Luthra *and* Luthra

LAW OFFICES INDIA

Telecommunications, Media and Technology (TMT)

July-September 2026 Edition



Luthra and Luthra
LAW OFFICES INDIA

INSIDE

FINTECH

- RBI proposes data-governance framework for regulated entities
- RBI consolidates cybersecurity and technology-risk requirements
- RBI strengthens digital payment security controls
- Government revises the UPI MDR framework
- RBI issues draft KYC Amendment Directions prescribing a Standard Operating Procedure for suspected money mule accounts
- RBI recognises the Unified Fintech Forum as the second Self-Regulatory Organisation for the FinTech sector

INFORMATION TECHNOLOGY & DATA PROTECTION

- The Ministry of Consumer Affairs releases the Consumer Protection (E-Commerce) (Amendment) Rules, 2026
- SEBI aligns its Cyber Incident Reporting Portal with the Financial Stability Board's FIRE format
- Gujarat and Uttar Pradesh notify their respective Data Centre Policies 2026

TELECOMMUNICATIONS

- Department of Telecommunications (DoT) notifies the Telecommunications (Authorisation for Telecommunication Network) Rules, 2026
- DoT notifies the Telecommunications (User Identification) Rules, 2026 mandating biometric verification for mobile connections
- DoT notifies the Telecommunications (Radio Equipment Possession Authorisation) Rules, 2026
- Telecom Regulatory Authority of India (TRAI) notifies the Telecom Commercial Communications Customer Preference (Third Amendment) Regulations, 2026

BROADCASTING & MEDIA

- **Ministry of Information and Broadcasting (MIB) publishes the draft Telecommunications (Television, Radio and Associated Services) Rules, 2026**
- **MIB removes the '10+2' advertising cap for television channels**

CASE LAW & LITIGATION UPDATES

- **Hon'ble Supreme Court issues nationwide directions to combat 'digital arrest' scams**
- **Hon'ble Supreme Court Lays Down CSEAM Detection and Reporting Framework for Intermediaries**

FINTECH

1. RBI proposes data-governance framework for regulated entities

The Reserve Bank of India (**RBI**), on July 15, 2026, released the draft *Guidance on Regulatory Expectations for Data Governance* (**Draft Data Governance Guidance**) for public consultation. The draft applies to commercial banks, small finance banks, payments banks, local area banks, regional rural banks, co-operative banks, All India Financial Institutions, non-banking financial companies (**NBFCs**), asset reconstruction companies and credit information companies. Comments were invited until August 17, 2026.

The Draft Data Governance Guidance treats data governance as an enterprise-wide responsibility rather than merely an information-technology function. It requires regulated entities to establish an accountable framework covering data ownership, stewardship, architecture, classification, quality, metadata, lineage, retention, disposal and third-party data-sharing arrangements.

Key Highlights

Governance framework - Regulated entities would be required to establish Board and executive-level oversight mechanisms, a central data-management function and identified data owners, data stewards and data custodians.

Single source of truth - An authoritative source would need to be identified for each material data element, with downstream systems, business processes and models deriving information from that source.

Metadata and lineage - Entities would be expected to document the origin, movement and transformation of data across systems, including the rules and logic applied during data processing.

Data security - Encryption, tokenisation, data-loss-prevention controls, anonymisation and secure disposal would need to be incorporated across the data lifecycle.

Third-party accountability - A regulated entity would remain responsible for data shared with service providers, group companies and other third parties.

Audit and assurance - Data-governance frameworks would be subject to risk-based internal and external audits, including audits by CERT-In-empanelled auditors where appropriate.

The proposed framework is particularly relevant for regulated entities and third parties, including group entities, with whom data sharing is contemplated. Regulated entities may need to identify critical data elements, maintain metadata and data lineage, implement controls governing access, usage and deletion of shared data, and review third-party arrangements to ensure appropriate audit, monitoring, confidentiality and security measures are in place.

2. RBI consolidates cybersecurity and technology-risk requirements

The RBI, on July 31, 2026, issued separate entity-specific *Cybersecurity, Technology: Risk, Resilience and Assurance Framework Directions, 2026* (**Cybersecurity Directions**) for commercial banks, small finance banks, payments banks, urban co-operative banks, All India Financial Institutions, NBFCs and credit information companies. The Cybersecurity Directions came into force immediately and consolidated the previously fragmented instructions on information-technology governance, cybersecurity, operational resilience and assurance.

Key Highlights

Board oversight - Regulated entities must adopt Board-approved cybersecurity and technology-risk policies and clearly allocate responsibility among the Board, senior management, information-technology function, risk function and Chief Information Security Officer.

Asset and access management - Entities must maintain inventories of information assets, implement identity and privileged-access controls and preserve audit trails for material information-technology assets and administrative activity.

Application security - Secure development, vulnerability management, source-code controls, patch management and periodic testing are required across the application lifecycle.

