verifies the accuracy

[59] https://cuts-ccier.org/pdf/comments-on-the-trai-cnap-consultation-paper.pdf
[60] https://prodcd.isb.edu/media/wkrbce4o/iids-police-report-july-23-2024-1.pdf
[61] *Ibid*
[62] https://timesofindia.indiatimes.com/city/hyderabad/telangana-leads-in-per-capita-income-essential-consumption/articleshow/118338553.cms
[63] https://ecostat.telangana.gov.in/PDF/PUBLICATIONS/Telangana_at_Glance_2024.pdf
[64] https://www.business-standard.com/companies/news/bsnl-data-breach-exposes-278-gb-of-sensitive-telecom-info-twice-in-6-mts-124062600314_1.html

of KYC data, and key infrastructure, such as the Telecom Analytics for Fraud Management and Consumer Protection (TAF-COP) portal, remains only partially operational.[65]

These findings indicate that telecom fraud primarily stems from SIM misuse or SIM issuance process leaks, facilitated by compromised KYC, rather than from misuse after issuance. Without reforming KYC protocols, enforcing agent accountability, and implementing robust biometric verification, the Amendment Rules risk treating the symptoms while leaving the core vulnerability unaddressed. These figures indicate fundamental gaps in data protection, network security, and KYC verification — issues that the current Rules do not address. While the objective of the Amendment Rules is valid, they address only one dimension of a broader telecom cybersecurity crisis.

[65] Supra Note 61

# 8 Need to Strengthen Existing Measures to Combat Telecom Fraud

Several existing frameworks already target the core issues of telecom fraud and cybercrime, indicating that the Amendment Rules duplicate regulatory efforts rather than build on them. The Indian Cyber Crime Coordination Centre (I4C), established under the Ministry of Home Affairs, already spearheads cross-jurisdictional coordination among law enforcement agencies to combat telecom-related fraud. Its initiatives include the National Cyber Crime Reporting Portal, the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS), and a dedicated helpline (1930). Under I4C's aegis, over ₹5,489 crore has been recovered from fraudsters through 17.82 lakh citizen complaints, and more than 9.42 lakhs SIMs and 263,348 IMEIs linked to scams have been blocked.[66]

These efforts directly address cross-servicing risks and identifier abuse, but the new MNV and IMEI mandates could overburden entities and increase compliance burdens.

Telecom operators further employ advanced AI/ML systems to detect anomalous call patterns, block spam SMS/calls, and flag suspicious transactions in real time.[67] Google's DigiKavach initiative, launched in 2023, partners with I4C and fintech associations to leverage AI-driven alerts and user-awareness programmes.[68]

Sectoral regulators such as RBI and SEBI already enforce KYC protocols for financial and capital-market services.[69] They also use other methods, such as Multi-Factor Authentication and Two-Factor Authentication, which are widely adopted and require users to provide two or more verification factors, such as a password + One-Time-Password via SMS, email, or an authenticator app, or a password + biometric scan, significantly increasing security against unauthorised access.

India's digital ecosystem already operates under a web of cybersecurity and data protection mandates designed to safeguard users and institutions across sectors. The

66 https://www.pib.gov.in/PressReleasePage.aspx?PRID=2146786
67 https://timesofindia.indiatimes.com/business/india-business/airtels-ai-powered-fraud-detection-system-blocked-1-8-lakh-malicious-links-shielded-5-4-million-users-in-telangana/articleshow/121783678.cms
68 https://blog.google/intl/en-in/company-news/googles-safety-charter-for-indias-ai-led-transformation/
69 https://economictimes.indiatimes.com/news/economy/policy/rbi-know-your-customer-kyc-rules-customer-onboarding-aadhaar-biometric-norms/articleshow/121797850.cms

Computer Emergency Response Team – India (CERT-In) provides national-level incident response and security guidelines, including mandatory breach-reporting and log-retention requirements. In the financial sector, the Reserve Bank of India (RBI) enforces stringent cybersecurity frameworks for banks and payment systems, ensuring resilience against threats such as phishing, ransomware, and data theft. Complementing these is the Digital Personal Data Protection Act, 2023, which mandates lawful processing of data and accountability for data breaches.

Adding another layer, telecom operators are piloting the Calling Name Presentation (CNAP) feature, a verified caller-ID system that displays a caller's name based on SIM-KYC records.[70] CNAP could help users identify legitimate callers, curbing impersonation and scam calls. Introducing the MNV framework alongside these existing measures could increase regulatory overlap and compliance complexity, adding another layer of verification and reporting obligations for entities already subject to multiple cybersecurity regimes. Instead of simplifying telecom identity management, it risks fragmenting compliance across overlapping mandates and escalating costs, particularly for smaller firms and platforms that may now have to integrate with both CNAP and MNV systems.

