To,

July 23, 2025

Joint Secretary (Telecom),
Department of Telecommunications,
Ministry of Communications,
Sanchar Bhawan,
20 Ashoka Road,
New Delhi - 110001

Email: jst-dot@gov.in

Sub: Feedback on the Draft Telecommunications (Telecom Cyber Rules) Amendment Rules, 2025

Dear Sir/Ma'am,

I write on behalf of Sahamati Foundation ("**we**", "**Sahamati**"), a not-for-profit organisation incorporated under Section 8 of the Companies Act, 2013. Sahamati is an industry body aimed at fostering the growth of the Account Aggregator ("**AA**") ecosystem, with more than 700 ecosystem participants comprising several regulated financial institutions including banks, account aggregators, and other financial institutions regulated by the Reserve Bank of India (RBI), Securities and Exchange Board of India (SEBI), Insurance Regulatory and Development Authority of India (IRDAI), and Pension Fund Regulatory and Development Authority (PFRDA).

At the onset we would like to acknowledge that the initiative to create trusted databases for customer identity verification can greatly help in combating the level of digital frauds and improving cyber security in the country across sectors. However, we would like to highlight a few areas that need more careful consideration to ensure that the proposed MNV platform meets its desired objective without creating practical challenges for entities, particularly in the financial sector. Several of our members have reached out to us with feedback on the Draft Telecommunications (Telecom Cyber Security) Amendment Rules, 2025 ("**Draft Amendments**") and have summarised the same in the attached document.

We have had detailed discussions with participants in our ecosystem and would like to take this opportunity to share the key areas of concern. We are annexing a note covering our inputs, and hope that our feedback will contribute to a review of the Draft Amendments. We would be honoured to present further representations and/or provide additional inputs in respect of these issues. We remain available for any questions or clarifications that you may have.

Sincerely,
Shalini Gupta
Chief Policy and Advocacy Officer, Sahamati Foundation

Feedback on the Draft Telecommunications (Telecom Cyber Rules) Amendment Rules, 2025

The Draft Telecommunications (Telecom Cyber Security) Amendment Rules, 2025 ("**Draft Amendments**") propose to amend the Telecommunications (Telecom Cyber Security) Rules, 2024 ("**Telecom Cyber Security Rules**").

The Draft Amendments are well intended to address digital frauds and strengthen cyber security in the country. However, there is a need for deeper assessment of the implications of specific legal and regulatory issues. There is a need to review the breadth of the TIUE construct sought to be introduced, as well as the corresponding framework for validation of telecom identifiers (such as mobile numbers) by such TIUEs through the proposed MNV platform. We have captured our assessment based on our experience and feedback received from the financial institutions for your consideration.

Broad definition of Telecommunication Identifier User Entity (TIUE)

The Draft Amendments introduce targeted cybersecurity obligations for entities beyond traditional telecom operators to include TIUEs. Rather than applying the full set of telecom cybersecurity rules to TIUEs, specific obligations have been proposed, including:

i. integration with a new Mobile Number Verification ('**MNV**') platform;
ii. adherence to security directives to suspend or ban users with specific telecom identifiers; and
iii. cooperation with enforcement authorities.

Proposed clause 2(i) defines a 'telecommunication identifier user entity (TIUE)' as:

> *"... a **person**, other than a licensee or authorised entity, which **uses telecommunication identifiers for** the **identification** of its customers or users, **or for provisioning and delivery of services**."*
>
> *(Emphasis supplied)*

The definition of TIUEs would render all corporations, individuals, companies and other bodies of individuals identifying their customers/ users with a telecom identifier or using a telecom identifier to provision or deliver services.

Most TIUEs do not operate telecom networks, hold telecom licences, or access network-level infrastructure. *Prima facie* the expansive scope of TIUEs risks regulating entities that have no connection whatsoever to the telecom ecosystem, being subject to the obligations of a TIUE. Treating such entities as part of a telecom cybersecurity framework may result in regulatory overlaps, and require entities to adopt processes and layers of validation disproportionate to their actual role or exposure to telecom-specific risks or business requirements.

