

VoIP Robocall Mitigation Program

This Robocall Mitigation Program establishes our comprehensive policies, procedures, and technical controls to prevent illegal robocalls and comply with FCC regulations, including the TRACED Act and STIR/SHAKEN requirements. This program applies to all voice services provided through our VoIP network.

1. Objectives

Prevent the transmission of illegal robocalls through our network and managed services
Ensure compliance with FCC robocall mitigation requirements
Implement and utilize STIR/SHAKEN authentication protocols
Maintain customer trust and service quality
Minimize regulatory and legal risks

2. Regulatory Framework

2.1 Applicable Regulations

- **TRACED Act (2019)**: Requires robocall mitigation programs
- **FCC Part 64**: Truth in Caller ID and robocall restrictions
- **TCPA (Telephone Consumer Protection Act)**: Consent requirements
- **CAN-SPAM Act**: Email and text message regulations
- **STIR/SHAKEN Requirements**: Call authentication protocols

2.2 Compliance Timeline

June 30, 2021: Large providers must implement STIR/SHAKEN

June 30, 2022: Small providers compliance deadline

Ongoing: Robocall mitigation program updates and reporting

3. Technical Implementation

3.1 STIR/SHAKEN Authentication

Implementation Requirements

Deploy and utilize STIR/SHAKEN authentication on all originated calls

Verify authentication on terminated calls

Utilize telecom partners existing infrastructure for call validation

Implement proper attestation levels:

A-Level: Full authentication (originating customer known)

B-Level: Partial authentication (customer known, number not verified)

C-Level: Gateway authentication (call from known source)

3.2 Call Analytics and Monitoring

Real-Time Analysis

Call pattern analysis for suspicious activity
Volume thresholds and anomaly detection
Caller ID validation and verification
Call duration and answer seizure ratio monitoring

Analytics Parameters

High-volume calling: >150 calls/hour per customer

Short duration calls: <6 seconds average

Sequential dialing: Consecutive number patterns

Low answer rates: <10% answer seizure ratio

3.3 Network-Level Controls

Traffic Shaping

Rate limiting per customer account
Geographic call routing restrictions
Time-of-day calling limitations
Destination number pattern blocking

Blocking and Filtering

[Customer Equipment] → [SIP Proxy/Partner] → [STIR/SHAKEN Engine] → [Carrier Network]
↓
[Authentication Service] ← [Certificate Authority] ← [Policy Administrator]

- Known robocaller number databases
- Suspicious caller ID patterns
- Invalid or malformed numbers
- International premium rate numbers

4. Customer Onboarding and Verification

4.1 Know Your Customer (KYC) Procedures

Business Verification

Federal Tax ID (EIN) verification
Business license validation
Physical address confirmation
Authorized representative identification

Individual Customer Verification

Government-issued photo ID
Social Security Number verification
Address verification

Credit check (if applicable)

High-Risk Customer Assessment

- Telemarketing and call center businesses
- Debt collection agencies
- Political campaigns and similar organizations
- Survey and polling companies

4.2 Service Agreement Requirements

Acceptable Use Policy

- Prohibition of illegal robocalls
- TCPA compliance requirements
- Caller ID accuracy mandates
- Volume and usage restrictions

Customer Responsibilities

- Maintain accurate caller ID information
- Obtain proper consent for automated calls
- Implement internal compliance procedures
- Report suspicious activity

5. Monitoring and Detection

5.1 Automated Monitoring Systems

Call Detail Record (CDR) Analysis

- Real-time call volume monitoring
- Pattern recognition algorithms
- Statistical anomaly detection
- Cross-reference with complaint databases

Key Performance Indicators

- Calls per minute/hour/day, per customer
- Average call duration
- Answer seizure ratio
- Complaint ratio per customer

5.2 Manual Review Processes

Tier 1 Review Triggers

- Customer complaint reports
- Regulatory agency notifications
- Carrier partner alerts
- Automated system flags and analytics/reports

Tier 2 Escalation Criteria

- Multiple complaint reports
- Regulatory investigation notices
- Carrier termination threats
- Legal action notifications

6. Response and Mitigation Procedures

6.1 Immediate Response Actions

Service Suspension Criteria

- Confirmed illegal robocall activity
- Customer non-response to investigation
- Regulatory enforcement action
- Carrier partner demands

Escalation Timeline

- 0 - 2 hours** - Initial investigation and customer contact
- 2 - 24 hours** - Service restriction implementation
- 24 - 72 hours** - Full investigation completion
- 72 + hours** - Final resolution and reporting