There are also victim support and grievance redressal mechanisms, such as through the National Cyber Crime Reporting Portal. It enables streamlined FIR registration across jurisdictions, and the I4C-launched e-Zero FIR in Delhi facilitates rapid incident reporting without jurisdictional hurdles.[71]

Finally, existing regulations aim to address impersonation, spam, and fraud across telecom and OTT channels, via both the Telecom Commercial Communications Customer Preference Regulations (TCCCPR-2018) and the IT Act. These Rules require telecommunications providers to scrub headers, block unregistered telemarketing calls, and penalise fraudulent communication. The IT Act also prescribes offences, including cheating by personation and identity theft, for OTT platforms under Sections 66C and 66D.[72]

Thus, India's policy landscape already includes a mix of institutional mechanisms, technological solutions, and legal safeguards to combat the fraud described above. The real challenge, however, lies in strengthening, effectively implementing, and cohesively integrating these efforts across fragmented telecom vendors, financial

[70] https://www.indiatoday.in/technology/news/story/india-to-launch-its-own-caller-id-tech-cnap-here-is-how-it-could-rival-truecaller-2811207-2025-10-31

[71] https://timesofindia.indiatimes.com/business/cybersecurity/e-zero-fir-initiative-launched-to-fast-track-cyber-fraud-cases-pilot-begins-in-delhi/articleshow/121379802.cms; https://www.business-standard.com/industry/news/cnap-service-nationwide-rollout-by-march-2026-dot-trai-telecom-125102901190_1.html

[72] https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=2080641

institutions, law enforcement agencies, and both traditional and OTT communication platforms.

Rather than addressing these coordination gaps, the Amendment Rules introduce overlapping regulatory regimes. Instead of fostering an interoperable, collaborative framework, they risk imposing additional compliance burdens on already regulated entities. This structural friction may undermine user trust, stifle innovation, and increase operational complexity. What is needed is regulatory convergence and targeted enforcement, not duplication and diffusion of accountability. The Amendments Rules risk doing the latter, at the cost of the former.

# 9 Recommendations

The Amendment Rules introduce critical compliance obligations for businesses, startups and industry, with reverberating effects on consumers and the digital economy. The recommendations below aim to recalibrate the framework so that telecom cybersecurity objectives are met without imposing disproportionate costs, creating overlap with existing regimes, or undermining digital inclusion.

### Adopt a Risk-Based, Graded Verification Model (User-centric Approach)

The Amendment Rules risk severing digital access for millions of dependent users. If strict name-matching requirements are enforced without recognising shared SIM/device realities, legitimate shared users — particularly women, children, and the elderly in rural and low-income households — will be disproportionately excluded.

A viable solution, drawing on banking precedents, is to adopt a risk-based, graded verification model rather than rigid one-size-fits-all mandates. The RBI's approach — allowing low-risk customers continued access while KYC updates are pending, enabling e-KYC, video KYC, and business correspondent support — provides a valuable template. Translating this flexible, risk-calibrated framework to the telecommunications sector could preserve access for underserved populations while maintaining verification standards for high-risk transactions.

### TIUE Scope: Risk-based, Use Case-led and Non-Duplicative

The purpose of the Rules is to strengthen telecommunications cybersecurity and reduce fraud associated with the misuse of mobile numbers. The definition of TIUEs should therefore be revised to target entities in which the misuse of telecom identifiers can cause the most significant harm — platforms that use mobile numbers to authenticate access to regulated financial services or critical government services.

- High-risk entities (regulated financial services, essential government platforms, critical information infrastructure as per the IT Act / NCIIPC) should be subject to full obligations under the Rules.
- Communication-centric entities (messaging platforms, bulk-SMS providers, VoIP services) require tiered obligations proportionate to the functions they provide and the specific risks (financial fraud, AML/CFT, CSAM, etc.). Definitions should align with the Information Technology Act, 2000.
- Low-risk entities that use telecom identifiers incidentally for routine notifications (transactional alerts, service messages) should be excluded from onerous obligations.

- MSMEs and DPIIT-recognised startups should generally be excluded or offered simplified compliance pathways to protect ease of doing business and innovation.

