

ROBOCALL MITIGATION PROGRAM DESCRIPTION

Company Name: CSB Technologies

Date: [Current Date - e.g., September 19, 2025]

FCC Registration Number (FRN): 0031430564

Operating Company Number (OCN): N/A (CSB Technologies operates as a VoIP service provider using Bandwidth's network infrastructure)

1. EXECUTIVE SUMMARY

CSB Technologies is committed to preventing illegal robocalls and protecting consumers from unwanted and fraudulent calling activities. Our robocall mitigation program implements reasonable steps to avoid originating, carrying, or processing illegal robocall traffic on our network.

As an interconnected VoIP service provider serving approximately 2,500 business customers, we partner with Bandwidth (a major facilities-based carrier) to provide voice services. Our robocall mitigation program leverages both our internal policies and procedures as well as Bandwidth's network-level protections and STIR/SHAKEN implementation.

Our program includes comprehensive customer verification procedures, traffic monitoring through our upstream provider partnerships, customer education, and incident response protocols to maintain network integrity and consumer protection. We work closely with Bandwidth to ensure that industry-standard robocall mitigation measures are applied to our traffic.

We continuously evaluate and improve our robocall mitigation measures to adapt to evolving threats and comply with all applicable FCC regulations and industry best practices.

2. COMPANY INFORMATION

2.1 Contact Information

- **Primary Contact Name:** Brian Robison
- **Title:** Chief Technology Officer
- **Department:** Engineering
- **Business Address:** 2035 Lakeside Centre Way # 200, Knoxville, TN 37922
- **Telephone Number:** 619-246-3188
- **Email Address:** brian.robison@shopboss.net

2.2 Service Provider Classification

- ☐ Voice service provider with STIR/SHAKEN implementation obligation directly serving end users
- ☐ Voice service provider with STIR/SHAKEN implementation obligation acting as wholesale provider
- ☒ Voice service provider without STIR/SHAKEN implementation obligation
- ☐ Gateway provider
- ☐ Intermediate provider

Note: CSB Technologies operates as an interconnected VoIP service provider that relies on Bandwidth's network infrastructure for call routing and STIR/SHAKEN implementation. As a reseller/retail provider using a facilities-based carrier's network, we do not have direct STIR/SHAKEN implementation obligations but rely on our upstream provider's implementation.

3. STIR/SHAKEN IMPLEMENTATION STATUS

3.1 Current Implementation Status

CSB Technologies does not directly implement STIR/SHAKEN as we operate as a VoIP service provider using Bandwidth's network infrastructure. Our STIR/SHAKEN implementation is handled at the network level by our upstream provider.

- **Implementation Date:** Not directly implemented by CSB Technologies
- **Reason for Non-Implementation:** CSB Technologies operates as a retail VoIP provider using Bandwidth's facilities-based network. STIR/SHAKEN authentication is handled by Bandwidth at the network infrastructure level.
- **Upstream Provider STIR/SHAKEN Status:** Bandwidth has implemented STIR/SHAKEN across their network infrastructure
- **Planned Direct Implementation:** Not applicable - robocall mitigation is achieved through upstream provider relationship and internal customer management policies

3.2 Technical Details

CSB Technologies relies on Bandwidth's network infrastructure for call routing and authentication services. Our robocall mitigation approach focuses on:

- Customer verification and management
- Traffic monitoring through our service agreements with Bandwidth
- Incident response and customer support
- Policy enforcement for our business customer base

Network Architecture: IP-based VoIP services delivered through Bandwidth's nationwide network infrastructure **Authentication Methods:** Handled by upstream provider (Bandwidth) with STIR/SHAKEN implementation **Verification Processes:** Customer-level verification and account management, with network-level verification handled by Bandwidth

3.3 Extensions or Exemptions

☒ No extensions or exemptions requested - CSB Technologies operates as a retail provider using facilities-based carrier infrastructure ☐ Extension granted for: N/A ☐ Exemption claimed as: N/A

4. ROBOCALL MITIGATION MEASURES

4.1 Call Origination Controls

Customer Verification Process:

- We maintain detailed records of all business customers authorized to originate calls on our network
- New customers must provide business name and registration information
- Tax ID/EIN numbers are collected during onboarding
- We verify the intended use of phone service during the signup process
- Regular reviews of customer accounts and calling patterns through our partnership with Bandwidth