6.2 Customer Communication

Notification Requirements

- Written and digital notice of investigation
- Opportunity to respond and provide evidence
- Clear explanation of violations
- Appeal process information

Documentation Standards

- Detailed investigation records
- Customer correspondence logs
- Technical evidence preservation
- Regulatory reporting preparation

7. Complaint Handling

7.1 Complaint Sources

- Direct customer reports
- Industry Traceback Group (ITG)
- FCC Consumer Complaint Center
- State regulatory agencies
- Carrier partner notifications

7.2 Investigation Process

Initial Assessment (24 hours)

- Complaint validity verification
- Customer account identification
- Call record analysis and investigation
- Preliminary finding documentation

Full Investigation (72 hours)

- Complete call history review
- Customer interview and evidence collection
- Technical analysis and verification
- Final determination and action plan

7.3 Resolution Actions

- Customer education and training
- Service limitations or restrictions
- Account suspension or termination
- Regulatory reporting and cooperation

8. Training and Awareness

8.1 Staff Training Program

Technical Training

- STIR/SHAKEN implementation and troubleshooting
- Call analytics and monitoring systems
- Regulatory compliance requirements
- Investigation procedures and documentation

Customer Service Training

- Complaint handling procedures
- Customer communication protocols
- Escalation processes
- Legal and regulatory awareness

8.2 Customer Education

Onboarding Materials

- Robocall compliance guidelines
- Best practices documentation and expectations
- Technical implementation guides
- Regulatory requirement summaries

Ongoing Communication

- Compliance updates
- Regulatory change notifications
- Industry trend reports
- Training program invitations

9. Record Keeping and Reporting

9.1 Documentation Requirements

Customer Records

- Verification and onboarding documentation
- Service agreements and amendments
- Complaint and investigation records
- Correspondence and communication logs

Technical Records

- Call detail records and analytics
- Monitoring system reports
- Network configuration change records

9.2 Regulatory Reporting

FCC Robocall Mitigation Database

- Annual program certifications with partners and Carriers
- Significant update notifications
- Compliance status reports
- Contact information maintenance

Industry Traceback Cooperation

- Traceback request responses
- Investigation cooperation
- Evidence and documentation sharing
- Resolution reporting

10. Program Governance

10.1 Organizational Structure

Program Leadership

Chief Compliance Officer:	Overall program responsibility
Technical Director:	Implementation and monitoring oversight
Customer Relations Manager:	Complaint handling and communication
Legal Counsel:	Regulatory compliance and risk management

Steering Committee

- Quarterly program effectiveness review meetings
- Annual program updates and improvements
- Regulatory change impact analysis

10.2 Performance Metrics

Operational Metrics

- Customer complaint rates
- Investigation response times
- Service suspension/termination rates
- Regulatory compliance scores

Technical Metrics

- STIR/SHAKEN authentication rates with partners/carriers
- Call blocking effectiveness
- False positive rates
- System availability and performance

11. Continuous Improvement

11.1 Program Review Process

Monthly Reviews

- Operational performance analysis
- Customer feedback evaluation
- Technical system performance
- Regulatory development monitoring

Quarterly Assessments

- Program effectiveness measurement
- Industry best practice comparison
- Technology update evaluation
- Training program assessment

11.2 Update and Enhancement Procedures

Regulatory Change Management

- New regulation impact assessment
- Implementation timeline development
- System and process updates
- Staff training and communication

Technology Improvements

- Monitoring system enhancements

Authentication protocol updates
Analytics capability expansion
Integration optimization

12. Emergency Response

12.1 Incident Response Team

Incident Commander:	Overall response coordination
Technical Lead:	System analysis and resolution
Communications Lead:	Stakeholder notification
Legal Counsel:	Regulatory and legal guidance

12.2 Response Procedures

Immediate Actions (0-1 hour)

- Incident assessment and classification
- Initial containment measures
- Stakeholder notifications
- Investigation team activation

Short-term Actions (1-24 hours)

- Detailed investigation and analysis
- Customer and carrier communications
- Regulatory authority notifications
- Service restoration planning

Long-term Actions (24+ hours)

- Root cause analysis completion
- Preventive measure implementation
- Process improvement identification
- Final reporting and documentation

Conclusion

This Robocall Mitigation Program provides a comprehensive framework for preventing illegal robocalls while maintaining compliance with federal regulations. Regular reviews and updates ensure continued effectiveness and regulatory cohesion.

All program elements must be implemented consistently and documented thoroughly to demonstrate good faith compliance efforts.

Document Control

Version:	1.2
Effective Date:	04/09/2024
Review Date:	06/12/2025
Approved By:	Jake Vinson
Next Review:	04/08/2026

