

ROBOCALL MITIGATION PROGRAM

TeleConnx Inc.

Version 2.0 - 2025

Document Control: RMP-2025-001

EXECUTIVE SUMMARY

This Robocall Mitigation Program demonstrates TeleConnx Inc.'s commitment to preventing illegal robocalling on our network in compliance with the TRACED Act, FCC regulations (47 CFR § 64.6305), and industry best practices. This program is filed with the FCC's Robocall Mitigation Database as required by federal regulations.

Company Information:

- Company Name: TeleConnx Inc.
 - Phone: (877) 630-5100
 - Email: Hello@TeleConnx.com
 - Website: www.TeleConnx.com
-

1. PROGRAM OVERVIEW

1.1 Purpose

This comprehensive program outlines TeleConnx Inc.'s policies, procedures, and technical measures to prevent, detect, mitigate, and respond to illegal robocalling activities on our network, ensuring full compliance with all applicable federal regulations.

1.2 Scope

This program applies to:

- All voice services provided by TeleConnx Inc.
- All customers utilizing our network
- All traffic originating from, terminating to, or transiting through our network
- Domestic voice traffic only (no international voice traffic accepted)

1.3 Regulatory Compliance Framework

This program ensures compliance with:

- The TRACED Act (Pallone-Thune Act)
 - 47 CFR § 64.6305 (Robocall Mitigation Database requirements)
 - 47 CFR § 64.6301 et seq. (STIR/SHAKEN implementation)
 - TCPA requirements
 - FCC Orders 20-136, 21-62, and subsequent relevant orders
 - State-specific robocalling regulations
-

2. STIR/SHAKEN IMPLEMENTATION

2.1 Implementation Status

Fully Implemented as of: June 2, 2025

2.2 Authentication Framework

Attestation Levels Supported:

- **Full Attestation (A):** Provided when TeleConnx has a direct authenticated relationship with the customer and full knowledge of the right to use the calling number
- **Partial Attestation (B):** Provided when TeleConnx has a direct authenticated relationship with the customer but cannot fully verify their right to use the calling number

Certificate Management:

- **Certificate Authority:** Iconectiv STI-CA
- **STIR/SHAKEN Service Provider:** Telonium
- **Certificate Repository:** <https://certs.telonium.net/>
- **Certificate Status:** Active and valid

Technical Implementation:

- **Signing Platform:** Telonium STIR/SHAKEN Service
- **Authentication Method:** SIP Identity header insertion
- **Protocol Support:** SHAKEN using ES256 algorithm

Attestation Policy:

- **Full Attestation (A) Criteria:**
 - Direct customer with verified identity
 - Documented ownership of originating numbers
 - Numbers verified through customer documentation
- **Partial Attestation (B) Criteria:**
 - Direct customer with verified identity
 - Customer-provided number authorization
 - Unable to independently verify number ownership

2.3 Implementation Timeline

- Phase 1: IP-based traffic authentication – June 2, 2025
- Phase 2: TDM traffic migration plan – N/A (No TDM traffic – 100% IP-based network)
- Phase 3: Full deployment across all originating traffic – June 2, 2025

2.4 Non-IP Traffic Mitigation

All TDM-to-IP conversions handled by upstream CLEC provider (Bandwidth Inc.)



3. KNOW YOUR CUSTOMER (KYC) PROCEDURES

3.1 Analytics and Monitoring Systems

Third-Party Vendor Disclosure: TeleConnx employs proprietary, in-house real-time monitoring systems for call analytics rather than third-party vendors. Our custom-built monitoring platform provides:

- Immediate email alerts for all failed call attempts
- Real-time Answer Seizure Ratio (ASR) tracking for every customer
- Call Detail Record (CDR) analysis with pattern detection
- Automated threshold monitoring with instant notifications

3.2 Current Customer Base Status

Closed Customer Base Declaration: TeleConnx maintains a closed customer base as of October 2023. We are not currently accepting new customers. All existing customers have established long-term relationships with documented vetting procedures.

3.3 Existing Customer Vetting Documentation

All current customers have been vetted through the following process and maintain active files containing:

Identity Verification Documents (On File)

- **Business Registration:** State incorporation documents or LLC formation papers
- **Federal Tax ID:** EIN verification through IRS documentation
- **State Tax Registration:** Active state tax account verification
- **Business License:** Local business operating permits where applicable

Principal Owner Verification

- **Government-issued ID:** Driver's license or passport of primary account holder
- **Proof of Authority:** Corporate resolution or operating agreement showing signatory authority
- **Background Verification:** Public records search for telecommunications-related violations

Physical Presence Verification

- **Business Address:** Verified through:
 - Utility bills in company name (electric, gas, or water)
 - Lease agreement or property ownership records
 - Google Street View verification of business signage
 - On-site photographs for certain customer categories
- **No P.O. Box Policy:** All customers must maintain verifiable physical addresses

