Response to Consultation on
Draft Telecom Commercial Communications Customer Preference (Third Amendment) Regulations, 2026

To: Secretary, Telecom Regulatory Authority of India,

Kind attention: Sh. Deepak Sharma, Advisor (QoS-II), advqos@trai.gov.in

From: Tanla Platforms Limited

Date: 19 April 2026

Reference: No. RG-25/(25)/2023-QoS dated 13 March 2026

Submission

Tanla Platforms Limited is thankful to the Telecom Regulatory Authority of India (**Authority**) for providing the opportunity to submit comments on its Consultation Paper on Draft Telecom Commercial Communications Customer Preference (Third Amendment) Regulations, 2026.

Preventing Unsolicited Commercial Communication (**UCC**) is a key priority for access providers and other stakeholders in the ecosystem, which will be better served by the draft amendments under consultation.

We respectfully submit that certain refinements are required to ensure that the framework is operationally efficient and robust. In particular, the framework should:

(i) Leverage DLT-based records across consent management, complaint handling, enforcement, and appeals for operational efficiencies and completeness of audit trails;
(ii) Ensure that complaint handling reflects the subscriber-facing role of the Terminating Access Provider, while preserving effective inter-operator coordination for enforcement;
(iii) Incorporate sufficiently granular consent and metadata requirements to distinguish legitimate high-volume commercial communications from UCC; and
(iv) Enable graded enforcement mechanism through certain additional criteria. These refinements would improve enforcement and reinforce consumer trust, without compromising the regulatory responsibilities of Access Providers in implementing the framework.

The following are the principle-level changes being proposed to the draft amendments.

- **Complaint handling should reflect the subscriber-facing role of the Terminating Access Provider.**

  The current framework appropriately assigns key complaint intake and reporting obligations to the Terminating Access Provider, while certain downstream examination and enforcement actions remain with the Originating Access Provider. Given that the Terminating Access Provider is the entity that has the direct relationship with the subscriber and receives the complaint first-hand, they are best placed to assess the surrounding facts, subscriber impact, and relevant communication evidence. Further, given that several of the proposed changes are also directed toward protecting subscribers and strengthening consumer trust, the complaint-handling architecture should expressly build upon the Terminating Access Provider's position as the primary subscriber-facing entity. Further, enforcement responsibilities should also remain with the Terminating Access Provider with Originating Access Providers assisting with any downstream examination

or enforcement that may be required. The stakeholders should remain clearly aligned and supported through effective digital coordination across access providers.

- **Consent must be granular, verifiable, and interoperable with the enforcement architecture.**

  A consent-led framework will work effectively only if the regulations require clear purpose limitation, line-of-business or equivalent granularity, channel specificity where relevant, and robust auditability. Overbroad or bundled consent structures undermine consumer choice and complicate compliance verification. Implementing these requirements will also ensure alignment with the standard for consent stipulated under the Digital Personal Data Protection Act, 2023.

- **The existing DLT architecture should be leveraged for trusted verification.**

  Effective scrubbing and complaint resolution require trusted verification of consent and subscriber preferences. In this context, the existing DLT architecture should be used more effectively to function as the central evidentiary layer across consent management, complaint handling, and enforcement processes. The effectiveness of the proposed amendments will depend on the structured, standardised, and machine-readable recording of consent artefacts, declarations, complaints, corroboration outcomes, enforcement actions, and appeal decisions.

- **Data informed enforcement.**

  The draft correctly moves toward differentiated treatment of senders and stronger action based on AI corroboration. However, enforcement should additionally consider factors such as compliance track record, consent status, and asset-level isolation where possible, to ensure that non-compliance is contained without unnecessary disruption to legitimate or critical communications.

Please see our detailed comments below.

Part A — Policy Framing

We offer three short notes taking reference of the Authority's own Explanatory Memorandum and the proposed amendments themselves.

A.1 — Three structural shifts the draft makes. The Memorandum records that the existing complaint-driven framework has not been effective against spammers and that the Authority proposes to strengthen deterrence, enhance auditability, and address enforcement gaps (paras 4, 13). Three shifts follow from the draft itself:

1. ***reactive to proactive***, via AI/ML-based UCC_Detect (Regulation 21A) coupled to a reduced complaint threshold where a CLI has been flagged (Regulation 25(5)(d)(i));
2. ***single-registrar trust to distributed verification***, via secondary validation under Schedule-I, Item 4(m), which the Memorandum (paras 10–11) makes each Access Provider independently responsible for, irrespective of the primary registrar's categorisation; and
3. ***complaint-only to multi-signal enforcement***, via ingestion of citizen-sourced reports from call management applications (Regulation 34A(2)), which the Memorandum (paras 16.1–16.3) expressly treats as a source of "faster identification of spammers."

