

SIPSYNCED Robocall Mitigation Strategy

1. Advanced Call Authentication

- **Implementation:** SIPSYNCED will integrate **STIR/SHAKEN protocols** into its VoIP infrastructure, ensuring all calls are authenticated, and suspicious calls are blocked at the network level.

2. Real-Time Robocall Detection

- **Action:** Deploy an advanced **real-time analytics engine** that monitors call patterns to instantly flag and block potential robocalls. This system learns and adapts to emerging scam tactics.

3. Dedicated Call Blocking Tools

- **Action:** Introduce a **user-controlled robocall blocking tool**, allowing customers to block high-risk numbers or set personalized filtering rules based on specific criteria, such as call volume or origin.

4. Partnership with Trusted Entities

- **Collaboration:** SIPSYNCED will collaborate with leading **anti-robocall organizations** and government bodies to share data, improve tracking, and report suspicious activity effectively.

5. Proactive Customer Engagement

- **Education:** SIPSYNCED will send regular **tips and alerts** to customers about recognizing and blocking robocalls, empowering users to take control of their call experience.

6. Robust Reporting and Transparency

- **Action:** Implement a transparent **reporting portal** for customers to easily flag unwanted calls and review mitigation effectiveness. This will allow SIPSYNCED to adjust filters based on user feedback.