Where sectoral regulators (RBI, SEBI, IRDAI, PFRDA) prescribe their own requirements, duplication should be avoided. Designation of such entities as TIUEs should occur only through explicit direction by the relevant regulator. Entities that can credibly demonstrate effective measures to curb misuse and provide adequate redress for affected users should also be excluded, thereby ensuring proportionate regulation focused on genuine risk.

| **Suggestions to Rationalise the Scope of TIUE** |
| --- |
| The Rule 2(b)(i) shall be substituted with following:<br><br>Telecommunication identifier user entity (TIUE)" means a person, other than a licensee or authorised entity, *that uses telecommunication identifiers for purposes of authentication of users to provide its services, and which falls within one of the following categories:*<br><br>*(a) entities that use telecommunication identifiers as a primary means to authenticate users for: (i) providing government services or benefits; or (iii) enabling access to critical information infrastructure, as defined in Section 70 of the Information Technology Act, 2000. These entities shall comply with all obligations under these Rules.*<br><br>*(b) entities (i) whose primary business is the transmission or exchange of information as defined under the Information Technology Act, 2000 (including messaging platforms, bulk SMS aggregators, VoIP/calling services), or (ii) which are regulated and the relevant sectoral regulator issues a specific notification designating such entities as TIUE for these Rules. These entities shall be subject to tailored obligations under these Rules, designed to address the financial fraud, anti-money laundering, countering the financing of terrorism, and child sexual exploitation and abuse material risks posed in the relevant sector in which such entities operate.*<br><br>*Provided that entities that can certify they have taken sufficient measures to curb misuse of telecom identifiers on their platforms and give redress to users in this regard are subject to proportionate obligations, including reporting attempts to misuse, blocking such attempts, implementing grievance redress mechanisms, and periodic disclosures.*<br><br>*Provided that a TIUEs shall exclude –* |

| Suggestions to Rationalise the Scope of TIUE |
| --- |
| *(i) entities which only use telecommunication identifiers for routine customer communication, including but not limited to, service notifications, or transactional alerts; and*<br><br>*(ii) Micro, Small and Medium Enterprises as defined under the Micro, Small and Medium Enterprises Development Act, 2006, and startups recognised by the Department for Promotion of Industry and Internal Trade, shall be excluded from the scope of TIUEs.* |

### Clear Validation Scenarios with Strong Safeguards

The Rules should specify the precise scenarios in which TIUEs may undertake validation requests to ensure MNV is used proportionately. Validation should be permitted for lawful authentication of new users, validity checks triggered by internal risk alerts, or when there is a reasonable suspicion of fraud. TIUEs undertaking *suo motu validations should be required to record the reasons in writing, thereby* creating an auditable trail. Similarly, the government should record and disclose the reasons for permitting or withholding approval of voluntary validations, as required under the Rules, to promote accountability and prevent arbitrary decision-making.

When validation is undertaken pursuant to government directions, safeguards must be strengthened: directions should be issued only by a senior government officer, be reasoned, specific, and time-bound, and remain subject to review by an independent adjudicatory authority. These measures balance national security and fraud-prevention objectives with due process and protection against arbitrary action.

The corresponding change to Rule 7A(3) should clarify that government entities may use the MNV platform in the same scenarios to reduce regulatory uncertainty and ensure consistent application.

| Suggestions to clarify the scenarios wherein validation can be undertaken |
| --- |
| *(a) A TIUE may, on a suo moto basis, in accordance with this rule, place a request on the MNV platform in the form and manner as specified therein, and on payment of fees as determined in accordance with the Schedule to these rules, seeking validation of whether the telecommunication identifiers as defined by their customers or users correspond to the users as present in the database of an authorised entity or licensee, subject to the following conditions–*<br><br>*(i) for lawful authentication of a new customer or user; or* |

| Suggestions to clarify the scenarios wherein validation can be undertaken |
| --- |
| *(ii) where the TIUE's internal monitoring systems have generated a risk alert indicating possible fraudulent or suspicious use of a telecommunication identifier; and in each such case, the TIUE shall record in writing the reasons and justification for seeking such validation.*<br><br>*(b) A TIUE may, upon a direction issued by the Central Government or State Government in accordance with this rule, place a request on the MNV platform in the form and manner as specified therein, and on payment of fees as determined in accordance with the Schedule to these rules, seeking validation of whether the telecommunication identifiers as specified by their customers or users correspond to the users as present in the database of an authorised entity or licensee, wherein the government's internal monitoring systems have generated a risk alert indicating possible fraudulent or suspicious use of a telecommunication identifier; and in each such case, the direction from the Central Government or State Government shall—*<br>*(i) be issued only by an officer not below the rank of Additional Secretary (Telecom) in the case of the Central Government, or not below the rank of Chief Secretary in the case of a State Government; and*<br>*(ii) be made in writing and shall state the legal basis, the specific objective sought to be achieved, the material relied upon, and the reasons for which MNV is considered necessary; and*<br>*(iii) be specific in scope and time-limited, unless renewed through a fresh direction meeting the requirements above.*<br><br>*Provided that any such direction from the Central Government or State Government shall be subject to review by an independent adjudicatory authority designated for this purpose, within a period of fifteen working days.* |