The Telecom Cyber Security Rules were introduced under Section 22 of the Telecommunications Act, 2023 ("**Telecom Act**"), aimed to "*enhance and maintain the security of* telecommunication *networks and telecommunication services.*" 'Telecom cyber security' is defined as "*cyber security of telecommunication networks and telecommunication services, which includes tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, assurance and technologies that can be used to safeguard telecommunication networks and telecommunication services against relevant security risks in the cyber environment.*" The emphasis is on securing licensed telecom infrastructure including networks, signalling systems, subscriber databases, and related assets, and not regulating downstream users of mobile numbers.

The mere use of a mobile number as a customer identifier does not create a material risk to telecom networks. TIUEs, in most cases, use mobile numbers for user identification or communication, without interacting with or compromising the integrity of any telecom infrastructure. They do not operate SIM provisioning, routing, or signalling systems, and have no control over the security of telecom networks. Most TIUEs only have "read" or "query" access to subscriber information, and cannot edit or otherwise compromise such data. Such entities largely operate on the 'application layer' and generally perform roles/ provide services that are widely different from that of telecom operators.

Mobile Number Verification under the Draft Amendments

The Draft Amendments create an enabling framework for TIUEs to integrate with the proposed Mobile Number Verification ("**MNV**") platform in two ways: either voluntarily or when specifically directed by the Central or State governments or any agency authorised by the Central or State governments.

A centralized MNV platform is proposed to verify the ownership of mobile numbers used by various entities. This is intended to curb fraud and impersonation facilitated by misuse of telecom identifiers.

As per proposed Rule 7A (Validation of telecommunication identifiers), a TIUE may suo moto, and must, upon direction from Central or State Government or any agency authorised by the Central or State Government, place a request on the MNV platform, upon payment of the prescribed fee, "*to seek 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.*"

A. Implications for the BFSI Sector

Almost all entities in the BFSI sector use customers' mobile numbers to identify them with their financial accounts, starting from account creation, ranging to various service delivery interactions by such regulated financial institutions to end customers. As per the proposed definition of a TIUE, all entities regulated by the RBI, SEBI, IRDAI and PFRDA may also be subject to the obligations of a TIUE.

Mobile numbers form an important aspect of the extant regulatory framework(s) for KYC registration, applicable in the BFSI sector. For example, they are relied on by banks, NBFCs, etc. under the RBI's Master Direction – KYC Directions, 2016 for conducting Aadhaar OTP-based e-KYC at the

time of opening an account and are also used to obtain a self-declaration from a customer as part of the KYC re-fresh mandate.

Regulatory Overlaps

The Draft Amendments clarify that the mobile number validation envisaged under the Rule 7A is solely for the purpose of validation of the customers or users associated with a telecom identifier for delivery of services. However, especially if made mandatory, it could result in a parallel set of obligations on such regulated entities, resulting in regulatory overlaps and placing an undue compliance burden on entities that already operate under well-established regulatory frameworks and oversight.

The addition of telecom-specific obligations for businesses that use telecom identifiers, without participating in telecom networks, may create a fractured regulatory landscape and risk duplication of similar obligations and conflicts with extant regulatory frameworks, especially in the BFSI sector.

Regulated financial institutions may be constrained to delay or suspend user access and/or service delivery simply because the MNV platform identifies a potential mismatch in the ownership status of a mobile number. Such disruptions have no bearing on telecom network security but could significantly impair customer experience, particularly where mobile numbers are the only user-facing handle. Additional practical challenges with the MNV framework have been outlined below.

Unintended consequences – Delayed/ Wrongful Denial of Service to genuine users/ customers

Mismatches and/ or false negatives or positives could lead to TIUEs incorrectly triggering additional KYC and/ or due diligence measures and in some cases, even wrongfully denying service and/ or placing unwarranted restrictions on account(s) of genuine customers/ users. It is also uncertain whether TIUEs would be protected in any manner from third party claims on account of such unintended consequences.

- **Financial accounts linked to phone numbers where such SIMs are registered under another person's credentials**. Often, family members may share a common SIM in the same household, which is used for linking in financial and other accounts of the entire family.