Cloud and outsourcing risk - Regulated entities remain accountable for technology and cyber risks arising from cloud-service providers and other outsourced arrangements.

Operational resilience - Business-continuity and disaster-recovery arrangements must cover severe but plausible cyber scenarios and be supported by periodic drills and recovery testing.

Testing and monitoring - The Directions contemplate continuous security monitoring, periodic vulnerability assessments, penetration testing and independent cybersecurity audits.

Incident management - Cyber incidents must be identified, escalated, reported and remediated under documented incident-response and cyber-crisis-management procedures.

Technology service providers supporting regulated entities, including cloud service providers, payment gateway operators, payment processors, software vendors, managed security service providers, ATM switch/application service providers and digital-lending technology partners, may see RBI-prescribed cybersecurity and operational resilience requirements impacting their contractual arrangements. These may include security controls, vendor due diligence requirements, audit and inspection rights, incident-notification obligations, business continuity and resilience testing requirements, and ongoing regulatory compliance obligations.

3. RBI strengthens digital payment security controls

Alongside the Cybersecurity Directions, the RBI on July 31, 2026 issued entity-specific *Digital Payment Security Controls Directions, 2026* (**Digital Payment Security Directions)** for commercial banks, small finance banks, payments banks, urban co-operative banks and eligible NBFCs. The NBFC-specific Directions apply to credit-card issuing NBFCs and cover digital-payment products offered directly or through RBI-authorised payment-system operators, together with the supporting applications, systems and infrastructure.

These directions cover both financial transactions and associated non-financial functions, including customer registration, balance enquiry, PIN creation or modification, generation of one-time passwords and digital grievance or dispute-management facilities.

Key Highlights

Board-approved policy - Regulated entities must adopt and periodically review a policy governing the functionality, security and performance of each digital-payment product.

Secure development - Digital-payment applications must follow secure-by-design development practices, threat modelling, secure coding and security testing throughout the application lifecycle.

Authentication - Multi-factor authentication must ordinarily be used for electronic payments and fund transfers, with at least one factor being dynamic or non-replicable.

Mobile applications - Controls include device binding, root and jailbreak detection, secure storage, identification of remote-access applications, session controls and phased deactivation of unsupported application versions.

Fraud monitoring - Regulated entities must monitor parameters such as transaction velocity, geolocation anomalies, high-risk merchant categories, rogue IP addresses and deviations from customer behaviour.

Reconciliation - Digital-payment transactions must be reconciled on a real-time or near-real-time basis, subject to the timelines prescribed in the applicable Direction.

Customer-facing alerts - Transaction alerts and statements should identify the actual merchant rather than merely displaying the payment aggregator or intermediary.

Third-party security - Regulated entities must assess the security posture of technology and payment partners and retain continuing oversight over outsourced payment functions.

Regulated entities may need to review authentication controls, mobile application security, fraud-monitoring parameters, reconciliation mechanisms, incident-management procedures and third-party

arrangements, and validate compliance through risk assessments, testing and control reviews, in addition to applicable PCI standards.

4. Government revises the UPI MDR framework

Central Government substantially altered the statutory framework governing charges on UPI transactions. The *Taxation and Other Laws (Amendment) Act, 2026* amended Section 10A of the Payment and Settlement Systems Act, 2007 by replacing the earlier linkage to payment modes prescribed under the income-tax legislation with a notification-based mechanism under which the Central Government may specify the electronic-payment modes that must remain charge-free.

The Ministry of Finance clarified on August 8, 2026 that consumers would not be charged for making UPI payments, all person-to-person transactions would remain free and any future merchant discount rate (**MDR**) would be restricted to a limited category of merchant transactions above a specified threshold. It also stated that the NPCI-led UPI and Services Steering Committee would determine the MDR structure. Thereafter, the Department of Financial Services issued Notification S.O. 5067(E) dated September 14, 2026, specifying:

- Debit cards powered by RuPay; and
- UPI transactions up to ₹2,000,

as the electronic-payment modes protected by Section 10A. Banks and system providers are prohibited from imposing, directly or indirectly, any charge on persons making or receiving payments through those specified modes. The ₹2,000 ceiling applies to UPI transactions; the Gazette notification does not prescribe a corresponding monetary ceiling for RuPay debit-card transactions.

The ensuing MDR framework provides for a 0.4% MDR on specified person-to-merchant UPI transactions above ₹2,000, effective from October 15, 2026, with a cap of ₹300 for transactions of ₹75,000 and above. Person-to-person transactions remain free, and small merchants receiving up to ₹1 lakh per month through UPI QR codes remain exempt; specified essential sectors attract a flat ₹5 charge, while capital-market transactions attract a differentiated rate of 0.02%.

