



Robocall Mitigation Plan

IT/Ops Management LLC

Date: December 20, 2024

Contact Information:

- **Robocall Mitigation Program Manager:** Ray Colmenares
 - **Phone Number:** 754.201.3366 x 9
 - **Email:** support@itops.co
-

1. Program Overview

This Robocall Mitigation Plan outlines IT/Ops Management LLC's strategies, policies, and procedures to detect, reduce, and prevent unlawful robocalls across our network. Our program complies with the Federal Communications Commission (FCC) requirements and is designed to ensure trust in our voice services.

2. Call Authentication Practices

Implementation of STIR/SHAKEN:

- Calls originating from our IP-based networks are signed using **Secure Telephone Identity (STI) certificates** from Third-Party Integrators to authenticate caller ID information.

Third-Party Integration:

- IT/Ops Management LLC partner with Vitelity, Telnyx, VoIP.ms, Twilio, and other third-party STIR/SHAKEN providers to enable call signing and verification.
-

3. Traffic Monitoring and Analytics

Traffic Analysis:

- Monitor network traffic for suspicious patterns such as:
 - High call volumes from a single source.
 - Short call durations.

- High frequency of invalid or unassigned numbers.

Fraud Detection Tools:

- Deploy analytics software and industry data to identify and flag potential robocall sources.
 - Maintain logs of flagged calls for reporting and investigation.
-

4. Call Blocking Policies

Blocking Fraudulent Calls:

- Use data from industry consortiums and FCC guidance to block calls from known illegal robocall sources.
- Maintain and update blacklists of flagged numbers.

Whitelist for Legitimate Traffic:

- Maintain a whitelist of verified numbers for critical communications (e.g., emergency services).
-

5. Caller ID Management

Verified Caller ID:

- Ensure all outbound calls use verified and legitimate caller IDs.
- Prohibit customers from using unregistered or spoofed caller IDs.

Customer Accountability:

- Terminate or suspend service for customers found engaging in caller ID spoofing or illegal robocall activity.
-

6. Customer Vetting and Education

Customer Onboarding:

- Screen new customers to identify potential high-risk entities.
- Require compliance agreements for customers using our voice services.

Education:

- Provide resources to customers on legal robocall practices and FCC compliance.
-

7. Secure Interconnections**Network Security:**

- Establish secure connections with upstream and downstream providers to prevent unauthorized access.
 - Work collaboratively with interconnecting providers to trace and mitigate robocall sources.
-

8. Reporting and Accountability**Call Logging:**

- Maintain detailed logs of call activity for compliance verification and fraud investigations.

FCC Reporting:

- Notify the FCC of any suspected unlawful activity and cooperate fully with enforcement actions.
-

9. STI Certificate Management**Certificate Issuance and Renewal:**

- Use FCC-approved certificate authorities to issue STI certificates.
 - Renew certificates as required to ensure continuous compliance.
-

10. Customer Complaint Handling**Complaint Mechanism:**

- Provide a dedicated email and phone line for customers to report suspected robocalls.

- Investigate complaints promptly and take corrective action as necessary.
-

11. Compliance with Regulations

Robocall Mitigation Database Certification:

- Maintain an up-to-date certification in the FCC's **Robocall Mitigation Database (RMD)**.

Regulatory Updates:

- Regularly review FCC guidance and update our practices accordingly.
-

12. Program Review and Updates

- Conduct periodic reviews of this plan to ensure its effectiveness and compliance with evolving regulations.
 - Document updates and communicate changes to relevant stakeholders.
-

13. Acknowledgment and Approval

IT/Ops Management LLC's leadership has reviewed and approved this plan.

Authorized Signature:

Raymond T Colmenares

President

IT/Ops Management LLC

Date: December 20, 2024