GSMA APAC
Suite 1207-10 12/F
Great Eagle Centre
23 Harbour Road
Wan Chai
Hong Kong
Tel: +852 3960 5000
gsma.com

**19th April 2026**

**To Shri Deepak Sharma,**
**Advisor (QoS-II),**
**Telecom Regulatory Authority of India (TRAI),**
**Government of India,**
**4th, 5th, 6th and 7th Floor, Tower-F, World Trade Centre, Nauroji Nagar, New Delhi 110029**

**Subject – GSMA Submission to TRAI on Consultation Paper on the Draft Telecom Commercial Communications Customer Preference (Third Amendment) Regulations, 2026**

The GSMA welcomes the opportunity to provide its response to the Telecom Regulatory Authority of India's (TRAI) Consultation Paper on the Draft Telecom Commercial Communications Customer Preference (Third Amendment) Regulations, 2026. The Authority's continued focus on strengthening the framework to address unsolicited commercial communications (UCC) and telecom-enabled fraud is both timely and necessary, particularly given the increasing sophistication, scale, and cross-channel nature of scam ecosystems.

At the outset, GSMA would like to express its strong support for TRAI's core objectives. These include addressing the growing incidence of scams, responding to the structural shift from SMS-based abuse to voice channels, and enabling faster and more effective enforcement through the use of AI/ML-based detection systems. These are legitimate and important policy goals, and GSMA fully supports efforts to enhance consumer protection and restore trust in digital communications.

At the same time, GSMA's review of the proposed amendments suggests that certain elements of the framework may inadvertently concentrate enforcement, operational, and financial responsibility disproportionately on Access Providers, even in situations where they have limited visibility into sender intent, content, or the broader context of communication activity. This creates a risk that the regulatory framework may rely too heavily on telecom operators as the primary enforcement anchor within what is, in reality, a multi-layered and cross-sectoral scam ecosystem.

In practice, such an approach could lead to several unintended consequences. These include the potential for over-blocking of legitimate enterprise and service communications, particularly where actions are triggered by probabilistic AI/ML outputs; the emergence of defensive compliance behaviours rather than targeted and intelligence-led enforcement; increased disputes and operational friction arising from false positives; and the displacement of malicious actors towards less regulated channels, including over-the-top (OTT) communication platforms and digital applications. These risks are particularly relevant in light of the growing role of platforms such as messaging applications including messaging and voice services such as WhatsApp and Telegram, as well as IP-based messaging channels offered by OTT applications and handset manufacturers which are increasingly significant vectors for scam and promotional activity but remain largely outside the scope of telecom-specific enforcement frameworks. In this context, differences in oversight across functionally similar communication channels may affect the overall effectiveness of the framework.

. A more holistic approach to spam management, taking into account the evolving and multi-channel nature of communications, may therefore be beneficial in ensuring that regulatory outcomes remain effective and proportionate across the broader digital ecosystem.

In this context, GSMA recommends that the regulatory framework be guided by a set of core design principles that have emerged from international experience and industry practice in combating scams.[1]

First, responsibility within the ecosystem should be aligned with control. Effective anti-scam frameworks allocate obligations based on which entity has the greatest ability to prevent or mitigate a specific risk. Access Providers are best placed to address network-level issues such as spoofing, SIM misuse, and abnormal traffic patterns. However, responsibility for content, consent, campaign design, and customer data integrity lies more directly with enterprises, telemarketers, and aggregators. Similarly, user-facing platforms and applications play a critical role in enabling reporting, filtering, and consumer awareness. A more explicit recognition of these differentiated roles would allow enforcement to be more targeted, proportionate, and effective.

Second, the framework should incorporate safe-harbour protections for good-faith compliance. As operators increasingly deploy AI/ML systems to detect suspected scam activity, it is essential that such actions, when undertaken in accordance with prescribed processes and technical standards, do not expose operators to

[1] These design principles are consistent with approaches observed across a number of mature regulatory frameworks internationally, where responsibility for scam prevention is increasingly aligned with control, supported by safe-harbour protections for good-faith compliance, and complemented by cross-sector coordination involving telecom networks, digital platforms and financial systems. GSMA report, Examination of Anti-Scam Frameworks in APAC, February 2026

disproportionate liability. The absence of such protections risks creating a disincentive for proactive intervention, thereby undermining the very objective of rapid scam prevention. Safe-harbour provisions would ensure that AI-driven systems function as enablers of enforcement rather than sources of regulatory risk.

Third, AI/ML systems should be treated as decision-support tools rather than automatic enforcement triggers. While GSMA strongly supports the use of advanced analytics and real-time intelligence to identify suspicious behaviour, regulatory action particularly actions with significant commercial or service implications should be based on corroborated evidence and clearly defined thresholds. This is important to minimise false positives, maintain trust in the system, and ensure that legitimate communications are not unduly disrupted. In this context, it may be important to ensure that AI/ML-based flagging serves as an input into a broader assessment process, rather than the sole basis for consequential enforcement measures. Given the inherent limitations of probabilistic systems, such an approach would help mitigate the risk of unintended impact on legitimate users, including enterprises and individuals engaged in lawful communications, while preserving the effectiveness and credibility of the overall framework.

Fourth, greater emphasis should be placed on accountability at the point of origination, particularly for high-volume enterprise senders and aggregators. Introducing enhanced obligations or tiered compliance requirements for such entities would reduce reliance on Access Providers as the primary enforcement mechanism and ensure that deterrence is directed towards those entities with the greatest influence over communication behaviour. In this context, approaches that improve the identification and differentiation of communication types at key network interconnection points may further support effective oversight. For instance, clearer delineation between commercial (A2P) and person-to-person (P2P) traffic, based on appropriate classification and declaration mechanisms, could enhance monitoring, reduce the risk of misuse of P2P channels for commercial purposes, and support more consistent treatment across the ecosystem. Such measures, when implemented in a flexible and proportionate manner, can strengthen overall framework effectiveness while preserving operational feasibility and encouraging coordinated action across stakeholders.

