INDIALAW

CONSUMER

Understanding TRAI’s UCC (Unsolicited Commercial Communications) Rules: Compliance Insights For Corporates

AUTHOR Aditi Rana

PUBLISHED 7 October 2025

Introduction

On October 1, 2025, National Commodity Clearing Limited (NCCL) issued Circular No. NCCL/COMPLIANCE-004/2025, directing its members to ensure full compliance with the amended Telecom Commercial Communications Customer Preference Regulations (TCCCPR), 2018, notified by the Telecom Regulatory Authority of India (TRAI). The circular reflects the regulator's continued effort to safeguard consumers from Unsolicited Commercial Communications (UCC) and underscores the heightened responsibilities of corporates handling mass communications.

Table of contents

- Introduction
- Legal and Regulatory Background
- Operational and Compliance Implications
- Legal Risks for Non-Compliance
- Practical Steps for Corporates
- The Broader Implication
- Conclusion

Legal and Regulatory Background

The TCCCPR, 2018, is grounded in the authority conferred on TRAI under Sections 11 and 13 of the Telecom Regulatory Authority of India Act, 1997. These regulations were introduced to create a structured mechanism for regulating commercial communications, including telemarketing calls, transactional messages, and promotional SMS. The objective has always been to empower consumers to control the commercial messages they receive, while imposing clear obligations on telemarketers, aggregators, and corporate entities.

The recent amendments to the TCCCPR are significant because they introduce stricter norms for the use of communication channels, templates, and headers. Importantly, corporates are now prohibited from using ordinary 10-digit mobile numbers for any commercial communication. Instead, all transactional or service-related communications must be routed through designated 1600-series numbers, ensuring traceability and regulatory oversight. This change directly affects entities sending high-volume messages, requiring upgrades to infrastructure and internal processes.

Operational and Compliance Implications

The NCCL circular emphasizes several practical steps for members, all of which carry legal weight. Corporates must whitelist all URLs, mobile applications (APKs), and digital assets used in communications to prevent unauthorized or malicious use. In addition, SIP/PRI connections—commonly used for bulk voice and transactional services—must operate strictly in compliance with TCCCPR standards.

Another critical aspect is cooperation with the Indian Cybercrime Coordination Centre (I4C) and TRAI. Companies are expected to participate in reporting protocols and respond promptly to any advisory issued by these authorities. This requirement highlights the convergence of cybersecurity, consumer protection, and regulatory compliance, placing a legal and operational responsibility on corporates to monitor and control the integrity of their communication channels.

Legal Risks for Non-Compliance

Failure to adhere to these regulations is not trivial. TRAI has the authority to impose monetary penalties, block non-compliant communication channels, and restrict services. Moreover, misuse of communication headers or templates can attract liabilities under the Information Technology Act, 2000, especially provisions dealing with unauthorized access, cyber fraud, or data misuse. From a corporate governance perspective, non-compliance also exposes organizations to reputational risk, which can affect customer trust and business relationships.

Practical Steps for Corporates

To navigate this regulatory environment, corporate legal and compliance teams must integrate TCCCPR compliance into their standard operating procedures. This includes auditing communication systems, ensuring that only whitelisted tools are used, and verifying that all outgoing messages follow the 1600-series number requirement. Internal controls must be robust enough to prevent accidental or malicious misuse of templates and headers. Regular staff training and awareness programs on UCC compliance and cybersecurity obligations are equally essential to ensure adherence across departments.

The Broader Implication

The NCCL circular is more than an administrative directive, it reflects a broader regulatory trend in India toward stricter consumer protection, accountability, and digital security in corporate communications. For businesses, it signals that compliance cannot be an afterthought; it must be a core component of operational strategy. By proactively aligning systems with TRAI's amendments, corporates not only mitigate legal and operational risk but also strengthen trust with consumers in a highly competitive digital landscape.

Conclusion

TRAI's amended TCCCPR, reinforced by NCCL's circular, is a clear message to the corporate sector: responsible communication is mandatory, not optional. Firms must take a proactive approach to compliance, integrating legal requirements, cybersecurity safeguards, and governance measures into daily operations. For corporates in India, the circular is a reminder that robust compliance frameworks are essential to protect consumers, uphold corporate integrity, and avoid regulatory or reputational fallout.

For more details, write to us at: contact@indialaw.in

Related Practice Areas

Media And Entertainment