



IPVOICE PLUS

3030 N Rocky Point Drive West
Suite 150
Tampa FL 33607
Phone 813-774-3551 | f.813-569-2366
<http://www.ipvoiceplus.com>

Because your business requires more than just a phone line.

In Re: **In the Matter of 2,411 Robocall Mitigation Database Filers,**

FCC ORDER Number: EB-TCD-24-00036891

Pursuant to the above referenced FCC Enforcement Bureau Order, IPVoice Plus hereby respectfully submits their Robo-Call Mitigation Plan to meet compliance with 47 CFR § 64.6305(d)-(e).

Robo-Call Mitigation Plan

1. Provider Overview

- **Company Name:** IPVoice Plus, LLC
- **Company RMDB No.** RMD0009420
- **FCC Registration Number (FRN):** 0031642614
- **Type of Provider:** Voice Service Provider
- **Contact Information for Robocall Mitigation Compliance Officer:**
 - Name: Mr. Jeff Miranda
 - Title: CIO
 - Email: jlmiranda@ipvoiceplus.com
 - Phone: 813-774-3570

2. IPVoice Plus Mitigation Practices

IPVoice Plus, LLC implements the below specified Robocall mitigation practices. Our Mitigation plan ensures compliance with 47 CFR § 64.6305(d)-(e), and further outlines IPVoice Plus's proactive measures to prevent, detect, and mitigate illegal robocalls while meeting the FCC's certification requirements.

A. Call Authentication

1. STIR/SHAKEN Compliance

- Implement the STIR/SHAKEN framework in the IP portions of the network to validate caller identity.
- Certify compliance with the STIR/SHAKEN protocols in accordance with 47 CFR § 64.6301.

2. Non-IP Network Mitigation

- For non-IP networks, employ alternative measures such as:
 - Monitoring traffic for suspicious patterns.
 - Signing and verifying calls using out-of-band mechanisms.

B. Traffic Monitoring and Analytics

1. Real-Time Call Analytics

- Deploy real-time analytics software to:
 - Detect anomalies in call patterns.
 - Identify high-volume, short-duration calls indicative of robocalling.

2. Traffic Blocking

- Block illegal calls identified using analytics tools or known bad actors listed in the FCC's Robocall Mitigation Database.
- Ensure blocking decisions align with the FCC's rules to minimize false positives.

C. Verification of Customers

1. Know-Your-Customer (KYC) Policy

- Conduct due diligence on all new customers before activation, verifying:
 - Identity.
 - Intended use of services.
- Monitor ongoing customer behavior to ensure continued compliance with terms of service.

2. Prohibited Use Enforcement

- Terminate service agreements with customers engaging in illegal robocalling.

3. Filing and Certification

A. Certification in FCC's Robocall Mitigation Database

- Submit a certification to the FCC's Robocall Mitigation Database stating:
 - Full implementation of the STIR/SHAKEN framework or specific mitigation practices for non-IP traffic.
 - An attestation that these practices are effective in curbing illegal robocalls.

B. Annual Updates

- Update the certification annually or as required to reflect any changes to mitigation practices.

4. Complaint Resolution Process

A. Complaint Handling

- Establish a process to handle robocall-related complaints, including:
 - A dedicated email and phone line for consumers to report illegal robocalls.
 - Timely investigation and resolution of complaints.

B. Coordination with Enforcement Agencies

- Cooperate with law enforcement and regulatory agencies, including the FCC, in investigating and mitigating illegal robocalling.

5. Compliance Monitoring and Reporting

A. Internal Audits

- Conduct periodic audits of call traffic, authentication measures, and customer onboarding processes to ensure compliance.

B. Incident Reporting

- Report significant illegal robocall incidents or security breaches to the FCC and other relevant agencies promptly.

6. Employee Training

- Develop training programs for employees to:
 - Identify illegal robocalling activity.
 - Understand the technical and regulatory requirements of STIR/SHAKEN and mitigation practices.
 - Respond effectively to customer inquiries and regulatory requests.

7. Record Retention

- Maintain records of all call traffic, mitigation efforts, and customer verification data for a minimum of three years.