The distinction between the legal instruments should be preserved in the newsletter: the September 14 Gazette notification defines the transactions protected from charges but does **not itself prescribe the 0.4% MDR**. The detailed rate structure arises from the subsequent payment-system framework and should not be attributed to S.O. 5067(E).

Banks, payment system providers and other payment ecosystem participants may need to ensure that no direct or indirect charge is imposed on persons making or receiving payments through UPI transactions up to ₹2,000 and review their payment processes and charging practices accordingly. Appropriate classification may now be required for charging specific type of transactions.

5. RBI issues draft KYC Amendment Directions prescribing a Standard Operating Procedure for suspected money mule accounts

The RBI on September 11, 2026 released the draft Reserve Bank of India (Know Your Customer) Amendment Directions, 2026 (**Draft KYC Amendment**). The Draft KYC Amendment modifies the existing instructions on operation of bank accounts and money mules under the KYC Directions, 2025 and introduces a Standard Operating Procedure on Suspected Money Mule Accounts to Prevent Cyber-enabled Financial Frauds.

Key Highlights:

Triggers – The procedure applies where transactions of ₹1,000 or more are flagged as suspicious by the bank's monitoring systems, or where account activity is unusual for, or disproportionate to, the account holder's declared profile.

Time-bound debit holds – Banks must place a temporary debit hold immediately upon identification and notify the customer instantly (for digital channels) or by the end of the next business day (for physical modes). Customers have 20 days to furnish an explanation, and the bank must decide within 10 days of receiving it, or within 30 days if no explanation is received. In the absence of instructions from law enforcement agencies, a debit hold may not exceed 60 days.

Applicability – The SOP is proposed to apply to commercial banks and urban co-operative banks, excluding nodal, pool and escrow accounts, with implementation by April 1, 2027.

Comments were invited until October 2, 2026. While the proposed SOP addresses a significant enforcement gap, fintechs and platforms relying on partner bank accounts may assess the operational impact of debit holds on their customers and settlement flows.

6. RBI recognises the Unified Fintech Forum as the second Self-Regulatory Organisation for the FinTech sector

The RBI, on September 10, 2026, recognised the Unified Fintech Forum (**UFF**), formerly the Digital Lenders Association of India, as a Self-Regulatory Organisation for the FinTech sector (**SRO-FT**). UFF is the second recognised SRO-FT after the Fintech Association for Consumer Empowerment.

Under the RBI's SRO-FT framework, a recognised organisation is expected to establish and enforce standards and codes of conduct, monitor members, promote consumer protection, data security and privacy, facilitate dispute resolution and act as an information bridge between the fintech industry and the RBI. Membership remains voluntary, and the framework primarily contemplates participation by fintechs not directly regulated by a financial-sector regulator, although regulated entities other than banks may also participate.

Digital lenders, lending-service providers, account-aggregation participants and other fintech firms may assess UFF's membership requirements, codes and accreditation mechanisms. Even where membership is not legally mandatory, standards issued by a recognised SRO may increasingly inform regulated entities' vendor-onboarding and due-diligence expectations.

INFORMATION TECHNOLOGY & DATA PROTECTION

7. The Ministry of Consumer Affairs releases the Consumer Protection (E-Commerce) (Amendment) Rules, 2026

The Ministry of Consumer Affairs has notified the Consumer Protection (E-Commerce) (Amendment) Rules, 2026, amending the Consumer Protection (E-Commerce) Rules, 2020 under the Consumer Protection Act, 2019. These amendments significantly tighten the framework on pricing transparency, search rankings, sponsored listings, dark patterns, data use and grievance redressal for e-commerce entities.

Commencement and scope

The Consumer Protection (E-Commerce) (Amendment) Rules, 2026 will come into force with effect from January 1, 2027. The amended rules apply to "e-commerce entities" and "marketplace e-commerce entities" operating in India and are framed under section 101(2)(zg) of the Consumer Protection Act, 2019 to modify the E-Commerce Rules, 2020.

What has changed – snapshot of key obligations

a. Price transparency and "prior price"

Whenever an e-commerce entity announces a price reduction, it must display both the reduced price and the "prior price" for the goods or services.

"Prior price" is defined as the lowest price at which the goods or services were offered during the 30 days preceding the announcement of the price reduction.

b. Search results and sponsored listings

E-commerce entities are barred from manipulating search results in a manner that misleads users or adversely affects the relevance of results to a user's search query

Sponsored or paid listings must be clearly and prominently identified as "sponsored" so that consumers can distinguish them from organic search results.

c. Dark patterns – mandatory compliance and audits

E-commerce entities are required to comply with the Guidelines for Prevention and Regulation of Dark Patterns, 2023.

Platforms must undertake an annual self-audit on dark patterns and prominently display a certificate of compliance on their website/app.

d. Grievance redressal and National Consumer Helpline (NCH)

Every e-commerce entity must become a convergence partner in the National Consumer Helpline (NCH) to integrate platform complaint handling with the national grievance mechanism.