Know Your Customer (KYC) Procedures:

- Customer onboarding includes business registration verification
- We maintain current contact information for all 2,500 business customers
- Tax identification verification is required for all business accounts
- Intended use documentation helps ensure legitimate business purposes
- Customer information is regularly reviewed and updated

Telephone Number Management:

- We track all telephone numbers assigned to customers through our Bandwidth partnership
- Numbers are assigned only for legitimate business purposes as verified during onboarding
- We monitor number usage through call detail records available via Bandwidth
- Regular audits of number assignments and customer authorization

Traffic Monitoring:

- Real-time monitoring of call volumes and patterns through Bandwidth's network systems
- Access to call detail records for all customer traffic
- Investigation of any unusual calling patterns identified by our upstream provider
- Ongoing review of customer accounts and calling behavior

4.2 Traffic Analysis and Blocking

Analytics Systems Used: ☒ Call detail record analysis through Bandwidth partnership ☒
 Upstream provider traffic monitoring and alerts ☐ Third-party robocall detection services ☐
 Custom analytics tools ☒ Partner-based traffic analysis and reporting

Call Blocking Criteria:

- Unusual calling patterns identified through Bandwidth's monitoring systems
- Reports from Bandwidth regarding suspicious traffic from our customer base
- Any traffic patterns inconsistent with documented business use
- Coordination with Bandwidth on network-level blocking decisions

List Management:

- Customer allowlists maintained based on verified business accounts
- Coordination with Bandwidth on traffic management decisions
- Regular review of customer accounts and calling authorization
- Partnership-based approach to traffic validation and management

4.3 Network Security Measures

- **Access Controls:** Network security managed through Bandwidth's infrastructure with customer-level access management by CSB Technologies
- **Fraud Detection:** Coordinated fraud detection through upstream provider monitoring and customer account management
- **Interconnection Security:** Secured through Bandwidth's network infrastructure and interconnection agreements
- **Call Detail Record (CDR) Analysis:** Regular analysis of customer traffic patterns through CDR access via Bandwidth

4.4 Customer Education and Support

- **Customer Notification Programs:** Direct communication with business customers regarding robocall policies and compliance
- **Complaint Handling:** CSB Technologies has not received robocall complaints from customers to date, but maintains procedures for investigation and coordination with Bandwidth if such complaints arise
- **Educational Resources:** Information provided to customers about appropriate use of voice services and robocall regulations

- **Call Labeling/Display:** Network-level call labeling handled by Bandwidth's STIR/SHAKEN implementation
-

5. UPSTREAM PROVIDER REQUIREMENTS

5.1 Provider Verification

- **Primary Upstream Provider:** Bandwidth Inc. - a major facilities-based telecommunications carrier
- **Due Diligence Process:** Bandwidth is a publicly traded telecommunications company (NASDAQ: BAND) with established FCC compliance and robocall mitigation programs
- **Robocall Mitigation Database Verification:** Bandwidth maintains active status in the FCC's Robocall Mitigation Database
- **Contract Requirements:** Service agreements with Bandwidth include robocall mitigation and compliance provisions
- **Performance Monitoring:** Ongoing oversight through service level agreements and regular account management

5.2 Traffic Acceptance Policies

- **Acceptance Criteria:** All traffic is routed through Bandwidth's network infrastructure with their established robocall mitigation measures
 - **Rejection Procedures:** Network-level blocking and filtering handled by Bandwidth's systems
 - **Documentation Requirements:** Traffic records maintained through Bandwidth's network management systems
 - **Quality Assurance:** Regular monitoring of service quality and compliance through upstream provider relationship
-

6. DOWNSTREAM CUSTOMER REQUIREMENTS

6.1 Customer Agreements

- **Acceptable Use Policies:** Service terms managed through partnership agreements, with Bandwidth handling network-level acceptable use enforcement
- **Compliance Requirements:** Business customers are required to provide legitimate business information and intended use documentation
- **Monitoring and Enforcement:** Customer compliance monitored through account management and coordination with Bandwidth
- **Termination Procedures:** Account termination procedures available for non-compliant customers, though no terminations have been necessary to date

