



CONSTITUTIONAL LAW

FOOD

TRAI Tightens the Screws on Spam: New Rules Target Robocalls, Rogue Senders and Weak Enforcement

The Telecom Regulatory Authority of India has published the Telecom Commercial Communications Customer Preference (Third Amendment) Regulations, 2026 in the Gazette of India. The amendment brings tougher rules, a revised tariff and more advanced monitoring to curb unsolicited commercial communications, including spam calls, robocalls and unauthorized messaging across Indian telecom networks. Robocallers Must Declare Their [...]

AUTHOR Aditee Bohra**PUBLISHED** 6 October 2026

The Telecom Regulatory Authority of India has published the Telecom Commercial Communications Customer Preference (Third Amendment) Regulations, 2026 in the Gazette of India. The amendment brings tougher rules, a revised tariff and more advanced monitoring to curb unsolicited commercial communications, including spam calls, robocalls and unauthorized messaging across Indian telecom networks.

Table of contents

- [Robocallers Must Declare Their Numbers in Advance](#)
- [Clear Limits for Call-Filtering Apps](#)
- [A Stronger Consent and Do Not Disturb Framework](#)
 - [What Consent Covers](#)
 - [Blocking Promotional Categories](#)
- [Faster Detection and Escalating Penalties](#)
 - [AI-Based Spam Detection](#)
 - [Penalties for Repeat Offenders](#)
- [Header Security, a New Call Fee and a Path to Appeal](#)
 - [SMS Header Suspension](#)
 - [A2P Call Termination Fee](#)
 - [Appealing Unresolved Complaints](#)
- [When the Rules Take Effect](#)

Robocallers Must Declare Their Numbers in Advance

Any business, software platform or other entity that places automated or pre-recorded voice calls (application-to-person, or A2P, calls) must now declare its **full series of calling line identification (CLI) numbers** to telecom service providers. It must also record them on Distributed Ledger Technology (DLT) platforms.

The consequence of skipping this step is automatic: a commercial call from an undeclared series will be treated as unsolicited commercial communication.

Clear Limits for Call-Filtering Apps

The regulations also set boundaries for third-party call management and filtering applications:

- These platforms may no longer apply blanket spam tags to official **government and regulatory number series**, or block them at the network or platform level.
- Individual users keep complete freedom to block any number on their own devices.
- In return, filtering apps must share their spam data with telecom access providers so that threat intelligence is aligned across the ecosystem.

A Stronger Consent and Do Not Disturb Framework

What Consent Covers

Consent given under the TRAI framework covers **calls and SMS only**. It is separate from the data processing consent governed by the Digital Personal Data Protection Act. Withdrawing consent stops promotional and marketing messages but does not affect essential transactional or service alerts, such as those a bank sends about account activity.

Blocking Promotional Categories

Users can also control which kinds of promotional messages they receive. By SMS, using the designated **BLOCK PROMO** keywords, or through the 1909 IVRS hotline, they can block or unblock specific categories such as banking, real estate or education.

Anyone whose preference is currently set to “Fully Blocked” will be moved automatically to the new BLOCK PROMO category structure.

Faster Detection and Escalating Penalties

AI-Based Spam Detection

Telecom access providers must deploy real-time artificial intelligence and machine learning systems to identify likely spam callers, and they must share what they find with other operators within **two hours**.

Penalties for Repeat Offenders

Penalties for offenders escalate in stages:

1. **First violation:** mandatory re-verification of the sender's Know Your Customer (KYC) documents.
2. **Second violation:** physical KYC verification. If the details turn out to be fraudulent or the resources have been abused, all of the sender's outgoing telecom resources, including SIMs and SIP trunks, are suspended for 15 days.
3. **Repeated violations:** total disconnection of services, IMEI hardware blocking and a network-wide blacklist lasting one full year.

Header Security, a New Call Fee and a Path to Appeal

SMS Header Suspension

Suspicious SMS headers, or message templates that have been misused, will be suspended within **six hours** of detection. If credentials are compromised or leaked, the sending entity must go through a full re-registration before it can regain access.

A2P Call Termination Fee

To discourage misuse, terminating access providers may charge originating providers an A2P call termination fee of up to **₹0.05 (five paise) per minute**, applied on a per-minute pulse basis. Special public interest and government series are exempt.

Appealing Unresolved Complaints

Consumers whose spam complaints go unresolved can take them to a designated **Appellate Authority**.

When the Rules Take Effect

The rules come into force in **three phases**, counted from the date of gazette publication:

1. **After 30 days:** the general provisions and the updated Do Not Disturb rules apply.
2. **After 60 days:** mandatory A2P declarations, Virtual Network Operator interfaces and header suspension protocols follow.
3. **After 90 days:** the appellate mechanism, blockchain integration and the multi-operator AI spam-matching infrastructure become fully operational.

Related Practice Areas

Food Safety and Regulatory Compliance