

Robocall Mitigation Plan

ACE Telecom

OCN: NA

5/27/2025

Submitted to the Federal Communications Commission's Robocall Mitigation Database

1. Introduction

ACE Telecom a small business VOICE SERVICE PROVIDER, is committed to combating illegal robocalls and protecting consumers from unwanted and fraudulent calls. This Robocall Mitigation Plan outlines the reasonable and effective steps we take to prevent the origination, carriage, or processing of illegal robocalls on our network, in compliance with the Federal Communications Commission (FCC) regulations, including the TRACED Act and STIR/SHAKEN implementation requirements.

This plan details our policies, procedures, and technological measures to mitigate illegal robocalls, including our approach to caller ID authentication, know-your-customer and know-your-upstream-provider practices, call analytics, and cooperation with industry and regulatory traceback efforts. We certify that this plan is actively implemented and adhered to across our operations.

2. STIR/SHAKEN Implementation Status

ACE Telecom has not yet implemented the STIR/SHAKEN caller ID authentication framework on our network, as described below:

My company has "No STIR/SHAKEN Implementation" due to a lack of control of the network infrastructure necessary to implement STIR/SHAKEN.

- We are taking affirmative steps to mitigate illegal robocalls through alternative measures, as detailed below.

3. Robocall Mitigation Program

To prevent the origination, carriage, or processing of illegal robocalls, ACE Telecom has implemented a comprehensive robocall mitigation program that includes the following reasonable steps:

3.1 Know-Your-Customer (KYC) Procedures

We maintain robust KYC processes to verify the identity and legitimacy of customers originating calls on our network:

- **Customer Onboarding:** All new and renewing customers undergo identity verification, including validation of business registration, contact information, and intended use of telephone numbers.

- **Due Diligence:** We review customer call patterns and usage to identify potential risks of illegal robocall activity. Customers flagged for suspicious activity are subject to additional scrutiny, including potential suspension of services.
- **Contractual Obligations:** Our customer agreements explicitly prohibit the use of our services for illegal robocalls or spoofing, with clear consequences for violations, including termination of service.

3.2 Know-Your-Upstream-Provider Procedures

For intermediate and gateway providers, we implement procedures to vet upstream providers:

- **Provider Vetting:** We verify that all upstream providers are registered in the FCC's Robocall Mitigation Database and have valid certifications. We do not accept traffic from unregistered providers.
- **Traffic Monitoring:** We monitor upstream traffic for signs of illegal robocalls, such as high call volumes, unusual calling patterns, or numbers associated with consumer complaints.
- **Contractual Requirements:** Upstream providers are required to certify compliance with FCC robocall mitigation rules and cooperate with traceback requests.

3.3 Call Analytics and Blocking Mechanisms

We deploy advanced call analytics to identify and block illegal robocalls:

- **Blacklist Implementation:** We maintain and regularly update blacklists of known robocall sources, including numbers on the FCC's Do Not Originate (DNO) list and numbers identified through industry traceback efforts. Calls from blacklisted numbers are blocked or diverted to a CAPTCHA-based Interactive Voice Response (IVR) system for further verification.
- **Call Labeling:** Suspicious calls are labeled to alert downstream providers and consumers, enabling informed call-blocking decisions.

3.4 Cooperation with Traceback Efforts

We actively participate in industry and regulatory traceback efforts to identify and stop illegal robocall campaigns:

- **FCC Cooperation:** We commit to fully cooperating with FCC Enforcement Bureau investigations, including providing call detail records and other relevant data.
- **Proactive Measures:** When notified of illegal robocall activity, we investigate promptly, terminate services to offending customers, and update our mitigation processes to prevent recurrence.

3.5 Do Not Call (DNC) Compliance

We ensure compliance with federal and state Do Not Call (DNC) regulations:

- **DNC Scrubbing:** We scrub outbound call lists against the National DNC Registry and applicable state DNC lists to prevent calls to registered numbers.
- **Consumer Opt-Outs:** We maintain an internal DNC list and honor consumer opt-out requests promptly.

3.6 Network Monitoring and Reporting

We continuously monitor our network to detect and mitigate illegal robocall activity:

- **Real-Time Monitoring:** Our systems monitor call volumes, durations, and patterns to identify anomalies indicative of robocall campaigns.
- **Incident Reporting:** Suspected illegal robocall activity is reported to our compliance team for investigation and, if necessary, escalated to the FCC or industry traceback groups.
- **Post-Incident Analysis:** After mitigating an illegal robocall incident, we analyze root causes and update our mitigation strategies to prevent future occurrences.

4. Organizational Information

To support FCC compliance and transparency, we provide the following details about our organization:

- **Company Name:** ACE Telecom
- **Business Address:** 9 Springlake Ct., Ballwin, MO 63011
- **Contact Person for Robocall Mitigation Issues:**
 - Name: Glenn Hanlin
 - Title: owner
 - Telephone: 314-503-4145
 - Email: glenn@ace-telecom.com
- **Prior Enforcement Actions:** ACE Telecom has not been subject to FCC, law enforcement, or regulatory actions related to illegal robocalls or spoofing in the past two years. No such actions or investigations have occurred in the prior two years.