The grievance officer of an e-commerce entity must provide the complainant with a copy of the complaint as recorded by the grievance officer.

e. Seller and product disclosures (including imports)

Marketplace e-commerce entities must display key product and seller information including best-before/use-before dates, return and refund policies, warranty terms, delivery timelines and payment details to enable informed consumer decisions.

For imported goods, marketplaces must disclose the importer's details and the country of origin on the product listing.

f. Use of consumer data and bundled charges

Marketplace e-commerce entities are prohibited from using consumer information for specified purposes without the consumer's express and affirmative consent.

Marketplace platforms cannot collect bundled fees for services unrelated to the e-commerce platform, subject to a limited exception for loyalty or membership programmes specifically provided for under the rules.

Practical implications for e-commerce entities

a. Platform design, pricing and search architecture

The statutory definition of "prior price" and the obligation to show both prices may require platforms to track and store price histories for at least the preceding 30 days for each product and align discount campaigns accordingly. Search and recommendation algorithms for marketplaces may need to be reviewed to ensure that ranking logic does not amount to "manipulation" that misleads users or undermines relevance, and that sponsored placements are transparently labelled.

b. Dark pattern governance and UI/UX review

The mandatory annual dark-pattern self-audit and public certificate of compliance effectively create an expectation of documented internal controls over interface design, consent flows, nudges and checkout

journeys. In-house and external counsel may likely need to work closely with product and UX teams to benchmark current practices against the 2023 Dark Pattern Guidelines and remediate high-risk patterns (e.g., forced opt-ins, confusing unsubscribe flows, bait-and-switch designs).

c. Data protection, consent and commercial charging models

The express and affirmative consent standard for using consumer information for specified purposes may require alignment with existing data-protection and privacy frameworks and clearer consent language in platform policies. Entities may also need to assess fee-charging practices in light of the express prohibition on collecting bundled fees for services unrelated to the e-commerce platform, subject to the specific exception for loyalty and membership programmes.

d. Contracts, seller onboarding and grievance processes

Enhanced disclosure requirements (expiry/use-before dates, warranties, refunds, delivery terms, importer details and country of origin) may flow into revised seller onboarding documentation, platform terms and internal listing guidelines for marketplace clients. Obligations relating to NCH convergence and providing complainants a recorded copy of their complaint may require updates to grievance-handling SOPs, consumer-facing policies and training of grievance officers for compliance by January 1, 2027.

8. SEBI aligns its Cyber Incident Reporting Portal with the Financial Stability Board's FIRE format

The Securities and Exchange Board of India (SEBI) issued Circular No. HO/(449)2026-ITD-5_DIV1/I/19448/2026 on August 24, 2026 (FIRE Circular). It aligns SEBI's Cyber Incident Reporting Portal with the Format for Incident Reporting Exchange (FIRE) developed by the Financial Stability Board (FSB). The FIRE Circular was issued under Section 11(1) of the Securities and Exchange Board of India Act, 1992. It must be read with the Cybersecurity and Cyber Resilience Framework of August 20, 2024 (CSCRF) and any later updates. The stock exchanges have since forwarded it to their members.

The FSB published FIRE in April 2025 as a common format for financial institutions to report operational incidents, including cyber incidents, to authorities. It responds to a long-standing industry concern: reporting requirements differ across regulators and jurisdictions. FIRE offers a common set of 87 information items, of which 39 are optional, grouped into reporting details, incident details, impact assessment and incident closure. It is modular, so each authority can adopt it in full or in part.

Key Highlights

a. Wide applicability - The FIRE Circular applies to almost every category of SEBI-regulated entity. These include:
   i. stock exchanges, clearing corporations, depositories, depository participants and stock brokers
   ii. mutual funds and AMCs, portfolio managers, AIFs, VCFs and collective investment schemes

iii. credit rating agencies, custodians, debenture trustees, merchant bankers, RTAs and KYC registration agencies

iv. bankers to an issue and SCSBs, investment advisers and research analysts

b. Existing timelines retained - The reporting deadlines in Annexure-O of the CSCRF do not change. Cyber incidents must still be reported by email to SEBI within 6 hours and on the SEBI Incident Reporting Portal within 24 hours.

c. Standardised data fields - Reports on the portal will now use FIRE's common information fields, standardised definitions and consistent classification of incident attributes. This includes identifying the locations and countries in which an incident occurred.

d. Lifecycle (staged) reporting - SEBI accepts that full information is rarely available when an incident is first detected. Reporting is now done in stages: an initial report, intermediate updates as the incident develops, and a final closure report. Updates must continue until the incident is resolved.

e. Single reporting channel - Regulated entities must report through SEBI's Cyber Incident Reporting Portal, accessed by logging in at siportal.sebi.gov.in.