## Equitable and Market-Linked Fee Structure

The fee structure should be rational, transparent, and grounded in market principles, with mutual agreement between TIUEs and authorised entities or licensees. Documentation must be public and subject to periodic review based on volume, costs, and risk. Mechanisms for graded pricing, bulk discounts, or exemptions for low-volume entities and MSMEs should be built in to avoid disproportionate burdens. Transparent revenue-sharing arrangements should be disclosed to prevent perverse incentives.

| Suggestions to Implement the Fee Structure |
| --- |
| *(c) The fees payable by a TIUE for placing a request on the MNV platform under clause (a) or clause (b) shall be determined by mutual agreement between the TIUE and the telecommunication entity operating the MNV platform, having due regard to the following factors–*<br>*(i) the volume of validation requests placed by the TIUE within a defined period;*<br>*(ii) the resources required to process such validation requests, including technical, infrastructural, and personnel costs; and*<br>*(iii) the risk of misuse of the telecommunication identifiers to access the services of the relevant entity, as reasonably assessed by the parties,*<br><br>*Provided that such fees shall be documented in writing and subject to periodic review by the parties,*<br>*(i) having regard to any material change in the volume of requests, resource requirements, or assessed risks; and*<br>*(ii) in a manner that ensures transparency, reasonableness, and proportionality in relation to the services rendered by the authorised entity or licensee.* |

### Rule-of-Law Safeguards for Enforcement

Introduce procedural safeguards into suspension or revocation processes that directly affect users' ability to communicate and access essential services. Require a written show-cause notice, disclosure of evidence, and reasonable opportunity for response and hearing. Orders should be reasoned, proportionate, and based on the nature of harm. An independent adjudicatory authority should review final orders to reinforce impartiality.

Provide for urgent interim suspension only in cases of imminent and grave harm, with recorded reasons, emergency hearings, and prompt review. Explicitly recognise that prior regulated KYC verification should shield entities and users from adverse action based solely on an MNV mismatch. Finally, guarantee a right of appeal to a judicial authority so that remedies are consistent with constitutional due-process norms.

| Rule-of-Law Safeguards for Suspension or Revocation of Identifiers |
| --- |
| In rule 5,<br>(a) Sub-rule (6) shall be substituted with the following: -<br><br>*Where the Central Government, based on information received under sub-rule (1), has reasonable grounds to believe that a telecommunication identifier is being used in contravention of rule 4, it shall issue a written show-cause notice to the person to whom such identifier has been issued. The notice shall–* |

**Rule-of-Law Safeguards for Suspension or Revocation of Identifiers**

*(a) specify the particulars of the alleged contravention;*
*(b) provide all relevant materials and evidence on which such belief is based, along with a copy of such material and evidence; and*
*(c) grant the person a reasonable opportunity, of not less than fifteen working days from the date of receipt of the notice, to submit a written response, including any material to correct factual inaccuracies or demonstrate compliance, and to be heard in person or through a legal representative.*

*A copy of the show-cause notice and any subsequent orders must be served on the end user associated with the telecommunication identifier.*

*(A) After considering the response, the Central Government may, if it finds that a contravention has occurred, place the matter before an independent adjudicatory authority designated for this purpose, along with the evidence and its recommendations.*

*(a) The adjudicatory authority shall, after affording the affected person a reasonable opportunity of being heard, pass a reasoned order in writing which may include directions to the telecommunication entity and, where applicable, the TIUE, to—*
*(i) temporarily suspend the use of the relevant telecommunication identifier for a specified period not exceeding fifteen working days; or*
*(ii) permanently disconnect or prohibit the use of the relevant telecommunication identifier.*

*Where an order of suspension, disconnection, or prohibition is withdrawn or modified to permit continued use, the relevant telecommunication identifier shall be restored within two working days from the date of such order.*