  Hence, the same identifier (mobile number) may be used by TIUEs to identify different account holders. If the customer/user discovered through the MNV platform does not match the TIUE's records, it could trigger a false/ inaccurate trigger to the TIUE, leading to wrongful denial of services/ unintended restrictions on the use of such accounts by genuine customers.

- **Joint accounts with minors where the registered mobile number is that of the guardian**. Similar concerns regarding issues of mismatches also arise for joint accounts, especially for joint accounts held with minors.

- **Corporate accounts where the registered mobile numbers invariably registered in the name of an individual**. It merits consideration to resolve for this scenario, as a validation request with

the MNV platform would likely result in a failure/ mismatch between the MNV platform's records and the TIUE's records.

- **Dormant or legacy accounts tied to deactivated or ported mobile numbers**. In the case of dormant bank accounts, long-standing demat holdings, or inactive insurance policies, it is common for the registered mobile number to be outdated, ported to another telecom provider, or even reassigned to a new subscriber. The MNV platform, relying on current telecom ownership data, may identify the new user of the number rather than the original account holder. This could cause false flags to the TIUE, including triggering internal KYC remediation workflows, freezing transactions, or marking such accounts as non-compliant, despite the fact that the account holder has not engaged in any fraudulent or malicious conduct.

B. Prohibitive costs for placing requests on MNV platform

To query the MNV platform, TIUEs would be required to incur per-request charges (₹1.50 when directed, ₹3.00 when voluntary).

While a fee of INR 1.50 to INR 3 per query may appear modest, the aggregate cost may be significant, especially if validation by banks, etc. is required on a large scale and high frequency, especially for low value transactions/loans/services. As per our understanding, bulk PAN verification is offered by various service providers at prices in the range of INR 12,000 per annum for verifying 750 PAN numbers per user per day. Even for other such services, the fee is ideally left to market factors.

The proposed 'per request' fee model under the Draft Amendments will place an onerous monetary burden on TIUEs.

Broad powers to seek production of data "related to" telecom identifiers from TIUEs

The extension of the powers to seek production of user data from TIUEs pursuant to clause 3(1)(aa) of the proposed Telecom Cyber Rules appears board to the extent that the proposed clause subjects TIUEs to provide data "related to" telecom identifiers, as it may extend to a wide array of personal data of end customers/ users.

It would be useful if the Proposed Amendments are suitably modified to specify the scope of the data that may be sought from TIUEs under this provision. Further, the telecom identifiers that may be sought under this provision should be limited to only such telecom identifiers which may have failed validation through the MNV platform.

Enhance due process for suspension and/or prohibition on the use of telecom identifiers for (i) identification of customers/ users and/or (ii) delivery of services

Read together, clauses 5(6)(b) and 5(8)(b) of the proposed Telecom Cyber Rules empower the central government to temporarily suspend and prohibit/ circumscribe the use of telecom identifiers by TIUEs for the purpose of identifying such customer/ user, as well as for delivery of services to them.

While there is an existing due process requirement to notify the end customer/ user **or** the TIUE, given the cross-sectoral scope of the TIUEs and breadth of end customers/ users affected across a range of services, it becomes important to ensure that end customers/ users are mandatorily provided a copy of the orders passed pursuant to the above powers, to enable them to make an appropriate representation against the suspension/ prohibition of their telecom identifier(s).

Under the TIUE construct, especially in the BFSI sector, an incorrect suspension and/or prohibition of the services could lead to severe adverse consequences for end customers/ users. An appropriate amendment may be made to include an 'and' requirement under Clauses 5(7) and 5(8), thereby ensuring that a copy of the order passed under Rules 5(6)(b) or 5(6)(8) is provided to the affected end customers/ users of TIUEs.

Recommendations

1. **Limit scope of TIUEs**

The scope TIUEs may be limited to entities within the purview of regulation of the DoT, and within the scope of the regulation under the Telecommunications Act, 2023, as under (proposed edits in red):

> "telecommunication identifier user entity (TIUE)" means a person, other than a licensee or authorised entity, which uses telecommunication identifiers for the identification of its customers or users, or for provisioning and delivery of telecom services."