The modifications recommended below are designed to strengthen the Authority's design.

A.2 — Cumulative effect on the DLT platform. Read together, the provisions discussed in the Memorandum [consent migration (Reg 2(y), paras 2.2, 5), AI detection sharing (Reg 21A with Schedule IV, para 4), structured complaint recording (Reg 25, paras 6–7), and enforcement action (Regs 25, 22, 26, paras 8–9, 13)] move the DLT platform beyond a registration ledger into a platform that must manage three interconnected functions:

1. consent lifecycle,
2. intelligence exchange, and
3. enforcement orchestration.

To keep this platform workable, our proposals observe a *share / record / retrieve* discipline: near-real-time sharing of suspected CLIs, confidence scores, etc.; authoritative recording on DLT of consent artefacts, enforcement decisions and appeal outcomes; and off-platform but audit-retrievable retention of model rationale and investigative material.

This calibration directly addresses the Memorandum's concern (para 8) that indiscriminate enforcement against enterprise senders can cause "large scale disruption." We also note an interoperability opportunity with the Sanchar Saathi FRI/MNRL systems operated by the Department of Telecommunications, offered as an opportunity rather than a settled comparison. We note further that the TAP, as the holder of the subscriber's TCCCPR consent and preference records, is the natural Data Fiduciary for those records under the Digital Personal Data Protection Act, 2023; the recipient-side allocation in A.3 below proceeds from that statutory position.

A.3 — Recipient-side adjudication of promotional communication. The scrubbing against DL-Preference and DL-Consent must operate on the Terminating Access Provider's leg of the delivery path.

First, the Access Provider serving the subscriber is, in respect of the TCCCPR consent and preference records of that subscriber, a Data Fiduciary within the meaning of the Digital Personal Data Protection Act, 2023; the TAP, and any data processors it engages, must therefore hold those records securely and process them only for the purposes for which the subscriber has registered preferences or given consent, from which it follows that the operation of scrubbing against DL-Preference and DL-Consent is properly under the TAP's control.

Second, we respectfully urge the Authority that for promotional commercial communications, the TAP shall be the primary authority for recipient-side determination of compliance via scrubbing, and consequently for the investigation of the resulting complaints. The Originating Access Provider retains its sender-side role in KYC of the sender, header and template control, and action against telecom resources allotted by it. It must, however, remain accountable where promotional content is delivered through a transactional or service route, because such mis-categorisation is a sender-side failure and remains an OAP matter.

Three operational disciplines make this division robust: TAP first classification of complaints based on scrubbing logs available with it; parallel recipient-side and sender-side proceedings expressly permitted; and a closure communication that identifies the locus of failure. The clause-level proposals implementing this position appear in the table below and in Part B.

S. No.	Regulation number	Sub-regulation / item number	Modification proposed to the draft amendment	Reasons / full justification for the proposed modifications
1.	Regulation 2	2(y) – "Explicit Consent"	Add proviso after Regulation 2(y): "*Provided that the procedure for registration of consent obtained through verifiable means prior to or outside the Consent Registration Function shall, at a minimum, include the following:* *(a) verification at the level of the Sender, based on risk profiling having regard to complaint history, traffic patterns, and registration compliance records available on the Distributed Ledger Technology platform of the Access Providers;* *(b) validation at the level of the Subscriber of individual consent claims against the Subscriber's preference status, complaint history, and such other intelligence*	The revised definition of "Explicit Consent" appropriately recognises consent obtained outside the CRF framework. However, the recognition of such consent should be accompanied by a sufficiently robust procedural framework so as not to create scope for unverifiable or unsupported historical consent claims. In this regard, it is submitted that the registration process should expressly incorporate enterprise-level verification, subscriber-level validation, mandatory subscriber notification, and recording on the DLT platform. Such a framework would make the provision operationally workable, materially reduce the risk of misuse, and facilitate the orderly migration of legitimate legacy enterprise consents into the regulated