Fifth, the framework should continue to evolve towards a whole-of-ecosystem approach. Scam prevention increasingly spans telecom networks, digital platforms, financial systems, and user interfaces. In practice, this asymmetry reflects not only differences in function but also limits on sector-specific regulatory jurisdiction, which can result in enforcement and liability being channelled disproportionately through licensed Access Providers rather than addressed at the point of origination or platform-level dissemination.

While GSMA acknowledges TRAI's efforts to bring certain third-party applications within the ambit of regulatory oversight, further consideration may be needed to address the broader issue of regulatory asymmetry, particularly in relation to large communication

platforms that are increasingly used for scam dissemination. Ensuring a more consistent baseline of obligations across functionally similar services would strengthen the overall effectiveness of the framework.

With respect to specific proposals in the consultation paper, GSMA offers the following observations.

The proposal to introduce termination charges for A2P voice calls represents a proportionate economic measure to address the current imbalance in cost structures that enables large-scale abuse. Extending such charges for all commercial calls including A2P calls, is a step in the right direction. Additionally, GSMA suggests the authority to include call attempts, given the reliance of scam of scam campaigns on high-volume, low-success-rate calling strategies. However, it will be important to ensure clarity in classification, along with narrowly tailored exemptions for legitimate use cases, such as government and critical service communications, while ensuring that exemptions are carefully targeted and do not inadvertently cover numbering resources primarily used for commercial communications, Appropriate safeguards should also be built in to prevent any unintended impact on essential services.

GSMA strongly supports the continued use and evolution of AI/ML-based detection systems. However, their integration into the regulatory framework should remain principles-based and flexible, allowing operators to innovate and adapt to emerging threat patterns. A federated model, in which operators deploy and continuously improve their own systems while adhering to common standards for reporting and interoperability, is likely to be more effective than a highly centralised or prescriptive approach. At the same time, AI/ML-based spam flagging should not be considered as the sole basis for punitive actions such as disconnection or service restriction, given the risks of false positives and unintended consequences for legitimate users.

On consumer grievance redressal and the proposed appeal mechanisms, GSMA recognises the importance of ensuring fairness, transparency, and timely resolution for consumers. At the same time, the introduction of additional procedural layers and tight timelines should be carefully aligned with the maturity of existing technological infrastructure, including the DLT platform, to ensure operational feasibility and system stability. In this context, it is also important to recognise that mobile connectivity today underpins access to a wide range of essential digital services, including financial transactions, e-commerce, and public service delivery. As such, any unintended disruption to legitimate services, including those that may arise from false positive identification, should be minimised through appropriate safeguards and proportionate remediation mechanisms. A phased and iterative approach to implementation may therefore be beneficial, allowing systems and processes to evolve in line with operational readiness while maintaining consumer confidence. Finally, with respect to financial disincentives and liability frameworks, GSMA recommends that proportionality

and control remain the guiding principles. While strengthening accountability is essential, care should be taken to ensure that liability is not extended to entities that do not have direct control over the underlying conduct. In this regard, anchoring enforcement more clearly at the level of originating entities, while supporting operators through clear guidance and protections, would lead to more effective outcomes.

In addition, ensuring greater accountability and transparency across entities participating in the commercial communications ecosystem may further strengthen overall outcomes. Approaches that promote clearer eligibility criteria, oversight, and responsible participation for entities engaged in large-scale messaging or calling activities could support more effective compliance and reduce misuse, while maintaining flexibility in how such mechanisms are operationalised. Finally, as regulatory frameworks in this area continue to evolve, maintaining coherence with broader legal and policy objectives particularly in relation to consumer protection, proportionality, and clarity of roles will be important to ensure that measures remain effective, predictable, and aligned with the wider digital ecosystem.

Finally, with respect to financial disincentives and liability frameworks, GSMA recommends that proportionality and alignment with control remain the guiding principles. While strengthening accountability across the ecosystem is essential, care should be taken to ensure that obligations are applied in a manner that reflects the role and capabilities of each participant. Telecom service providers have implemented a range of technical and operational measures including mechanisms such as distributed ledger-based systems, filtering tools, and scrubbing processes to support the detection and mitigation of unsolicited communications. These measures play an important enabling role within the broader ecosystem, but do not in themselves confer control over the content, intent, or origination of communications generated by other actors.

In this context, approaches that seek to reinforce accountability at the point of origination, while providing clarity and certainty around the role of different stakeholders, may support more effective and proportionate outcomes. It may also be important to ensure that regulatory expectations remain aligned with the practical and operational remit of Access Providers, so that frameworks do not inadvertently create uncertainty or disincentives for proactive action. As the regulatory landscape continues to evolve, maintaining coherence with broader legal and policy principles including clarity of roles, proportionality, and predictability will be important to ensure that enforcement remains both effective and sustainable.

In conclusion, GSMA reiterates its strong support for TRAI's efforts to combat spam and fraud and to enhance consumer protection in India's rapidly evolving digital ecosystem. The proposed amendments represent an important step forward. At the same time, refining the framework to ensure that responsibility is proportionate, innovation is

enabled, and enforcement is aligned with control across the ecosystem will be critical to achieving sustainable and effective outcomes.

GSMA remains committed to working closely with TRAI and other stakeholders to support the development of a robust, future-ready, and collaborative anti-scam framework for India.

Warm regards,

Jeanette Whyte
Head of Policy & External Affairs, APAC
GSMA
+852 9615 2331