5. Certification of Compliance

ACE Telecom certifies, under penalty of perjury, that:

- We have implemented the robocall mitigation measures described in this plan and are actively adhering to them.
- We have not yet implemented STIR/SHAKEN, as described in Section 2.
- We take reasonable steps to prevent the origination, carriage, or processing of illegal robocalls, including KYC procedures, call analytics, and cooperation with traceback efforts.
- We comply with FCC regulations, including timely updates to our Robocall Mitigation Database filings within 10 business days of any changes to the information provided.
- We commit to responding to traceback requests within 24 hours and cooperating fully with FCC and industry investigations.

Signed:

Glenn Hanlin, (owner)

5-27-2025

6. Ongoing Compliance and Updates

[Your Company Name] is committed to maintaining and updating this robocall mitigation plan to ensure ongoing compliance with FCC regulations:

- **Regular Assessments:** We conduct quarterly reviews of our robocall mitigation program to evaluate its effectiveness and incorporate new industry best practices.
- **Employee Training:** We provide regular training to employees on robocall mitigation techniques, FCC regulations, and emerging robocall threats.
- **Database Updates:** We update our Robocall Mitigation Database filing within 10 business days of any changes to our contact information, STIR/SHAKEN implementation status, or mitigation practices.
- **Technology Upgrades:** We continuously evaluate and adopt new technologies to enhance our robocall mitigation capabilities, including advancements in call analytics and STIR/SHAKEN implementation.

7. Filing Instructions and Submission

This Robocall Mitigation Plan and accompanying certification will be filed in the FCC's Robocall Mitigation Database via the online portal at <https://www.fcc.gov/robocall-mitigation-database> by [insert filing date, e.g., February 26, 2024, or other applicable deadline]. The submission will include:

- A PDF of this Robocall Mitigation Plan.
- A completed certification form, electronically signed by an officer of the company.
- Our FCC Registration Number (FRN) and associated business information, as registered in the FCC's Commission Registration System (CORES).

8. Consequences of Non-Compliance

We understand that failure to comply with FCC robocall mitigation requirements, including filing a complete and accurate certification and plan, may result in:

- Removal from the Robocall Mitigation Database, leading to mandatory call blocking by downstream providers.
- Fines of up to \$23,727 per call for violations of mandatory blocking requirements.
- Enforcement actions by the FCC's Enforcement Bureau, including cease-and-desist orders.

[Your Company Name] is committed to avoiding these consequences by maintaining full compliance with FCC regulations and actively combating illegal robocalls.

End of Robocall Mitigation Plan

Notes for Customization

1. **Tailor to Your Operations:** Replace placeholders (e.g., [Your Company Name], [specific reasons]) with details specific to your organization, such as network type (IP or non-IP), services offered, and actual mitigation practices.
2. **STIR/SHAKEN Details:** Clearly state your STIR/SHAKEN implementation status. If not implemented, provide a detailed explanation and emphasize alternative mitigation measures.
3. **Vendor Information:** If using third-party vendors for analytics or call-blocking, include their names and a brief description of their services.
4. **Legal Review:** Consult with legal counsel or a compliance expert to ensure the plan meets FCC requirements and addresses any unique aspects of your operations, especially if you are a gateway or foreign provider.
5. **Filing Deadline:** Ensure submission by the FCC's deadline (e.g., February 26, 2024, for updated filings, or other applicable dates).
6. **Documentation:** Maintain records of your mitigation efforts, traceback cooperation, and customer vetting processes to support your certification if audited by the FCC.

Filing Instructions

- **Register for an FRN:** Obtain an FCC Registration Number via the FCC's CORES system if you do not already have one.
- **Access the Portal:** Submit the plan and certification via the FCC's Robocall Mitigation Database portal at <https://www.fcc.gov/robocall-mitigation-database>.
- **Format:** Submit the plan as a PDF and ensure the certification is electronically signed by an officer of the company.

Additional Resources

- FCC Robocall Mitigation Database: <https://www.fcc.gov/robocall-mitigation-database>
- FCC STIR/SHAKEN Guidelines: <https://www.fcc.gov/call-authentication>
- TransNexus Robocall Mitigation Solutions: <https://transnexus.com>
- USTelecom Industry Traceback Group: <https://www.ustelecom.org>

This template provides a framework to meet FCC requirements, but it is not exhaustive. Ensure your plan is detailed, specific, and reflective of your actual practices to avoid deficiencies or enforcement actions. If you need further assistance, consider engaging a compliance consultant or contacting the FCC's Enforcement Bureau for clarification.

Certification Statement

I, [Name], [Title], certify under penalty of perjury that the information provided in this Robocall Mitigation Plan is true and correct to the best of my knowledge and that [Your Company Name] is actively implementing the described measures to mitigate illegal robocalls.

Signed: _____

Date: [MM/DD/YYYY]

This plan is designed to help you comply with FCC requirements while providing a clear, actionable framework to combat illegal robocalls. Let me know if you need help tailoring specific sections or additional guidance!