			as may be available on the Distributed Ledger Technology platform of the Access Providers; *(c) issuance of a notice to the Subscriber, through such means as may be specified by the Authority, enabling the Subscriber to view, confirm, modify, or reject the claimed consent records, and the response or absence of response from the Subscriber shall be treated in accordance with the preference status recorded under the Regulations;* *(d) recording of all such validated consents by the Access Provider on the Distributed Ledger Technology platform in a non-repudiable and immutable manner;* *(e) completion of such registration within a migration period as may be specified by the Authority, failing which the Sender shall obtain consent only through the Consent Registration Function in accordance with these Regulations; and* *(f) the procedure specified under this clause shall be in compliance with the applicable provisions of the Digital Personal Data Protection Act, 2023, including the provisions relating to notice, consent, withdrawal of consent, and processing of personal data collected prior to the commencement of that Act.*"	ecosystem. It is also recommended that the consent standard should align with the requirements under the Digital Personal Data Protection Act, 2023.
2.	Regulation 4		Replace the draft text so that the declaration obligation is not restricted to OAP alone. Proposed modification: "*Every Sender shall, in advance, declare to the Access Provider about the use of Application-to-Person (A2P) calling. Such declarations shall be recorded by the Access Provider on the Distributed Ledger Technology platform.* *Provided that any such call made by a sender without prior declaration shall be treated as unsolicited commercial communication, and the concerned*	The current draft requires such declaration to be made only to the Originating Access Provider. However, given that the TCCCPR is a legislation for protecting consumers, a broader formulation would better serve the object of these regulations, which is to enable timely detection, verification, and enforcement in relation to communications that may affect subscribers. Further, where such declaration is captured through the DLT workflow, it would become machine-readable, auditable, and capable of being enforced through the same regulatory systems and controls that govern other forms of commercial communication,

			Access Provider shall take action against such sender in accordance with the provisions of these regulations."	thereby improving traceability, facilitating closer enforcement, and strengthening consumer protection.
3.	Regulation 5 read with Schedule II	5(4), read with point 8 in Schedule II	It is proposed that the following proviso is added to Regulation 5(4): "*Provided that consent may also be revoked, suspended, or marked as inactive by the concerned Access Provider, Sender, or any authority competent in law, in such circumstances and subject to such safeguards as may be specified by the Authority from time to time. Further that every such revocation, suspension, or inactivation shall be recorded in the DLT platform and made visible to the subscriber in such form and manner as may be specified.*"	This provision enables timely and risk-based intervention by Access Providers and Senders in circumstances where continued reliance on a recorded consent may expose Subscribers to potential harm, particularly in the context of complaints made against UCC. It strengthens the integrity of the consent framework by ensuring that consent remains accurate, current, and capable of being acted upon in real time within the complaint-handling and enforcement lifecycle. The requirement to record such actions on the Distributed Ledger Technology platform further ensures transparency, auditability, and alignment with the consumer protection objectives of the Regulations.
4.	Regulation 8	New 8(1)(f)	It is proposed that Regulation 8(1) be amended as follows: "*(f) or any other Code of Practice, as may be specified by the Authority from time to time.*"	This modification is proposed to provide the Authority with sufficient flexibility to specify additional Codes of Practice from time to time in response to emerging technologies and new operational requirements in the commercial communications ecosystem. Given the rapid development of digital communication tools, consent management mechanisms, complaint handling systems, and technology-enabled compliance processes, a closed list of Codes of Practice may limit the ability of the regulatory framework to adapt effectively.
5.	Regulation 21A	21A(a)	Modifications to Regulation 21A(a) are set out in bold: "*For taking action against the senders suspected of sending unsolicited commercial communication, as detected by the AI/ML-based UCC_Detect system established by the access providers in accordance with Schedule IV, every access provider shall implement the following:* *(a) every Terminating Access Provider (TAP) shall, through its AI/ML-based UCC_Detect system, identify and flag the Calling Line Identification (CLI) of the sender as*	The present draft requires that the flagged CLI to be shared but does not specify the structure or format of such shared intelligence. In the absence of a standardised format, different access providers may implement this process in different ways, which may reduce interoperability and create operational difficulties in downstream processing. A standardised format would also facilitate integration with broader fraud intelligence systems. Further, the present draft treats AI detections as binary outputs. However, AI/ML systems