*Provided that any such order shall be proportionate to the nature and extent of the harm caused, and must take into account: (i) the actual or potential harm resulting from the use of the relevant telecommunication identifier; (ii) the likely impact of the order on the affected user; and (iii) the overall benefit to the security of telecommunications systems.*

*(B) Notwithstanding anything contained in sub-rule (6), where the adjudicatory authority considers that immediate action is necessary to prevent imminent and grave harm, it may, for reasons recorded in writing, pass an interim order directing the temporary suspension of the relevant telecommunication identifier for a period not exceeding fifteen working days.*

**Rule-of-Law Safeguards for Suspension or Revocation of Identifiers**

*Explanation. – For this Rule, "imminent and grave harm" shall include the use of a telecommunication identifier for–*
*(a) the commission or facilitation of terrorism, or organised crime*
*(b) the commission or facilitation of money laundering;*
*(c) the distribution or transmission of child sexual abuse material;*

*Provided that a copy of such interim order, along with the reasons recorded, shall be served upon the affected person forthwith. An emergency hearing shall be granted to the person within seven working days from the date of the order, after which the interim order may be confirmed, modified, or annulled, and such order is retained for audit.*

*Provided further that any person aggrieved by an order of suspension, disconnection, or prohibition passed under this sub-rule shall have a right to appeal to a judicial authority, within thirty days of receipt of the order.*

*(C) Where a TIUE demonstrates that an account has already undergone regulated KYC verification, a mismatch on the MNV platform shall not by itself constitute grounds for adverse regulatory action or mandatory suspension.*

## Focus on Harmonisation and Strengthen Ongoing Initiatives

The government should prioritise strengthening ongoing initiatives to address telecommunications cybersecurity and avoid inconsistent or overlapping approaches. India's digital landscape is already governed by multiple sector-specific cybersecurity frameworks — including CERT-In guidelines, RBI mandates for financial institutions, and data-protection norms under the Digital Personal Data Protection Act. Overlaying an additional compliance regime without alignment risks creating an incoherent and contradictory regulatory environment.

Rather than expanding new compliance requirements through the Telecom Act alone, there is a pressing need to harmonise efforts across sectors and focus on practical implementation. An inter-ministerial coordination mechanism bringing together DoT, MeitY, RBI, and other key regulators, along with consumer groups (which can act as eyes and ears of regulators on the ground), should be established. This would ensure a unified approach to digital risk management and telecom cybersecurity, reduce duplicative obligations, promote predictability for service providers, and encourage meaningful compliance without regulatory fatigue.

## Comprehensive Regulatory and Privacy Impact Assessments

Before issuing new requirements, the government should conduct a comprehensive Regulatory Impact Assessment (RIA) and require Privacy Impact Assessments (PIAs) to quantify costs for SMBs, startups, and consumers. The RIA should examine differential impacts across entity size, sector, and geography. The Rules should consider differentiated compliance models based on risk and scale to ensure requirements are proportionate, do not inhibit competition, and protect inclusion.

These assessments should be used to define exemptions, graded obligations, and thresholds, so that MSMEs and DPIIT-recognised startups are not unduly burdened and regulatory costs do not become barriers to entry or innovation.

## Pilot Testing, Phased Roll-Out and Performance Metrics

Design and implementation of any new rule must be grounded in evidence. A phased rollout, beginning with sandbox pilots across representative sectors (fintech, logistics, OTT), will test technical feasibility, latency, data handling, and societal impacts. Pilots should include performance metrics—accuracy, latency, dispute rates, and exclusion incidents—and structured stakeholder feedback to improve the system before iteratively implementing nationwide enforcement.

## Leverage Technology & Existing Fraud Tools

Private-sector AI-enabled tools that perform real-time fraud detection already flag suspicious behaviour and provide user context during incoming calls. The Rules should promote interoperability with such tools and established initiatives (I4C, CERT-In, DoT analytics) to balance protection with accessibility. This tech-enabled, differentiated approach can help ensure vulnerable populations remain connected rather than excluded by overly strict name-matching.

CUTS International

D-217, Bhaskar Marg, Bani Park, Jaipur 302 016, India
Ph: 91.141.228 2821, Fax: 91.141.228 2485
Email: cuts1@cuts.org, Website: www.cuts-international.org
Also at Delhi, Kolkata and Chittorgarh (India); Lusaka (Zambia); Nairobi (Kenya); Accra (Ghana); Hanoi (Vietnam); Geneva (Switzerland) and Washington DC (USA).