The Circular aligns SEBI's Cyber Incident Reporting Portal with the FIRE reporting format and requires regulated entities to ensure that their incident-reporting processes and templates can capture and submit the prescribed FIRE-format information within existing reporting timelines.

9. Gujarat and Uttar Pradesh notify their respective Data Centre Policies 2026

The Government of Gujarat on July 9, 2026 launched the Viksit Gujarat Data Centre Policy 2026-29, targeting investment of ₹6 lakh crore and 7.5 GW of AI-ready, green data centre capacity, with Dholera positioned as a dedicated data centre cluster.

For projects with a minimum IT load of 150 MW, the policy offers a 20-year power tariff subsidy of ₹1 per unit, 100% stamp duty exemption, SGST reimbursement, interest subsidy capped at ₹25 crore per year, and total financial assistance capped at 75% of eligible fixed capital investment. The policy also mandates that at least 51% of energy for core operations be sourced from renewable energy and designates data centres as an "essential service", ensuring uninterrupted power and water supply. Read with the data localisation conditions under the Network Authorisation Rules, State-level incentives of this kind are likely to shape site selection for hyperscale and AI-compute infrastructure.

Similarly, the UP Cabinet approved the UP Data Center Policy on July 6, 2026. It is aimed at AI-ready, green data centres. It targets more than 2 GW of new capacity and over ₹2 lakh crore of investment. Incentives include capital and interest subsidies, stamp-duty, and electricity concessions among other benefits.

TELECOMMUNICATIONS

10. Department of Telecommunications (DoT) notifies the Telecommunications (Authorisation for Telecommunication Network) Rules, 2026

The DoT on July 20, 2026 notified the Telecommunications (Authorisation for Telecommunication Network) Rules, 2026 (**Network Authorisation Rules**), which came into force on the same date. The Network Authorisation Rules operationalise Section 3(1)(b) of the Telecommunications Act, 2023 (**Telecom Act**) and follow the draft rules published for stakeholder comments on October 9, 2025.

A network authorisation permits an entity to establish, operate, maintain or expand the relevant telecommunication network. It does not, however, authorise the provision of the underlying telecommunication service, which must be provided by an entity holding the applicable service authorization, and it does not confer a right to spectrum.

The network authorisation rules categorize authorisations as Infrastructure Provider (**IP**), Digital Connectivity Infrastructure Provider (**DCIP**), Internet Exchange Point (**IXP**) provider, Satellite Earth Station Gateway (**SESG**) provider, Cloud-hosted Telecommunication Network (**CTN**) provider and Mobile Number Portability (**MNP**) provider. The first five are granted at the national level, while MNP continues to be granted on a zonal basis across two MNP zones.

Authorisations under these rules are granted for a term of twenty years (*except for MNP authorisation which shall be granted for ten years)* with an option for renewal of upto twenty years (*ten for MNP authorisation*).

An application under the Network Authorization Rules is to be made on the designated portal along with payment of a non-refundable fee.

Any applicant having an overlapping license or authorization will relinquish the same prior to making the application under these rules. Any pending liabilities associated with the overlapping authorization specifically those such as roll out obligations, financial dues, determination of violations and imposition of penalty will remain applicable even after the relinquishment. Further any resource provided or permission given regarding the overlapping authorization will continue to apply, unless specifically determined by the Central Government.

The grant of authorization will be preceded by a letter of intent, requiring fulfillment of conditions such as reporting and disclosure obligations, transfer restrictions, technical, operating and security conditions among others.

Read with the release of Telecommunications (Authorisation for Provision of Principal Telecommunication Services) Rules, 2026 notified on June 23, 2026 (*covered in our last newsletter*), the

Network Authorisation Rules mark a decisive step in the sector's transition from the Unified Licence regime to an authorisation-based framework.

11. DoT notifies the Telecommunications (User Identification) Rules, 2026 mandating biometric verification for mobile connections

The DoT on August 21, 2026 notified the Telecommunications (User Identification) Rules, 2026 (**User Identification Rules**) under the Telecom Act.

The User Identification Rules have been notified in the backdrop of draft Telecommunications (User Identification) Rules, 2025 released in September 2025. These rules apply to wireless access service and internet telephony via mobile terminals, with a three-month time to comply, which the DoT may extend by up to a further three months.

Key Highlights:

Mandatory biometric identification – Biometric-based identification is required for enrolment of a new user, updating user information (such as name, gender or date of birth), SIM replacement, disconnection of services and any re-verification directed by the DoT.

KYC process – Users holding an Aadhaar number are to be verified through Aadhaar-based biometric e-KYC. For users without Aadhaar, the authorised entity must undertake a digital KYC process. For business users, the KYC of the authorized representative and each end user of the business connection is required.