			"Suspected UCC CLI" based upon the behavioural parameters as specified in the AI/ML-based UCC_Detect system, and immediately upon such flagging and in any case within two hours of such flagging, share, through the Distributed Ledger Technology (DLT) platform ***in a structured, machine-readable format as may be specified by the Authority from time to time****, the flagged CLI with the concerned Originating Access Providers (OAPs);* ***Provided further that the Authority may, from time to time, specify that the shared intelligence shall include a confidence score or risk classification reflecting the degree of certainty of the AI/ML-based detection, and may prescribe the methodology for computing such scores.***"	ordinarily generate probabilistic outputs with varying degrees of confidence. Incorporating a confidence score or risk classification would enable more proportionate downstream enforcement, reduce the likelihood of false positives, and assist in calibration of corroboration thresholds under the complaint mechanism.
6.	Regulation 21A	New sub-regulation 21A(f)	"*The Authority may, from time to time, specify additional categories of threat indicators, including but not limited to URLs, domain names, sender IDs, content template identifiers, and device identifiers, that shall be shared through the DLT platform in accordance with the procedures and formats specified by the Authority.*"	Regulation 21A is presently confined to CLI-based intelligence, whereas UCC and fraud campaigns often involve a broader set of indicators such as URLs, headers, content templates, and devices. Extending the regulation through an enabling provision would allow the DLT platform to support campaign-level intelligence sharing as the ecosystem evolves, without requiring further amendment at a later stage.
7.	Regulation 21A	New sub-regulation 21A(g)	"*The Authority may, in consultation with the Department of Telecommunications, specify that intelligence shared on the DLT platform under this regulation may be made available, in such format and through such interfaces as may be specified, to other government agencies, financial sector regulators, and entities authorised by the Central Government for the purpose of fraud prevention.*"	This has been introduced as there is merit in enabling the DLT platform to serve as a common source of telecom threat intelligence for cross-sector fraud prevention, while ensuring appropriate consultation with the Department of Telecommunications.
8.	Regulation 21A	General proviso	It is proposed that the following proviso be added to Regulation 21A: "*Provided that the intelligence shared under this regulation shall be capable of being correlated with consent records and complaint records available on the DLT platform, so as to enable the concerned access providers to*	Consent status is a critical signal of legitimacy and should be part of the intelligence loop. Correlating AI detections with consent and complaint records will allow for more accurate differentiation between legitimate high-volume communications and actual UCC.

			distinguish between the following categories of senders: *(i) a sender who holds valid, subscriber-confirmed consents for the category of communication in question, and whose calling or messaging patterns have triggered detection flags;* *(ii) a sender who holds no valid consent records on the DLT platform and whose patterns have triggered detection flags; and* *(iii) a sender whose detection flags are corroborated by complaints from subscribers who have not given consent for the category of communication received.*"	
9.	Regulation 22	22(1)(a)	It is proposed that the following proviso be added to Regulation 22(1)(a): "*Provided that the details of every such suspension, the notice issued to the sender, the remedial actions taken by the sender, and the outcome of any restoration shall be recorded on the DLT platform by the Access Provider.*"	The draft amendment introduces a detailed remedial framework for misuse of headers and content templates. Recording each step of this process on the DLT platform would create a verifiable audit trail, enable cross-operator visibility, and prevent a sender from bypassing the suspension by moving traffic elsewhere during the remediation period.
10.	Regulation 23	23(1)(c)	It is proposed that the following proviso be added to Regulation 23(1)(c): "*Provided that the entire appeals workflow, from the filing of the appeal, through the Appellate Authority's investigation, to the final decision and any restoration of services, shall be recorded on the DLT platform*."	Recording the appeals workflow on the DLT platform would improve transparency for complainants, enable regulatory audit of compliance with appeal timelines, and support greater consistency in decision-making across access providers. It would also create a useful body of recorded outcomes that may inform future enforcement practice.
11.	Regulation 25	Preamble	It is proposed that after the words "across all the access providers", the following words be inserted: "*shall make available the results of such corroboration, in a structured format on the DLT platform, to all access providers for the purpose of enabling coordinated enforcement under this regulation and shall verify the complaint against consent and preference records of the complainant held on the DLT platform;*"	The current draft requires corroboration of complaint data with AI-based detection data but does not expressly provide for sharing the result of such corroboration with all access providers. As a result, coordinated enforcement across operators may be delayed or fragmented. Recording and sharing the corroboration outcome on the DLT platform would ensure that all relevant operators act on the same information.
12.	Regulation 25	Preamble	It is proposed that after the words "*…and against which the UCC complaint has been made.)*", the following words be inserted:	The current statutory architecture already places the Terminating Access Provider at the subscriber-facing front end, but assigns Communication Detail Record examination, regulatory pre-check

