

Hostcomm LLC Robocall Mitigation Program Description

Dated 14th February 2025

Author: Chris Key

Hostcomm LLC

Robocall Mitigation Program

Description

Executive Summary

1. Network Architecture and Service Provider Integration

1.1 System Architecture Overview

1.2 Upstream Provider Integration

2. Know Your Customer (KYC) Implementation

2.1 Initial Customer Verification Process

2.2 Ongoing Customer Monitoring

3. Analytics and Traffic Monitoring

3.1 Traffic Analysis Systems

3.2 Pattern Detection

4. Mitigation Implementation

4.1 Call Blocking Procedures

4.2 Mitigation Response Procedures

5. Traceback and Law Enforcement Cooperation

5.1 Traceback Response Implementation

5.2 Law Enforcement Cooperation

6. Staff Training and Compliance Program

6.1 Initial Staff Training

6.2 Ongoing Training Program

7. Documentation and Record Keeping

7.1 Call Record Management

7.2 Compliance Documentation

7.3 Traceback and Investigation Records

8. Program Maintenance and Evolution

8.1 Regular Review Process

8.2 Continuous Improvement

9. Additional Policy Implementations

9.1 Contract Enforcement

9.2 Call Blocking Implementation

9.3 Law Enforcement Cooperation

Hostcomm LLC implements this robocall mitigation program in compliance with 47 CFR § 64.6305 and related regulations, using upstream carriers for STIR/SHAKEN authentication.

Executive Summary

This program implements comprehensive measures to prevent illegal robocalls while maintaining compliance with all applicable regulations. Our infrastructure consists of a carrier-grade soft switch and an asterisk-based cloud contact center platform, with connectivity to multiple upstream carriers for STIR/SHAKEN authentication. While our systems include built-in STIR/SHAKEN capabilities, implementation requires both a valid Operating Carrier Number (OCN) for the deployment of cryptographic certificates. Due to the significant investment required for carrier interconnections across multiple providers, and the current OCN mandate, we have opted to rely on our upstream carriers' STIR/SHAKEN authentication services until revenues justify the investment. This approach ensures immediate compliance while avoiding redundant infrastructure investments until regulatory requirements or market conditions change. However if the regulations change Hostcomm is able to implement STIR/SHAKEN through it's equipment, it will not have to replace any components.

These policies apply to all customers and/or prospective customers of Hostcomm LLC and comprise our Robocall Mitigation Plan to avoid originating illegal robocall traffic from our network.

Our multi-layered approach focuses on:

1. Comprehensive customer verification and monitoring
2. Advanced traffic analysis and pattern detection
3. Robust incident response and mitigation procedures
4. Detailed record keeping and compliance documentation

1. Network Architecture and Service Provider Integration

1.1 System Architecture Overview

Our voice service infrastructure integrates multiple components to ensure comprehensive robocall mitigation:

The carrier grade softswitch serves as our core switching platform, providing essential call control and routing capabilities. This system implements robust security measures including access control lists, rate limiting, and comprehensive call detail record (CDR) logging. All outbound traffic is routed through the upstream carrier, which provides STIR/SHAKEN authentication and additional security measures. Hostcomm is likely to add a second and third carrier to increase fault tolerance and load balancing, the carriers will be sourced from the Robocall Mitigation Database and will be fully STIR/SHAKEN compliant.

The asterisk-based cloud contact center platform integrates with our core infrastructure, providing campaign management, call monitoring, and quality assurance capabilities. This integration enables comprehensive oversight of all outbound calling activities while ensuring compliance with regulatory requirements.

System security is maintained through multiple layers:

- Encrypted SIP signaling using TLS
- Protected media streams using SRTP
- Strict access control through IP-based ACLs
- Multi-factor authentication for system access
- Regular security audits and updates
- IP filtering

1.2 Upstream Provider Integration

Our integration with our primary upstream carrier includes:

Call Authentication:

- All outbound calls are routed through Twilio for STIR/SHAKEN authentication
- Authentication levels are assigned based on our customer verification data
- Regular verification of authentication status and call completion rates

Compliance Monitoring:

- Real-time access to call authentication results
- Regular audits of call routing and completion
- Compliance reporting and documentation
- Automated alerts for authentication failures

2. Know Your Customer (KYC) Implementation

2.1 Initial Customer Verification Process

Our comprehensive customer verification process includes multiple steps to ensure proper validation of all customers, as specified in our customer disclosure requirements:

Business Verification:

- Collection and verification of business registration documents
- Physical location verification
- Federal tax I.D. or non-USA government I.D. verification

- State/country of incorporation or business formation documentation
- Cross-reference checks with state and federal databases
- DUNS number verification and business credit checks

Identity Verification:

- Multi-factor authentication of authorized representatives
- Government-issued ID verification
- Background checks for key personnel
- Verification of business ownership and authority
- Disclosure of contact personnel

Service Documentation:

- Detailed service agreements explicitly prohibiting illegal robocalls
- Documentation of intended call volumes and patterns
- Verification of number ownership and authority
- Implementation of customer-specific calling limits
- Clear definition of ASR, LCD, and other traffic statistics requirements
- Disclosure of business practices and nature of services

Additional Foreign Customer Requirements:

- Enhanced verification procedures for non-USA customers
- Additional documentation of traffic sources
- Verification of compliance with all US regulations
- Extra precautions for traffic origination verification

2.2 Ongoing Customer Monitoring

We maintain continuous oversight of customer activities through:

Traffic Analysis:

- Real-time monitoring of calling patterns
- Analysis of call duration and completion rates (ACD, ASR)
- Geographic distribution monitoring
- Detection of unusual pattern changes
- Regular compliance audits

Documentation Maintenance:

- Regular updates of customer information
- Verification of continuing business operations
- Updates to authorized personnel lists
- Review of number utilization and authorization

Risk Assessment:

- Regular evaluation of customer risk profiles
- Analysis of complaint patterns
- Review of authentication results
- Assessment of compliance history

The soft switch used by Hostcomm LLC can be set to monitor the most important call metrics such as ACD and ASR and then act on the alert by notifying the nominated person and automatically suspending the customer object.

3. Analytics and Traffic Monitoring

3.1 Traffic Analysis Systems

Our comprehensive traffic analysis system monitors multiple parameters:

Volume Metrics:

- Calls per second per customer
- Daily/weekly/monthly volume patterns
- Geographic distribution analysis
- Time-of-day pattern monitoring
- Concurrent call monitoring

Quality Metrics:

- Answer seizure ratio analysis
- Average call duration tracking
- Call completion rate monitoring
- Failed call attempt analysis
- Pattern deviation detection

3.2 Pattern Detection

Our system implements sophisticated pattern detection:

Suspicious Activity Detection:

- Sequential number dialing

- Short duration call patterns
- High-volume calling bursts
- Geographic anomalies
- Invalid number calling

Risk Scoring:

- Real-time risk assessment
- Historical pattern comparison
- Customer profile correlation
- Industry pattern matching
- Automated risk alerts

4. Mitigation Implementation

4.1 Call Blocking Procedures

Our system implements multi-layered blocking based on specific triggers:

Volume-Based Triggers:

- Exceeding 10 calls per second per customer initiates automatic review
- Burst patterns exceeding 1000 calls in 5 minutes trigger temporary suspension
- Sustained high-volume patterns outside customer profile trigger investigation
- Geographic anomalies exceeding normal distribution patterns flag for review
- Multiple simultaneous calls to sequential numbers initiate blocking

Pattern-Based Triggers:

- Short duration calls (under 6 seconds) exceeding 30% of total volume
- Answer rates falling below 15% of attempted calls
- Invalid number calling exceeding 2% of attempts
- Off-hour calling patterns outside business specifications
- Unusual geographic distribution patterns

4.2 Mitigation Response Procedures

When triggers are activated, our system implements a tiered response:

Immediate Actions:

- Automatic suspension of calling capability for severe violations
- Real-time notification to customer technical contacts via email
- Logging of incident details and trigger conditions

- Preservation of call detail records for investigation
- Notification to compliance team for review

Investigation Process:

- Analysis of call patterns leading to trigger
- Review of customer history and risk profile
- Evaluation of similar patterns across customer base
- Documentation of findings and recommendations
- Development of corrective action plans

Resolution Steps:

- Customer consultation on findings
- Implementation of corrective measures
- Adjustment of monitoring thresholds if needed
- Documentation of resolution actions
- Follow-up monitoring for pattern recurrence

5. Traceback and Law Enforcement Cooperation

5.1 Traceback Response Implementation

Our traceback response process includes:

Initial Response:

- Immediate acknowledgment of traceback requests
- Assignment to designated response team
- Preliminary data gathering and assessment
- Status update to requesting entity
- Initiation of internal investigation

Data Collection:

- Extraction of relevant call detail records
- Gathering of customer identification information
- Collection of authentication status records
- Compilation of routing information
- Assembly of pattern analysis data

Response Delivery:

- Formatted response package preparation
- Technical analysis summary

- Supporting documentation assembly
- Secure transmission of information within 24 hours
- Follow-up availability confirmation

5.2 Law Enforcement Cooperation

Our cooperation procedures include:

Response Protocol:

- Designated law enforcement liaison
- Secure communication channels
- Expedited response procedures
- Evidence preservation protocols
- Chain of custody documentation

Information Sharing:

- Call record access procedures
- Customer information protocols
- Pattern analysis sharing
- Technical assistance provision
- Ongoing investigation support

6. Staff Training and Compliance Program

6.1 Initial Staff Training

Our comprehensive training program covers:

Technical Training:

- System operation and monitoring
- Traffic analysis interpretation
- Pattern recognition techniques
- Blocking implementation procedures
- Investigation methodologies

Compliance Training:

- Regulatory requirements review
- Documentation procedures
- Customer verification protocols
- Response time requirements

- Evidence preservation methods

6.2 Ongoing Training Program

Regular training updates include:

Quarterly Reviews:

- Regulatory requirement updates
- New pattern recognition training
- System update training
- Procedure modification review
- Best practice updates

Annual Certification:

- Compliance requirement testing
- Technical competency verification
- Protocol adherence assessment
- Documentation accuracy review
- Emergency response drills

7. Documentation and Record Keeping

7.1 Call Record Management

Our record keeping system maintains:

Call Records:

- Complete CDR storage for 18 months
- Detailed routing information
- Authentication status records
- Blocking event documentation
- Pattern analysis reports

Customer Records:

- Verification documentation
- Communication histories
- Compliance reviews
- Incident reports
- Resolution documentation

7.2 Compliance Documentation

We maintain comprehensive compliance records, including:

Policy Documentation:

- Written procedures and policies
- Public website publication of Robocall Mitigation Plan
- Customer notification records
- Regular review documentation
- Update histories and justifications
- Implementation guidelines
- Compliance verification records

Database Registration:

- Verification of wholesale customer registration in Robocall Mitigation Database
- Regular audits of customer registration status
- Documentation of registration compliance

7.3 Traceback and Investigation Records

We maintain detailed records of:

- All traceback requests and responses
- Customer explanations and corrective actions
- Investigation findings and outcomes
- Law enforcement cooperation documentation
- Blocking implementation records

8. Program Maintenance and Evolution

8.1 Regular Review Process

Our program undergoes regular review:

Monthly Reviews:

- Pattern detection effectiveness
- Response time performance
- Blocking accuracy assessment
- Customer compliance verification
- Documentation completeness

Quarterly Assessments:

- System performance evaluation
- Process efficiency analysis
- Resource allocation review
- Training effectiveness assessment
- Technology update planning

8.2 Continuous Improvement

Our improvement process includes:

Performance Monitoring:

- Key metric tracking
- Goal achievement assessment
- Efficiency measurement
- Cost-effectiveness analysis
- Quality assurance reviews

Update Implementation:

- Technology enhancement planning
- Process improvement implementation
- Training program updates
- Documentation revision
- Compliance enhancement

9. Additional Policy Implementations

9.1 Contract Enforcement

- Immediate termination protocol for policy violations
- Forfeiture of confidentiality for illegal traffic cases
- Information sharing procedures with industry partners and law enforcement
- Documentation of enforcement actions

9.2 Call Blocking Implementation

- Maintenance of known illegal robocall source numbers
- Implementation of destination-based blocking
- Regular updates to blocking lists
- Documentation of blocking effectiveness

9.3 Law Enforcement Cooperation

- Designated single point of contact for traceback requests
- Coordination procedures with investigation authorities
- Collaboration with industry traceback groups
- Partnership with FCC and official consortium
- Response protocols for investigation requests

This robocall mitigation program represents our comprehensive approach to preventing illegal robocalls while maintaining compliance with 47 CFR § 64.6305. The program undergoes regular review and updates to ensure continued effectiveness and adaptation to emerging threats and regulatory requirements.