

ROBocall Mitigation Plan

Southeastern Technology Specialists, LLC

1. Introduction

Southeastern Technology Specialists, LLC (“STSSC”) is a South Carolina-based interconnected VoIP and hosted PBX service provider serving small and medium-sized business customers.

STSSC is committed to full compliance with the Federal Communications Commission (FCC) rules regarding:

- 47 C.F.R. § 64.6305 (Robocall Mitigation)
- STIR/SHAKEN implementation requirements
- Industry Traceback Group (ITG) cooperation
- FCC Robocall Mitigation Database (RMD) certification requirements

STSSC maintains a documented and actively enforced robocall mitigation program designed to prevent unlawful robocalls and illegal caller ID spoofing.

2. Role in the Call Chain

STSSC operates as:

- ✓ An originating interconnected VoIP provider
- ✓ A hosted PBX provider
- ✗ Not an intermediate provider
- ✗ Not a gateway provider
- ✗ Not a facilities-based carrier

STSSC provides hosted VoIP services and assigns telephone numbers to business end users.

All calls are routed to the Public Switched Telephone Network (PSTN) through **Sangoma Carrier Services**, which provides PSTN interconnection and call authentication services.

STSSC does not:

- Operate its own SS7 network

- Maintain direct PSTN interconnection facilities
 - Operate a standalone STIR/SHAKEN Authentication Service
 - Hold its own SPC token at this time
-

3. STIR/SHAKEN Implementation Status

STSSC currently relies on **Sangoma Carrier Services** to perform call signing and attestation under Sangoma's STIR/SHAKEN certificate.

- Calls are signed by Sangoma under its own certificate.
- Attestation levels are determined by Sangoma.
- STSSC does not independently sign calls.
- STSSC does not currently maintain an SPC token.

STSSC reserves the right to obtain its own SPC token and certificate in the future if required by FCC rule changes or upstream carrier policy.

4. Upstream Provider Verification

STSSC verifies that:

- Sangoma Carrier Services is registered in the FCC Robocall Mitigation Database.
- Sangoma maintains active STIR/SHAKEN implementation.
- Sangoma complies with FCC traceback and authentication requirements.

STSSC periodically reviews its upstream provider's compliance status.

5. Know Your Customer (KYC) Procedures

STSSC maintains enhanced customer onboarding controls, including:

Identity Verification

- Collection of government-issued identification for individuals
- Verification of business registration for commercial accounts
- Verification of business address and contact information

Contractual Controls

- Written Master Service Agreement (MSA)
- Explicit prohibition of:
 - Illegal robocalling
 - Caller ID spoofing
 - Use of autodialers for unlawful activity
- Immediate termination clause for violations

Screening Procedures

- Screening customers against:
 - FCC enforcement action lists
 - Known robocall enforcement databases
 - Review of intended call use cases prior to activation
-

6. Traffic Monitoring and Mitigation

STSSC actively monitors network traffic for suspicious activity.

Monitoring includes:

- High call volume spikes
- Short-duration calls
- Sequential dialing patterns
- Excessive calls to high-risk destinations
- Unusual answer-seizure ratios

If suspicious activity is detected:

1. Customer is contacted immediately.
2. Traffic may be suspended.
3. Service may be terminated.
4. Upstream provider may be notified.

7. Traceback Cooperation Policy

STSSC designates the following traceback contact:

Joseph Pedalino

Southeastern Technology Specialists, LLC

Email: jpedalino@stssc.net

Phone: (843) 480-3745

Traceback Commitments

- STSSC will respond to all Industry Traceback Group (ITG) or FCC traceback requests within 24 hours.
- STSSC maintains Call Detail Records (CDRs) for a minimum of 24 months.
- STSSC cooperates fully with law enforcement investigations.
- STSSC will preserve relevant call records upon request.

8. Data Retention Policy

STSSC maintains:

- Call Detail Records (CDRs) for 24 months
- Customer onboarding documentation
- Signed service agreements
- Identity verification records

All records are securely stored and accessible for regulatory compliance.

9. Enforcement & Escalation Policy

If unlawful traffic is identified:

- Immediate service suspension may occur.
- Customer account is reviewed.
- Upstream carrier is notified.

- Authorities may be notified if required.

Repeat violations result in permanent service termination.

10. Annual RMD Certification Compliance

STSSC certifies that:

- It maintains an active robocall mitigation program.
- It complies with 47 C.F.R. § 64.6305.
- It has not been removed from the RMD within the last two years.
- It has not been subject to FCC enforcement for illegal robocalling.
- All information submitted to the FCC is true and correct.
- STSSC understands that false certification may result in penalties.

11. Future Compliance Enhancements

STSSC will continue evaluating:

- Obtaining its own SPC token
- Implementing independent call authentication
- Enhancing analytics and traffic monitoring tools
- Strengthening customer vetting procedures

12. Conclusion

Southeastern Technology Specialists, LLC is committed to:

- Protecting consumers
- Preventing illegal robocalls
- Maintaining regulatory compliance
- Cooperating fully with federal and industry enforcement efforts

This mitigation plan is reviewed annually and updated as required by FCC rule changes.

