

Here's a **robocall mitigation plan** that outlines the steps and strategies to combat unwanted robocalls:

Robocall Mitigation Plan

1. Caller ID Authentication Framework (STIR/SHAKEN) Implementation

- Deploy the **STIR/SHAKEN** framework across our voice network.
- Verify caller identities by matching them with displayed caller IDs.
- Reject calls with invalid or unauthenticated caller information.

2. Certification in the Robocall Mitigation Database

- File regular certifications in the **Robocall Mitigation Database**.
- If STIR/SHAKEN is implemented:
 - Certify compliance with the framework.
- If not using STIR/SHAKEN:
 - Detail reasonable steps taken to prevent illegal robocall traffic.
- Ensure timely filing to avoid fines and restrictions.

3. Traceback Cooperation and Investigation

- Commit to responding within 24 hours to traceback requests.
- Collaborate with the FCC, law enforcement, and traceback consortia.
- Investigate and stop illegal robocallers exploiting our network.

4. Continuous Monitoring and Reporting

- Regularly monitor call traffic patterns.
- Identify suspicious activity related to robocalls.
- Report anomalies promptly for corrective action.

5. Educational Campaigns

- Launch consumer awareness campaigns:
 - Educate users about robocall risks.
 - Teach them how to recognize and report illegal calls.
 - Empower consumers to protect themselves.

6. Technological Solutions

- Implement call-blocking technologies:
 - Real-time analytics to identify fraudulent calls.
 - Spam filters to prevent unwanted calls.
- Enhance network security to maintain call integrity.

Remember, this plan aims to protect consumers, maintain network trust, and reduce the impact of robocalls. Regular reviews and updates are essential to stay ahead of evolving robocall tactics.