User duties and enforcement – Users must furnish accurate information and must not use forged documents, impersonate others or suppress material information, and SIMs may not be resold or transferred (other than to relatives or legal heirs). Contraventions attract action under the user-duty and penalty provisions of the Telecom Act.

The User Identification Rules significantly tighten subscriber verification. Telecom service providers may need to rework onboarding measures and point-of-sale processes within the compliance window.

12. DoT notifies the Telecommunications (Radio Equipment Possession Authorisation) Rules, 2026

The DoT on July 8, 2026 notified the Telecommunications (Radio Equipment Possession Authorisation) Rules, 2026 (**Possession Rules**), which operationalise the authorisation requirement under Section 3(1)(c) of the Telecom Act for possession of radio equipment, while identifying categories of persons and equipment for which a separate possession authorisation is not required. The Possession rules come into effect immediately, any pending applications for grant of license under the Indian Wireless Telegraphy Act, 1933 will stand lapsed.

The Possession Rules establish a framework governing authorisation, possession, testing, demonstration, renewal, surrender, disposal and compliance relating to radio equipment. Authorisations may be obtained for the manufacture, import, purchase, sale, hire, repair, testing or demonstration of radio equipment.

Eligible applicants include companies and LLPs compliant with the applicable FDI policy, sole proprietors and partnership firms, Central and State Government agencies, and existing licensees under the Indian Wireless Telegraphy (Possession) Rules, 1965.

Applications are to be made through DoT's online portal with a non-refundable application fee, together with details of the make, model and quantity of the equipment.

13. Telecom Regulatory Authority of India (TRAI) notifies the Telecom Commercial Communications Customer Preference (Third Amendment) Regulations, 2026

The Telecom Commercial Communications Customer Preference Regulations, 2018 (**TCCPR**) were issued by TRAI on July 19, 2018 to address the growing instances of Unsolicited Commercial Communications (**UCC**) such as spam calls and messages.

In our January-March 2026 edition, we reported on the draft amendments to the TCCPR released by the TRAI on March 13, 2026 (**Draft Amendments**). TRAI on September 18, 2026 has finalised the Telecom Commercial Communications Customer Preference (Third Amendment) Regulations, 2026 (**Third Amendment**). The Third Amendment has been notified on the same date.

Its provisions come into force as follows; Regs 4, 6, 8(a), 18 at 60 days and Annexure items (23(1)(c), main clause of 25, proviso to 25(4)(d)(ii)) at 90 days, and the remaining regulations coming into force at 30 days.

Key Highlights:

Changes to the definition of Relationship and Consent - the proposed amendment reads down and clarifies the definition of Consent notably introducing three explanations to the definition addressing - establishment of communication channel, revocation of consent and the continued application of DPDP Act in addition to the obligations under these rules. The Third Amendment deletes first proviso to clause 2 (ah) which limited consent obtained herein to the duration of the obligation/contract between the sender and recipient.

Call management apps – The earlier suggested prohibition on Call management apps to blanketly tag, block or filter calls from the 140xx, 1600xx and 1601xx number series continues to apply. Failing to comply may result in TRAI action.

Application-to-Person (A2P) calls – Senders of UCC must declare use of A2P calls in advance, along with the details such as the Calling Line Identification (**CLI**) ranges used to making A2P calls. These

details will be recorded by originating access providers (**OAP**) and any A2P call made without prior declaration to the OAP will be treated as UCC.

AI/ML-based detection – Under Regulation 21A, terminating access providers must detect and flag suspected unsolicited commercial communications via AL/ML-based UCC Detect systems as *'suspected high probability of UCC CLI'* and within two hours of such identification share them with the originating access provider via the distributed ledger technology (**DLT**).

The behavior patterns to determine suspected high probability of UCCs will be notified by TRAI from time to time.

The tiered action mechanism by originating access providers against senders of suspected UCCs has been retained. These actions range from a re-KYC of the sender, barring the sender from using the access providers' network to blacklisting of the sender devices used in making UCCs by access providers.

Regulatory action against a sender of suspected UCCs will require both customer complaints and AI/ML flags.

Phased implementation – Provisions on AI/ML detection, A2P pre-declaration, restrictions on call management apps, and legacy consent take effect within 30 days; A2P charges and DLT digital interface access within 60 days; and the lowered complaint threshold (three complaints instead of five) within 90 days.

The third amendment brings changes to key blocks of the proposed amendments tightening thresholds against UCCs while creating defined pathways for legitimate business communications.

BROADCASTING & MEDIA

14. Ministry of Information and Broadcasting (MIB) publishes the draft Telecommunications (Television, Radio and Associated Services) Rules, 2026

The MIB via gazette notification dated September 2, 2026 has issued the Draft Telecommunications (Television, Radio and Associated Services) Rules, 2026 (**Draft Rules**) under the Telecom Act, proposing an authorisation framework for television channels, Direct-to-Home (**DTH**), Headend-in-the-Sky (**HITS**), private FM radio, community radio and Internet Protocol Television (**IPTV**) services. The Draft Rules replace the fragmented legacy framework with authorisations under the Telecom Act.

