

Robocall Mitigation Program

The Robocall Mitigation Program establishes a structured framework for telecommunications service providers to implement technical and operational solutions to reduce the impact of unwanted or fraudulent robocalls. Below are the key technical processes:

1. Call Authentication (STIR/SHAKEN)

Implementation of STIR/SHAKEN protocols: Providers must deploy call authentication protocols to verify the legitimacy of the origin of each call. This includes generating digital certificates that validate the caller's identity.

Validation of incoming calls: Receiving systems analyze the certificates associated with each call to identify potentially fraudulent calls.

2. Suspicious Call Blocking

Pattern-based call filtering: Algorithms analyze behavioral patterns associated with unwanted robocalls.

Blacklist and whitelist integration: Use of trusted databases to block numbers reported as abusive while ensuring valid numbers are not affected.

3. Collaboration and Transparency

Compliance reporting: Providers must submit regular reports to regulatory authorities detailing the measures implemented and their effectiveness.

Data sharing: Participation in information exchange networks to share intelligence on new threats and technological updates.

4. Consumer Education

Automatic alerts: Notifications to users when a suspicious call is blocked, Awareness campaigns: Education on how to identify and report fraudulent robocalls.

5. Monitoring and Continuous Improvement

Performance analysis: Regular evaluations of the effectiveness of implemented measures.

Technology updates: Adoption of new tools and methods to counter emerging tactics used by robocallers.