			"It is clarified that the Terminating Access Provider shall also be permitted to be involved and facilitate the entire complaint management process, including but not limited to carrying out scrubbing functions, complaint intake, preliminary validation, customer communication, and operational coordination through interoperable systems."	examination, and formal action to the Originating Access Provider in specified cases. A clarificatory provision would preserve this allocation while allowing the complaint process to remain efficient and customer-facing.
13.	Regulation 25	25(1)	After "in non-repudiable and immutable manner," insert: "*including such structured metadata as the Authority may specify from time to time, which may include the category of commercial communication complained of, the channel (SMS, voice call, or A2P call), the header or CLI used, the content template identifier, and a timestamp of the complained communication,*"	Complaint records must be structured if they are to be correlated with AI detections, app-based reports, and other complaint records. A metadata-enabled complaint record will make DL-Complaints more useful for pattern analysis and enforcement.
14.	Regulation 25	25(4)(f) and 25(5)(d)	It is proposed that after the words "different enforcement measures for different classes of senders", the following further proviso be added: "*Provided further that such enforcement measures may be graduated by asset level (content template, header to line of business, or sender account).*"	The draft rightly contemplates differentiated treatment for different classes of senders. Asset-level enforcement would make that framework more proportionate by isolating non-compliance more precisely at the level at which it occurs so as to enable the Authority to isolate non-compliance at the level at which it occurs without requiring suspension or disconnection of the sender's entire operations.
15.	Regulation 25	25(4)(f) and 25(5)(d)	It is proposed that after the six existing classification criteria, the following additional criterion be inserted: "*compliance track record of the sender on the DLT platform, including consent-related compliance, complaint rate per line of business, and history of enforcement actions,*"	Classification should not depend only on economic importance or scale. Compliance behaviour on the platform is a better indicator of whether differentiated treatment is justified and creates incentives for better conduct by senders.
16.	Regulation 25	25(5)(d)(i)	It is proposed that the following further proviso be added to Regulation 25(5)(d)(i): "*Provided further that where enforcement under this sub-regulation is triggered against a sender classified by the Authority as belonging to a critical sector (including banking, financial services, healthcare, and government services), the concerned access provider shall, before communicating the*	The Explanatory Note recognises that enforcement action against enterprise senders in critical sectors may cause large-scale disruption to services and consumers. A limited requirement of documented human review before cross-operator communication would operate as a proportionate safeguard in such cases without diluting enforcement against ordinary senders.

			enforcement to all access providers, conduct and document a human review of the evidence, including verification of the sender's consent status on the DLT platform. The findings of such review shall be recorded on the DLT platform."	
17.	Regulation 25	25(4)(f) and 25(5)(d)	It is proposed that the following proviso be added: "*Provided that where a sender successfully demonstrates to the concerned access provider, within the representation period, that the enforcement action was based on a false positive, the Access Provider shall reinstate the sender's telecom resources and also communicate the same to all other access providers within one business day. Such reinstatement and associated communication shall be recorded on the DLT platform.*"	The draft provides a representation period but does not specify the timeline or mechanism for reinstatement across operators where an enforcement action is reversed. To ensure fairness and avoid structural bias towards enforcement over correction, the reinstatement process should be capable of operating at the same speed and scope as the enforcement process.
18.	Regulation 26	New 26(2B)	It is proposed that the following sub-regulation be added as Regulation 26(2B): "*(2B) Every access provider shall record, on the DLT platform, the enforcement actions taken under Regulation 25, including the date of action, the type of action (barring, disconnection, blacklisting, or suspension of headers or content templates), the telecom resources affected, and the outcome of any representation or appeal by the sender under Regulation 29. Such records shall be maintained for a period of not less than three years.*"	The draft requires recording complaints and alleged violations but does not require equivalent recording of enforcement outcomes. Without an end-to-end audit trail, it is difficult to verify whether operators acted within statutory timelines and in compliance with the regulations.
19.	Regulation 27	27(1)	Consider a consequential modification clarifying the allocation of financial disincentives where complaint-handling decisions are operationally taken at the TAP-facing layer. Proposed language: "*Where complaint processing, preliminary validation, or communication of closure is undertaken operationally by the Terminating Access Provider in accordance with Regulation 25, financial disincentives under this regulation shall attach to such Access Provider responsible under the Regulations for the relevant statutory act or omission.*"	There may be a mismatch if complaint decisions become more TAP-led while financial penalties remain targeted only at OAPs. Clearer allocation of responsibility would reduce this risk.
20.	Regulation 34A	34A(2)	It is proposed that the words "*to the DND registry maintained by*	As set out in the Explanatory Note, the objective is to ensure that

