

Inmateaid, LLC Robocall Mitigation Plan

—

1. Mitigation Plan Overview

The Federal Communications Commission (FCC) requires certain communication service providers to adopt the STIR/SHAKEN call authentication framework and other measures to combat robocalls. The rules also mandate that all voice service providers certify their progress in implementing STIR/SHAKEN. Providers not fully compliant, including those with extensions, must apply a robocall mitigation program to the exempted parts of their network.

Core requirements for a robocall mitigation program as outlined by the FCC:

- a. Preventing illegal robocalls
- b. Traceback cooperation
- c. Investigating and stopping illegal activity

This Robocall Mitigation Plan outlines the measures Inmateaid, LLC has implemented to prevent the transmission of illegal robocalls, ensuring compliance with FCC regulations. Inmateaid, LLC helps families of the incarcerated save money on phone communications and provides services globally to connect with individuals incarcerated in U.S. jails and prisons.

All calls facilitated by Inmateaid, LLC are initiated by inmates. Our Direct Inward Dialing (DID) numbers are exclusively for receiving inbound calls. Inmates dial these cost-optimized DIDs, which then forward the calls to the customer's existing phone lines. Due to this design, customers cannot place outbound calls using Inmateaid, LLC services, making it impossible for robocalls to originate from the Inmateaid, LLC voice network under normal use.

2. Operational Context

- Call Origination: All calls facilitated through our services are initiated by inmates from correctional facilities.
- Call Reception: End users utilize the provided DIDs exclusively to receive these inbound calls.
- Outbound Calls: Our company does not originate outbound calls over IP networks.

3. Robocall Mitigation Strategies

- Know Your Customer (KYC) Procedures:
 - When a user creates an account through Inmateaid, LLC, we conduct thorough due diligence on all end users to verify their legitimacy and intent.

- Monitor for any suspicious or unordinary user activities
- Network Monitoring and Analytics:
 - Use backend tools to detect patterns indicative of unauthorized use of DIDs.
 - Utilize analytics to identify and address any anomalies in call reception that may suggest misuse.
- Collaboration and Traceback Response:
 - Commit to responding promptly to traceback requests from the FCC, law enforcement, and industry traceback consortiums.
 - Cooperate fully in investigations to identify and halt any misuse of our services.
- Employee Training:
 - Provide regular training to employees on robocall mitigation techniques and regulatory compliance.
 - Establish clear protocols for identifying and reporting suspected misuse of our services.

4. Record-Keeping

Maintain detailed records of all mitigation efforts, including end user verification processes, monitoring activities, and responses to traceback requests. Ensure records are readily available for FCC review upon request.

5. Customer Education

Provide resources and support to help end users understand their role in maintaining the integrity of our services.

6. Compliance and Review

Regularly review and update the Robocall Mitigation Plan to align with evolving FCC regulations and industry best practices. Conduct periodic audits to assess the effectiveness of mitigation strategies and implement improvements as necessary.

7. Certification

Inmateaid, LLC certifies that it has implemented this Robocall Mitigation Plan in compliance with FCC regulations and is committed to preventing the transmission of illegal robocalls through its services.