6.2 Customer Support Systems

- **Onboarding Process:** New business customers provide business registration, tax ID, and intended use information
 - **Ongoing Monitoring:** Regular account reviews and traffic monitoring through Bandwidth partnership
 - **Violation Response:** Procedures in place for addressing any identified violations in coordination with upstream provider
 - **Account Management:** Continuous review of all 2,500 business customer accounts
-

7. MONITORING AND ENFORCEMENT

7.1 Internal Monitoring

- **Real-time Monitoring:** Network-level monitoring through Bandwidth's infrastructure with customer account oversight by CSB Technologies
- **Reporting Systems:** Access to traffic reports and analytics through upstream provider partnership
- **Performance Metrics:** Customer account management and service quality monitoring
- **Audit Procedures:** Regular review of customer accounts and service usage patterns

7.2 External Cooperation

- **Industry Collaboration:** Participation in robocall mitigation through upstream provider industry involvement
 - **Information Sharing:** Coordination with Bandwidth on traffic analysis and threat intelligence
 - **Regulatory Cooperation:** Full cooperation with FCC inquiries and enforcement actions
 - **Law Enforcement Cooperation:** Available to assist with investigations through proper channels and upstream provider coordination
-

8. CONTINUOUS IMPROVEMENT

8.1 Technology Updates

- **System Upgrades:** Technology improvements implemented through Bandwidth's network infrastructure upgrades
- **New Technology Evaluation:** Ongoing evaluation of service enhancements and robocall mitigation technologies through upstream provider
- **Performance Optimization:** Regular optimization of customer services and account management processes

8.2 Policy and Procedure Updates

- **Regular Reviews:** Ongoing review of customer management policies and procedures
 - **Staff Training:** Employee education on robocall regulations and customer management best practices
 - **Best Practice Implementation:** Adoption of industry standards through upstream provider partnership and internal policy development
-

9. REPORTING AND DOCUMENTATION

9.1 Record Keeping

- **Data Retention:** Customer records and service documentation maintained in accordance with regulatory requirements
- **Documentation Standards:** Business customer information, tax identification, and service usage records maintained
- **Access Controls:** Appropriate access controls for sensitive customer information and service records

9.2 Reporting Procedures

- **Regulatory Reporting:** Compliance with all FCC reporting requirements including this Robocall Mitigation Database filing
 - **Incident Reporting:** Procedures in place for reporting any significant events or compliance issues
 - **Performance Reporting:** Regular monitoring and reporting of service quality and customer account status
-

10. EFFECTIVENESS MEASURES

10.1 Key Performance Indicators

- **Customer Account Management:** Successful onboarding and management of 2,500 business customers
- **Service Quality:** Maintaining high-quality voice services through upstream provider partnership
- **Compliance Record:** Zero customer terminations for robocall violations to date
- **Customer Satisfaction:** Ongoing customer account management and service delivery

10.2 Success Metrics

- **Customer Retention:** Strong customer relationships and service satisfaction
 - **Compliance History:** No robocall complaints or violations reported
 - **Account Management:** Effective oversight of all business customer accounts
 - **Partnership Performance:** Successful coordination with upstream provider for service delivery and compliance
-

11. CONFIDENTIAL INFORMATION NOTICE

[Note: This section should be included in your confidential version but redacted in the public version]

11.1 Proprietary Technology Details

[Detailed technical specifications that could compromise security if disclosed publicly]

11.2 Sensitive Business Information

[Customer lists, financial data, or other commercially sensitive information]

11.3 Security-Related Information

[Specific security measures that could be exploited if publicly disclosed]

12. CERTIFICATION

I hereby certify under penalty of perjury that I am an officer or employee of CSB Technologies and that I have examined the foregoing robocall mitigation program description and that all statements of fact contained therein are true and correct to the best of my knowledge, information, and belief.

Signature: 
Name: Brian Robison
Title: Chief Technology Officer
Date: 9.19.2025

APPENDICES

Appendix A: Technical Architecture Diagrams

[Network diagrams showing STIR/SHAKEN implementation]

Appendix B: Policy Documents

[Copies of relevant internal policies and procedures]

Appendix C: Vendor Agreements

[Relevant portions of agreements with technology vendors]

Appendix D: Performance Data

[Historical data on robocall mitigation effectiveness]

This document contains both confidential and non-confidential information. The confidential version includes proprietary technical details, while the non-confidential version redacts sensitive information that could compromise network security or competitive position.