			the access providers" be replaced with the following: "*to the DLT platform maintained by the Access Providers, in such structured format as the Authority may specify, so as to enable corroboration with the data generated under Regulation 21A and the complaints recorded under Regulation 25.*"	increased reporting through call management applications leads to faster identification of spammers and quicker action. This objective would be better served if such reports are routed to the DLT platform, where complaint, intelligence, and enforcement data are maintained, rather than to the DND registry, which serves a different function.
21.	Regulation 34A	34A(2)	It is proposed that the following proviso be added to Regulation 34A(2): "*Provided that the Authority shall specify the format and minimum data fields for such reports, which shall include at a minimum: the reported telephone number or header, the date and time of the reported communication, the category of report, and such other fields as the Authority may prescribe. The format shall be designed to enable automated ingestion and corroboration with intelligence generated under Regulations 21A and 25.*"	The proposed proviso makes it explicit that the format must be designed for machine-readability and integration with the broader intelligence exchange for effective corroboration.
22.	Schedule I	Item 4(m)(ii)	It is proposed that the following further proviso be added to Schedule I, Item 4(m)(ii): "*Provided further that secondary validation shall be capable of being performed through the DLT platform infrastructure, using information recorded at the time of primary registration and such other data as the Authority may prescribe that are sufficient to support independent categorisation assessment by the validating access provider.*"	The draft amendment correctly provides that secondary validation shall be conducted using information available on the DLT platform and shall impose no additional formality on the sender. This design places the validation burden on the platform and the validating access provider, not on the sender. However, this approach is premised on the DLT platform containing sufficient structured information to enable independent categorisation assessment. The proposed proviso ensures that the enabling infrastructure is expressly required to support the validation obligation.
23.	Schedule I	Item 4(m)(iii)	It is proposed that the following proviso be added to Schedule I, Item 4(m)(iii): "*Provided that where the validating Access Provider's categorisation assessment differs from the categorisation assigned at the time of primary registration, the classification assigned by the Terminating Access Provider shall prevail in so far as the Terminating Access Provider's own subscribers*	The draft amendment renders each access provider independently responsible for compliance with categorisation of content templates and liable for breach irrespective of the categorisation carried out by the primary registering access provider. However, in the absence of a mechanism for resolving categorisation discrepancies, access providers may either accept the primary registrar's categorisation without independent review or

			are concerned. Traffic to the Terminating Access Provider's subscribers shall remain blocked until the discrepancy is resolved."	over-block traffic out of an abundance of caution. The proposed proviso provides a clear rule of precedence for disputed cases and ensures that the financial disincentive mechanism under Regulation 27 operates fairly between the originating and terminating access providers.
24.	Schedule II	Item 1(1), Note-4	It is proposed that after the words "*Such migration shall be completed within 15 days of the commencement of these regulations*", the following words be added: *"During this period, the Access Provider shall notify all affected subscribers that their 'Fully Block' preference will be converted to 'Block Promotional' and that transactional and service-type commercial communications will no longer be blocked under this preference setting."*	Where subscriber preferences are migrated by default, subscribers should be notified clearly. This is important for transparency and aligns with the principles set out under the Digital Personal Data Protection Act, 2023.

Part B — Additional Proposed Modifications

The following further modifications are proposed in addition to the clause-by-clause submissions in the table above. They address areas where the draft creates an obligation but does not specify a supporting structural mechanism.

Modification A — Schedule IV: AI detection outputs on the DLT platform

Provision: Schedule IV, Item 1 — new sub-item (5).

Proposed text: Add sub-item (5): "The Authority may, from time to time, specify that the outputs of the AI/ML-based UCC detection systems, including the behavioural parameters that triggered the detection, the confidence level of the detection, and the volume and pattern of communications observed, shall be recorded in a structured format on the DLT platform, for the purpose of enabling corroboration under Regulation 25, cross-operator intelligence sharing under Regulation 21A, and audit of the detection systems under Regulation 26(4A)."

