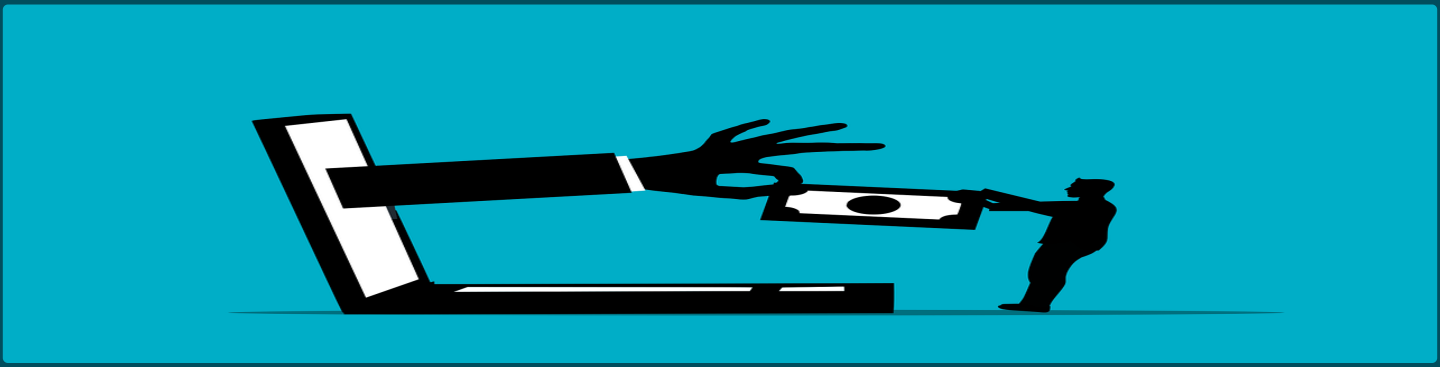

CIVIL

Preventing Financial Frauds Perpetrated Using Voice Calls and SMS: Key Highlights from the RBI Circular

AUTHOR Rahul Sundaram

PUBLISHED 20 January 2025

The Reserve Bank of India (RBI) has issued a critical circular (Circular No. RBI/2024-25/105, dated January 17, 2025, titled "Prevention of Financial Frauds Perpetrated Using Voice Calls and SMS – Regulatory Prescriptions and Institutional Safeguards") aimed at addressing the growing menace of financial frauds perpetrated through voice calls and SMS. With digital transactions becoming an integral part of modern banking, this circular provides regulatory measures and safeguards to ensure enhanced consumer protection. Below is an in-depth exploration of the circular's objectives, background, and actionable steps for Regulated Entities (REs).

Table of contents

Objective

The primary objective of the circular is to mitigate the risks of financial fraud arising from the misuse of mobile numbers, which are pivotal in authentication processes for digital transactions. Fraudsters often exploit these identifiers to access sensitive financial communications such as OTPs, transaction alerts, and account updates.

Background

While digital banking offers unmatched convenience, it has also become a fertile ground for fraudsters. Mobile numbers, being key identifiers in the banking ecosystem, have become vulnerable to misuse. Criminals use these identifiers for activities such as obtaining unauthorized access to accounts or diverting funds fraudulently. To combat this, the RBI has outlined measures that combine regulatory oversight, technological integration, and customer awareness.

Measures Required of Regulated Entities (REs)

The circular directs REs, including banks, non-banking financial companies (NBFCs), prepaid payment instrument issuers, and others, to implement the following measures:

1. Use the Mobile Number Revocation List (MNRL):

- **Source and Purpose:** The MNRL is available on the Digital Intelligence Platform (DIP) developed by the Department of Telecommunications (DoT). It contains categories of disconnected mobile numbers such as:
  - Numbers taken on forged documents.
  - Numbers involved in cybercrimes or financial frauds.
  - Numbers reported by citizens or disconnected due to fraud analysis by Telecom Service Providers (TSPs).
- **Actions for REs:**
  - Clean and update customer databases using the MNRL.
  - Enhance monitoring of accounts linked to revoked mobile numbers.
  - Prevent such accounts from being used as "money mules" or in other fraudulent activities.

2. Verified Customer Care Numbers:

- REs are required to share verified customer care numbers with the DIP to enable publication on the "Sanchar Saathi" portal " https://sancharsaathi.gov.in".

3. Use Specified Numbering Series for Communication:

- **Transactional and Service Calls:**
  - Use the '1600xx" numbering series (to be operationalized soon).
- **Promotional Voice Calls:**

- Use only the “140xx” numbering series.

- **Guidelines Compliance:**
  - Adhere to TRAI’s “Important Guidelines for sending commercial communication using telecom resources through Voice Calls or SMS.”

4. Awareness Initiatives:

- **Channels of Communication:**
  - REs must educate customers through emails, SMS, and other means, including vernacular languages, about these measures.
- **Content:**
  - Awareness campaigns should include information on identifying fraud, using DND registration to block unsolicited communications, and recognizing trusted communication from REs.

5. Implementation Timeline:

- REs must ensure full compliance with these directives by **March 31, 2025**.

Key Highlights from the Annexure

The circular includes an annexure detailing TRAI’s Telecom Commercial Communications Customer Preference Regulations, 2018 (TCCCPR-2018), which are critical for curbing unsolicited commercial communications (UCC). Some important regulatory requirements include:

- **Registration on DLT Platforms:**
  - All entities sending commercial communications must register on Distributed Ledger Technology (DLT) platforms.
  - Use only registered headers and content templates.
- **Digital Consent Acquisition (DCA):**
  - Obtain explicit digital consent from customers for promotional communications.
  - Use only the DCA systems deployed by Access Providers.
- **Data Confidentiality and Security:**
  - Ensure confidentiality and security of customer data.
  - Minimize the number of intermediaries (e.g., telemarketers) handling customer information.
- **Measures Against Misuse:**
  - Register only the necessary headers and content templates.
  - Deactivate unused headers to prevent unauthorized use.
  - Prohibit the use of URL shortening services that do not clearly indicate the sender’s identity.
- **Actionable Penalties:**
  - Non-compliance can result in disconnection of telecom resources and blacklisting of the entity for up to two years.

Conclusion

The RBI’s proactive measures underline the importance of a secure digital ecosystem, especially as reliance on mobile-based transactions continues to grow. By mandating the use of advanced fraud detection tools, standardized communication protocols, and strong customer awareness programs, this circular seeks to create a safer financial environment for all stakeholders. The timely adoption of these measures by REs will be central to minimizing fraud risks and building trust in digital banking services.

For further details write to contact@indialaw.in