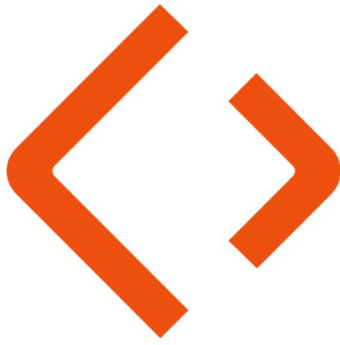




JAWEX
A TECHNOLOGY COMPANY

ROBOCALL MITIGATION PLAN

FCC Registration Number (FRN): 0037134152

11-24-25

Plan Version: 1.0

1. EXECUTIVE SUMMARY

JAWEX is a voice service provider that provides telecommunications services to business customers in Oklahoma and surrounding regions. This Robocall Mitigation Plan describes the specific, reasonable steps the Company has implemented to prevent the origination, transmission, and processing of illegal robocall traffic on our network, in compliance with 47 CFR § 64.6305 and the FCC's Sixth Caller ID Authentication Report and Order.

Provider Type(s): Voice Service Provider with STIR/SHAKEN implementation obligation serving end-users

STIR/SHAKEN Implementation Status: Fully

2. STIR/SHAKEN IMPLEMENTATION

2.1 Current Implementation Status

We are a white label partner of www.skyswitch.com, A BCM One company. They comply with STIR/SHAKEN implementation.

3. REASONABLE STEPS TO PREVENT ILLEGAL ROBOCALLS

The Company has implemented the following specific, detailed practices that can reasonably be expected to significantly reduce the origination, carrying, and processing of illegal robocall traffic:

3.1 Customer Onboarding and Verification ("Know Your Customer")

3.1.1 New Customer Procedures

All prospective customers undergo a comprehensive verification process before service activation:

- Verification of Business:
 - In person meeting to verify business's legitimacy
 - Business license verification and Secretary of State registration checks for business entities
 - Physical address verification
- Use Case Documentation: Customers must provide:
 - Detailed description of intended call use cases
 - Expected call volumes and patterns
 - Types of calls to originate (transactional, informational, marketing, etc.)

- Documentation of any marketing campaigns and TCPA compliance procedures

3.1.2 Service Denials

We maintain right to refuse service to:

- All businesses who refuse an in-person meeting to initiate service
- All businesses who refuse to provide sufficient information proving their state filings or intended business use is legitimate.

3.2 Renewing Customer Procedures

3.2.1 Annual Recertification

All existing customers must annually:

- Update business information and contact details
- Provide current use case documentation if calling patterns have changed
- Certify continued compliance with TCPA and TSR requirements

3.2.2 Ongoing Monitoring

Customer accounts are subject to continuous review:

- Quarterly reviews of call patterns and volumes
- Investigation of any significant changes in calling behavior
- Review of customer complaint rates
- Checks against updated FCC enforcement actions and traceback reports

3.3 Know-Your-Upstream Provider Procedures

3.3.1 Upstream Provider Vetting

Skyswitch.com provides upstream vetting

3.3.2 Contractual Requirements

All contracts with upstream providers include provisions requiring:

- Compliance with all FCC robocall mitigation rules
- Prohibition on sending illegal robocall traffic
- Immediate notification of any traceback investigations
- Right to immediately terminate for non-compliance
- Indemnification for any illegal traffic originated by the upstream provider

3.3.3 Ongoing Upstream Monitoring

We monitor upstream providers through:

- Quarterly reviews of traffic quality and complaint rates
- Immediate investigation of any traceback requests related to upstream traffic
- Suspension or termination of providers that fail to maintain compliance

3.4 Call Analytics and Blocking

3.4.1 Call Analytics System

The Company utilizes a manual review process inside our Skyswitch customer dashboard

3.4.2 Blocking and Mitigation Actions

- We block calls exhibiting clear illegal robocall patterns
- We investigate and collaborate with Skyswitch to determine the best plan for mitigation

****3.4.3 Manual Review Process****

Our operations team reviews flagged traffic within [timeframe, e.g., "2 hours"] and:

- Contacts customers to verify legitimate business purposes
- Implements additional restrictions if unable to verify legitimacy
- Suspends service for confirmed illegal activity
- Documents all reviews for FCC compliance purposes

3.5 Number Management

3.5.1 Number Allocation Controls

We maintain strict controls over telephone number allocation:

- Numbers are only assigned to verified customers
- Numbers are not ported out without customer identity verification

3.5.2 Ported Number Monitoring

For numbers ported into our network, we:

- Verify the porting customer's identity matches the authorized user
- Monitor newly ported numbers for immediate high-volume calling (indicative of number hijacking)
- Investigate any consumer complaints about recently ported numbers

3.6 Complaint Handling and Investigation

3.6.1 Consumer Complaint Process

We maintain a dedicated process for handling robocall complaints:

- Complaints can be submitted via phone, email, or web portal
- All complaints are logged and investigated within 24 hours

- Customers are contacted immediately regarding complaints
- Repeat offenders face service suspension or termination

3.6.2 Investigation Procedures

For each complaint, we:

- Pull complete call detail records (CDRs)
- Review customer's calling patterns for similar behavior
- Interview customer regarding the specific calls
- Take immediate action to prevent recurrence
- Document findings for FCC compliance records

3.7 Employee Training and Compliance

3.7.1 Training Program

All employees involved in customer onboarding, network operations, or compliance receive training on:

- FCC robocall mitigation requirements
- TCPA and TSR requirements
- Identifying illegal robocall patterns
- Proper complaint handling procedures
- Traceback response requirements

Training is conducted yearly and upon hire for new employees.

3.7.2 Compliance Officer

We have designated Jacob White as our Robocall Mitigation Compliance Officer responsible for:

- Overseeing implementation of this mitigation plan
- Serving as primary contact for FCC and law enforcement
- Managing traceback responses
- Ensuring ongoing compliance with all requirements

4. TRACEBACK RESPONSE COMMITMENT

4.1 24-Hour Response Guarantee

The Company commits to respond fully and completely to all traceback requests from the FCC, the USTelecom Industry Traceback Group (ITG), law enforcement agencies, and state regulatory bodies within 24 hours of receipt.

4.2 Traceback Contact Information

Primary Contact: Jacob White

Title: Owner

Email: jacob@jawexsupport.com

Phone: 918-740-1931

Backup Contact: Tyler Wilkerson at help@jawexsupport.com/918-631-5299

4.3 Traceback Response Process

Upon receiving a traceback request, we will:

1. Immediately acknowledge receipt (target: within 12 hours)
2. Pull all relevant call detail records (CDRs) for the identified calls
3. Identify the customer or upstream provider that originated the traffic
4. Provide complete information to the requesting party within 24 hours including:

- Customer identification and contact information
- Complete CDRs for the traced calls
- Any relevant contractual documentation
- Actions taken to address the issue

5. Take immediate mitigation action including:

- Suspending service if illegal activity is confirmed
- Blocking the specific numbers used for illegal calls
- Terminating repeat offenders

6. Cooperate fully with ongoing investigations

4.4 Upstream Tracebacks

For traffic received from upstream providers, we will:

- Immediately forward traceback requests to the appropriate upstream provider
- Verify the upstream provider responds within 24 hours
- Terminate upstream relationships if providers fail to respond appropriately
- Provide all available information even if the originating provider is upstream

4.5 Voluntary Reporting

In addition to responding to tracebacks, we proactively report suspected illegal robocall campaigns to the ITG when we identify them through our monitoring systems.

5. ENFORCEMENT AND REMEDIATION

5.1 Service Suspension/Termination

We will immediately suspend or terminate service for customers who:

- Are confirmed to be originating illegal robocalls

- Fail to respond to inquiries regarding suspected illegal traffic
- Refuse to cooperate with investigations
- Violate our Acceptable Use Policy
- Are named in FCC enforcement actions
- Fail to respond to traceback-related inquiries

5.2 Financial Penalties

Our customer contracts include provisions for:

- Financial penalties for AUP violations
- Cost recovery for investigation and compliance activities
- Liquidated damages for causing regulatory actions against the Company

5.3 Law Enforcement Cooperation

We cooperate fully with:

- FCC Enforcement Bureau investigations
- Federal law enforcement (FBI, FTC, DOJ)
- State attorneys general
- State public utility commissions
- Private civil litigation related to TCPA violations

6. RECORD KEEPING

6.1 Required Records

We maintain the following records for a minimum of 2 years:

- Customer verification documentation
- Acceptable Use Policy acknowledgments

- Call detail records (CDRs)
- Complaint logs and investigation reports
- Traceback requests and responses
- Service suspension/termination notices
- Employee training records
- Analytics system logs and blocked call reports

6.2 Record Availability

All records are maintained in electronic format and can be produced to the FCC, law enforcement, or regulatory agencies within 72 hours of request.

7. PLAN REVIEW AND UPDATES

7.1 Regular Review

This Robocall Mitigation Plan is reviewed and updated:

- Annually at minimum
- Upon any changes to FCC requirements
- Following any significant robocall-related incident learnings
- When new analytics capabilities are deployed

7.2 FCC Notification

Any material changes to this plan will be reflected in an updated filing to the FCC Robocall Mitigation Database within 10 business days of implementation.

8. NETWORK SECURITY

8.1 Network Access Controls

Our network implements security measures to prevent unauthorized use:

- Regular password rotation requirements
- Two-factor authentication for administrative access

8.2 Fraud Detection

We monitor for signs of account compromise:

- Unusual login locations or times
- Sudden changes in call volumes
- Calls to unusual destinations
- Multiple failed authentication attempts

8.3 Incident Response

Upon detecting potential account compromise, we:

- Immediately suspend the affected service
- Contact the customer via verified contact information
- Investigate the extent of any unauthorized usage
- Reset all credentials before restoring service

9. REGULATORY ACTIONS AND INVESTIGATIONS

The Company has not been subject to any Commission, law enforcement, or regulatory agency action or investigation related to suspected unlawful robocalling or spoofing.

10. CERTIFICATIONS

10.1 Compliance Certification

I, Jacob White, Owner of JAWEX, hereby certify under penalty of perjury that:

1. All calls that originate on our network are subject to the robocall mitigation program described in this plan
2. This plan includes detailed practices that can reasonably be expected to significantly reduce the origination of illegal robocall traffic
3. The Company complies with the practices described in this plan
4. The Company will respond fully to traceback requests within 24 hours
5. Any prior certification filed by the Company has not been removed by Commission action
6. The Company has not been prohibited from filing in the Robocall Mitigation Database
7. All information provided in this plan is true, accurate, and complete

10.2 Officer Signature

A handwritten signature in black ink, appearing to read 'J. White', is written over a horizontal line.

Jacob White

Owner

11-24-2025

APPENDIX A: CONTACT INFORMATION

Robocall Mitigation Point of Contact:

- Name: Jacob White
- Title: Owner
- Department: IT
- Business Address: 11005 S. Granite Ave. Tulsa, OK 74137 USA
- Phone: 918-359-5299
- Email: jacob@jawexsupport.com

24/7 Traceback Response Contact:

- Phone: 918-359-5299 (Press number for on-call engineer)
- Email: help@jawexsupport.com

Legal/Regulatory Contact:

- Name: Jacob White
- Phone: 918-359-5299
- Email: jacob@jawexsupport.com

APPENDIX B: DEFINITIONS

****Illegal Robocall:**** Any call that violates the Telephone Consumer Protection Act (TCPA), the Telemarketing Sales Rule (TSR), or other applicable federal or state laws, including calls made without prior express written consent, calls to numbers on the National Do Not Call

Registry, spoofed calls intended to defraud, and calls that deliver artificial or prerecorded voice messages without proper consent.

****STIR/SHAKEN:**** The Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using toKENs (SHAKEN) standards that provide a framework for caller ID authentication.

****Traceback:**** An investigation process used to identify the source of illegal robocalls by tracing the call path through multiple providers back to the originating source.

****END OF ROBOCALL MITIGATION PLAN****

This plan is submitted in compliance with 47 CFR § 64.6305 and the requirements established in the FCC's Sixth Caller ID Authentication Report and Order (FCC 23-18) and Public Notice DA 24-73.