Justification: Schedule IV governs AI/ML detection parameters but does not connect the outputs to the DLT platform, without which the receiving Access Provider cannot independently assess the quality of the flag, cannot calibrate its own response, and cannot provide meaningful input in the event of an appeal.

Modification B — Regulation 25 preamble: Recipient-side promotional compliance — TAP as primary authority

Provision: Regulation 25 preamble — new substantive proviso.

Proposed text: Insert: "It is clarified that for promotional commercial communications the Terminating Access Provider shall be the primary authority for recipient-side compliance determination, including determination of whether the subscriber's Do-Not-Disturb preference status permitted delivery, whether valid consent was recorded for the category of communication, whether scrubbing against DL-Preference and DL-Consent occurred correctly, and whether the communication was delivered within the permitted time-band and day-type. The Originating Access Provider shall remain responsible for all sender-side examination and enforcement, including examination of sender KYC, header and template correctness, and action against the telecom resources allotted by it. Where

promotional content is delivered through a transactional or service route, the failure shall be classified as a sender-side breach and responsibility shall rest with the Originating Access Provider."

Justification: The draft's text ties promotional delivery to Preference Register and Consent Register status, and it is proposed above that the scrubbing architecture should run on the recipient side to comply with TAP's role as Data Fiduciary.

Modification C — Regulation 25: Closure communication identifying the locus of failure

Provision: Regulation 25 — new closure proviso.

Proposed text: Insert: "The Access Provider communicating closure to the complainant shall, to the extent the available records permit, identify whether the breach arose from (i) recipient-side scrubbing or preference failure or (ii) sender-side act or omission."

Part C — Cross-Cutting Recommendations

C.1 — Recognise the DLT platform as a consent-and-intelligence platform

The cumulative effect of the Third Amendment provisions [consent migration (Regulation 2(y)), consent revocation (Regulation 5), secondary validation (Schedule-I Item 4(m)), AI/ML intelligence sharing (Regulation 21A), structured complaint recording (Regulation 25), app-sourced report ingestion (Regulation 34A(2)), and enforcement orchestration] transforms the DLT platform's role. We recommend that the Authority explicitly recognise this evolution and specify interoperability standards that enable the platform to serve all three functions (consent lifecycle, intelligence exchange, enforcement orchestration) coherently, while observing the share / record / retrieve distinction set out in Part A.2.

C.2 — Align with the Sanchar Saathi / FRI ecosystem

As the intelligence generated under Regulation 21A matures, there is an expectation that it will be a suitable upstream source for the FRI and MNRL systems operated by the Department of Telecommunications. We recommend that the Authority, in consultation with the Department of Telecommunications, explore making the DLT platform's intelligence feed available as the upstream data source for the FRI/MNRL systems. This is an opportunity to be evaluated on the evidence rather than as a settled comparison with existing feeds.

C.3 — DPDP Act alignment across all consent provisions

The consent-related provisions of the Third Amendment, particularly Regulation 2(y), Regulation 5, Schedule-I Item 4(m), and the Schedule-II preference management changes, operate in parallel with the Digital Personal Data Protection Act, 2023, which applies in addition to and not in derogation of other laws. A single procedure that satisfies both TCCCPR and DPDP requirements avoids creating a dual-compliance burden and is more likely to achieve adoption by the enterprises whose participation is essential to the success of these provisions.

C.4 — Principle in regulation, procedure in Direction or Code of Practice

Several provisions in the draft amendment appropriately delegate implementation details to future prescription by the Authority. We recommend that the Authority apply this discipline consistently: the regulation should state the governing principle and essential safeguards. The operational workflow, such as timelines, data formats, subscriber-notice templates, classification rules, evidentiary standards, dispute mechanisms, should be specified through a Direction or Code of Practice. The modification proposed to Regulation 8(1) (Row 4 of the table above) creates an explicit enabling provision for additional Codes of Practice. This approach keeps the regulation-level text lean and stable, while providing the needed operational granularity in implementation.

We would be pleased to provide any further clarification that may assist the Authority in finalising the amendments.

Santhosh Kumar Posina
VP- Regulatory & Product Ops
Tanla Platforms Limted