A few salient features of the Draft Rules are as below:

Scope of authorisations - The Draft Rules provide authorisations for television channels, television channel distribution services, teleports, news agencies for television, private radio services and community radio services. The framework provides that television channels, distribution services, teleports and news agencies will have a national service area, while private and community radio services will operate within specified geographical areas.

Grant of authorisation - An application for authorisation is subject to payment of application processing fee, security clearance of key managerial personnel. Certain authorisations such as IPTV require applicants to hold internet service authorisation or registration as a multi-system operator. The term for authorisation is ten years for television channel, teleport, community radio service and news agency for television, twenty years for television channel distribution service and fifteen years for private radio service.

Migration of existing authorisations - An application for migration to the authorisation framework has to be made via the same process as fresh applications barring levy of application process fee. Migration provisions are not applicable to permission holders of FM radio broadcasting service; in their cases the permissions will continue till its respective term.

Key operational obligations - Key operational obligations such as adherence to programme and broadcasting code, restrictions on sub-let/sub-leasing/assignment of authorisation continue to apply. Authorised television channels must broadcast programmes of national importance and social relevance for a minimum of 30 minutes each day between 6:00 AM and 11:00 PM, covering themes including education, agriculture, health, science and technology, welfare of women and weaker sections, environmental and cultural heritage, animal welfare and national integration.

Security, enforcement and penalties - Breach of any terms of authorisation is equated to a breach of the Telecom Act and attracts financial penalties on the same terms.

The Draft Rules propose transition of broadcasting sector to an authorisation-based framework under the Telecom Act while consolidating existing sector-specific guidelines. These materially impact television broadcasters, DTH and HITS operators, teleports, IPTV providers, private FM operators, community radio operators and other sectoral entities.

The Draft Rules were open for comments till October 2, 2026.

15. MIB removes the '10+2' advertising cap for television channels

The MIB by a Gazette notification dated August 21, 2026 notified the Cable Television Networks (Amendment) Rules, 2026, deleting sub-rule (11) of Rule 7 of the Cable Television Networks Rules, 1994. Rule 7 of the said rules stated:

'*No programme shall carry advertisements exceeding 12 minutes per hour, which may include up to 10 minutes per hour of commercial advertisements, and up to 2 minutes per hour of a channel's self-promotional programmes.*'

The deleted provision restricted television channels to 10 minutes of commercial advertising and 2 minutes of self-promotional content in an hour (the **10+2 cap**).

In consonance with this change, TRAI on September 10, 2026, also notified 'The Standards of Quality of Service (Duration of Advertisements in Television Channels) (Repealing) Regulations, 2026', repealing the Standards of Quality of Service (Duration of Advertisements in Television Channels) Regulations, 2012 dated May 14, 2012 which prescribed a ceiling of twelve minutes per clock hour on advertisements.

The amendments together give broadcasters flexibility in structuring advertising inventory, including sponsorships, branded content and in-programme integrations. Advertisers and broadcasters should, however, note that the content requirements of the Advertising Code under the Cable Television Networks Rules, 1994 continue to apply.

CASE LAW & LITIGATION UPDATES

16. Hon'ble Supreme Court issues nationwide directions to combat 'digital arrest' scams

The Hon'ble Supreme Court, in In Re: Victims of Digital Arrest Related to Forged Documents (*Suo Motu Writ Petition (Criminal) No. 3 of 2025*), by an order dated August 4, 2026 passed by a bench comprising Chief Justice Surya Kant, Justice Joymalya Bagchi and Justice V. Mohana, issued a series of nationwide directions to curb digital arrest scams.

The Court directed the RBI to adopt and circulate, an SOP prescribing action to be taken by banks for temporary debit holds on amounts or accounts linked to mule activity and cyber-enabled fraud (which led to the Draft KYC Amendment discussed above). States, Union Territories and law enforcement agencies were directed to operationalise the grievance redressal and money restoration modules under the Ministry of Home Affairs' cyber fraud framework and to create public awareness about them. The Court also directed the Inter-Departmental Committee to consult with intermediaries and banks on technological measures to prevent digital arrests and assist in recovery of defrauded amounts, and addressed the misuse of SIM cards and SIM boxes.

Pursuant to this direction, the RBI has released the Draft KYC Amendment introducing SOPs on suspected money mule accounts for preventing such frauds.

17. Hon'ble Supreme Court Lays Down CSEAM Detection and Reporting Framework for Intermediaries

In an order dated October 15, 2026 in *Just Rights for Children Alliance v S. Harish*, the Hon'ble Supreme Court took note of its earlier order dated September 23, 2024, expressing concern over the increase in circulation of child sexual exploitation and abuse material **(CSEAM)** on social media platforms.