OR

2. **Empower financial sector regulators to pass directions, if any, regarding use of the proposed MNV platform by their regulated entities**

Since regulated entities operate under strict supervision of the relevant regulators and further, are required to follow detailed KYC obligations, it would be prudent to empower the financial sector regulators to pass directions, if any, to their regulated entities regarding use of the proposed MNV platform. A suitable proviso to proposed clause 7A may be included, as under:

> "Provided that in relation to any person regulated by RBI, SEBI, IRDAI or PFRDA, the relevant regulator shall have the power to pass directions regarding use of the MNV platform."

3. Review the fee structure for use of the proposed MNV platform

As briefly discussed above, the proposed 'per request' fee model and the associated costs will place an undue burden on a wide array of businesses. In the circumstances, we request a complete review of the fee model for placing requests on the proposed MNV platform.

4. Adopt a tiered compliance framework based on scale and risk

We recommend implementing a structured compliance model that differentiates between high-risk and low-risk TIUEs. Not all entities using telecom identifiers present the same cybersecurity risks. The rules should enable the government to specify compliance obligations according to an objective criterion such as monthly transaction volume, integration depth with telecom APIs, the nature of services provided etc. This approach would ensure that regulatory focus remains on entities that are genuinely vital to telecom integrity, rather than imposing a blanket regime that equally burdens all digital service providers.

5. Implement stricter KYC requirements for SIM issuance

The proposed MNV platform is predicated on the records of licensees and authorised entities. Considering known concerns pertaining to the authenticity of the customer verifications at the time of SIM issuance, the existing records of the authorised entities and licensees would not serve as a complete, accurate and reliable database to use for further downstream user/ customer validation.

A more appropriate policy response may first begin with mandating and enforcing stricter KYC norms for issuance of SIMs. Without such a regime, and resultant accuracy and completeness of the records of the authorised entities and licencees, the well-intended objectives of the MNV platform may lead to wrongful lockouts of users/ customers from their legitimate accounts (financial and others), as discussed above. In this context, it is relevant to note the obligations of data fiduciaries to ensure the completeness, accuracy and consistency of personal data processed by them. Section 8(3) of the Digital Personal Data Protection Act, 2023 reads as under:

> *"(3) Where personal data processed by a Data Fiduciary is likely to be—*
> *(a) used to make a decision that affects the Data Principal; or*
> *(b) disclosed to another Data Fiduciary,*
>
> *the Data Fiduciary processing such personal data shall ensure its completeness, accuracy and consistency."*

6. Provide safe-harbour protection for verified accounts with MNV mismatches

Mismatches between MNV platform data and a TIUE's internal records may occur even in legitimate scenarios, such as accounts with shared SIMs, minor guardianships, or corporate accounts linked to employee numbers. In such cases, we recommend adding an appropriate safe-harbour clause stating that a mismatch alone will not lead to adverse regulatory action, as long as the TIUE can prove that the account has already been through a regulated KYC process. This shields genuine customers from

unnecessary service disruption and allows TIUEs to operate confidently without overreacting to false positives generated by telecom validation tools.

7. **Institute adequate safeguards in the provisions obligating TIUEs to provide data "related to" telecom identifiers**

As discussed hereinabove, the proposed clause 2(aa) lacks adequate constitutional safeguards in relation to such requisitions from the central government and agencies authorised by it. The scope of telecom identifier data that can be sought may be specified. Further, the telecom identifiers that may be sought under this provision should be limited to only such telecom identifiers which may have failed validation through the MNV platform.

8. **Enhance the due process framework such that end customers/ users are enabled to effectively make representations against suspensions and/or banning of their telecom identifiers**

As discussed hereinabove, in order to ensure meaningful due process is followed for suspension/ prohibition of telecom identifiers by TIUEs pursuant to the powers under clause 5 of the Telecom Cyber Rules, an 'and' requirement may be suitably included in clauses 5(6)(b) and 5(8)(b) of the Telecom Cyber Security Rules, to empower end customers/ users to make representations against such suspension/ prohibition.

****