The court primarily identified circulation of indirect links to bypass provisions of POCSO Act and IT Act and failure of a reporting obligation to Special Juvenile Police Unit as the underlying issues. To resolve these, the court directed the following:

Framework for detection and removal of CSEAM – Appropriate guidelines and SoPs to be framed by the Government for use of perpetual hash matching and URL listing by all major social-media intermediaries for detecting and removing CSEAM from their platforms. These guidelines will encompass all tools and technical measures that every intermediary will deploy for detection and removal, and will include any necessary amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 **(IT Rules)**.

Comprehensive National Database for detection and removal of CSEAM - A National Hash and URL list database, created solely to detect and remove CSEAM, can be built through the Sahyog portal or as a standalone repository. Each entry into this database will undergo multiple layers of verification, with the

final verification performed by three human analysts. Intermediaries will cross-check an entry against the database when removing or detecting CSEAM. If a match is found, it will be classified as being of *unknown origin*. When an intermediary removes CSEAM from an unknown source, proper verification and due diligence are required under the IT Rules. The intermediary should also report such matters to the authorities pursuant to the relevant law.

Notice Obligation - When an intermediary removes CSEAM material, it shall prominently display a notice at the materials' location on its platform. The notice must also indicate whether the material was removed on the intermediary's own detection or because a match was found against a known entry in the National Hash and URL list database.

Grievance redressal for any material removed - If material is removed by the intermediary's own detection, grievance redressal will be before the Grievance Appellate Committee under IT Rules. If material is removed because it matches the National Hash and URL List database, the challenge will lie before the authority designated and entrusted with maintaining the database.

Mechanisms for reporting of CSEAM – When material is removed or disabled as CSEAM due to a violation of Section 15 of the POCSO Act or Section 67B of the IT Act, it must be reported in accordance with POCSO rules to the Special Juvenile Police Unit, the local police, or the cybercrime portal, as required.

Where an intermediary removes or disables any CSEAM of *unknown origin*, this must also be reported to the authority responsible for maintaining the National Hash and URL List database. Further, if a CSEAM of *unknown origin* is removed, whether because of a complaint, its own diligence, or a court order, it must be reported within two hours of its removal.

If a CSEAM of *known origin* is disabled, the intermediary must submit a consolidated weekly report to the authority designated for maintaining the National Hash and URL List database.

Complaint mechanism and the publication of complaint mechanisms for addressing CSEAM - The IT rules already provide for the creation and publication of grievance officers' details. The same grievance mechanism is expanded to include a clear and distinct label category for reporting CSEAM. The mechanism should also be accessible within two steps and the nomenclature of the same should be simple enough to be understood by any person, irrespective of age, literacy, or familiarity with technology.

Further every intermediary must also publish a monthly compliance report detailing the number of complaints received by it, the action taken in respect of the same, the time within which such complaints were resolved, and the content, information or link or any part thereof removed or disabled pursuant to such complaint or by its own due diligence.

The court directed MeitY and Ministry of law and justice to take appropriate action for overseeing and implementing these suggestions, measures and safeguards and report progress to the court via an affidavit before the matter's next date on December 10, 2026.

Luthra and Luthra
LAW OFFICES INDIA

This newsletter is only for general informational purposes, and nothing in this edition of the newsletter could possibly constitute legal advice (which can only be given after being formally engaged and familiarizing ourselves with all the relevant facts). However, should you have any queries, require any assistance, or clarifications with regard to anything contained in this newsletter, please feel free to contact Vikash Kukreti, at the below mentioned coordinates.

© Luthra and Luthra Law Offices India 2026. All rights reserved.

The Team



VIKASH KUKRETI
Partner
vkukreti@luthra.com



GAURAV TIWARI
Senior Associate
Gtiwari@luthra.com



AKASH TAHENGURIA
Senior Associate
atahenguria@luthra.com

Offices

NEW DELHI
1st and 9th Floors, Ashoka Estate,
24 Barakhamba Road, New Delhi - 110 001
T: +91 11 4121 5100
F: +91 11 2372 3909
E: delhi@luthra.com

MUMBAI
20th Floor, Indiabulls Finance Center,
Tower 2 Unit A2, Elphinstone Road,
Senapati Bapat Marg, Mumbai - 400 013
T: +91 22 4354 7000
E: mumbai@luthra.com

BENGALURU
3rd Floor, Onyx Centre, No. 5, Museum Road,
Bengaluru - 560 001
T: +91 80 4112 2800 / +91 80 4165 9245
F: +91 80 4112 2332
E: bengaluru@luthra.com

HYDERABAD
Serene Towers,
House No. 8-2-623/A,
Road No. 10, Banjara Hills,
Hyderabad, Telangana - 500034
T: +91 40 7969 6162
E: hyderabad@luthra.com