Business Legitimacy Verification

- **Operational History:**
 - Length of time in business: Minimum 12 months required
 - Previous telecommunications service references
 - Banking relationship verification (redacted bank statements)
- **Online Presence Review:**
 - Active business website matching services offered
 - Consistent business listings across directories
 - Social media presence where applicable
 - Domain registration history
- **Better Business Bureau:** Checked for complaints and ratings
- **State Database Checks:**
 - Secretary of State active/good standing status
 - No telecommunications-related violations
 - No consumer protection violations

3.4 Enhanced Due Diligence for Existing Customers

Given our closed customer base, we maintain heightened ongoing monitoring:

Annual Re-Verification Process

Every 12 months, we require:

1. **Updated Business Documentation:**
 - Current Secretary of State good standing certificate
 - Updated business license
 - Renewed insurance certificates where applicable
2. **Attestation Requirements:**
 - Written certification of TCPA compliance
 - Do-Not-Call Registry compliance attestation
 - Confirmation of business model (no changes to call types)
 - Updated authorized user list
3. **Financial Verification:**
 - Current credit check through business credit bureau
 - Payment history review (must maintain current status)
 - No bankruptcies or significant judgments

Quarterly Reviews

- **Traffic Pattern Analysis:** Compare current calling patterns to established baseline
- **Complaint Review:** Check FCC, BBB, and state databases for complaints
- **Volume Assessment:** Ensure volumes match stated business purpose
- **Destination Analysis:** Flag new countries or unusual geographic patterns

Monthly Monitoring

- **ASR Tracking:** Document Answer Seizure Ratios for trend analysis
- **Failure Rate Analysis:** Review "not in service" and "invalid number" rates
- **Time-of-Day Patterns:** Ensure calling remains within TCPA hours
- **Caller ID Consistency:** Verify consistent legitimate number presentation

3.5 Customer Risk Scoring System

Each customer is assigned a risk score based on:

Low Risk (Score 1-3)

- Established business (5+ years)
- Consistent traffic patterns
- ASR above 30%
- No complaints or violations
- Local/regional calling only

Medium Risk (Score 4-6)

- Business 2-5 years old
- Some variation in traffic patterns
- ASR between 15-30%
- Minor historical issues (resolved)
- National calling patterns

High Risk (Score 7-10)

- Business under 2 years old
- Significant pattern variations
- ASR below 15%
- Previous warnings or violations
- International or high-risk destinations

Enhanced Monitoring by Risk Level:

- **Low Risk:** Standard monthly reviews
- **Medium Risk:** Bi-weekly reviews with automated alerts
- **High Risk:** Daily monitoring with hair-trigger thresholds

3.6 Prohibited Customer Activities

Regardless of customer history, the following result in immediate investigation:

- Robocalling or automated dialing without proper consent
- Caller ID spoofing or number rotation schemes
- Lead generation without verified end-user consent
- Debt collection without compliance documentation
- Political calling without required disclosures
- Charity solicitation without registration
- Survey calls that transition to sales
- Any traffic to known Do-Not-Call numbers

3.7 Customer Documentation Requirements

Required Agreements (All on File)

- **Master Service Agreement** with specific anti-robocalling provisions
- **Acceptable Use Policy** acknowledgment (renewed annually)
- **TCPA Compliance Addendum** with indemnification clause
- **Caller ID Authentication Agreement** for accurate number display
- **Traceback Cooperation Agreement** for investigation assistance

Campaign-Specific Requirements

For any calling campaigns, customers must provide:

- Sample of consent records (if applicable)
- Script approval for compliance review
- Target list sources and verification
- Do-Not-Call scrubbing evidence
- Campaign duration and volume estimates

3.8 Customer Onboarding (Historical - For Reference)

Although we maintain a closed customer base, our vetting process for existing customers included:

Initial Vetting Steps

1. **Application Review** (5 business days)
 - Completeness check
 - Initial risk assessment
 - Reference verification
2. **Document Collection** (10 business days)
 - All documents listed in Section 3.3
 - Legal review of agreements
 - Compliance team approval
3. **Test Period** (30 days)
 - Limited volume approval
 - Daily monitoring
 - Pattern establishment
4. **Full Activation**
 - Executive approval required
 - Baseline metrics established
 - Regular monitoring commenced

3.9 Record Retention

Customer Records Maintained Include:

- Original vetting documentation: Permanent retention
- Annual re-verification records: 5 years
- Monitoring reports: 24 months minimum
- Violation/investigation records: Permanent retention
- Communication logs: 24 months
- CDRs related to investigations: 24 months

3.10 Future Customer Acceptance Policy

Should TeleConnx reopen customer acquisition, additional requirements will include:

- **Enhanced Vetting:**
 - Third-party background check service
 - Telecom industry reference requirements
 - Minimum 24-month business history
 - Performance bond for first 6 months
- **Probationary Period:**
 - 90-day initial monitoring period
 - Daily traffic review
 - Volume restrictions
 - Prepayment required

3.11 KYC Program Governance

Responsible Parties:

- **Chief Compliance Officer:** Overall KYC program oversight
- **Operations Manager:** Daily monitoring and alerts
- **Customer Success Manager:** Customer communication and documentation
- **Executive Team:** Risk scoring and major decisions

Review Schedule:

- **Weekly:** High-risk customer review
 - **Monthly:** All customer scorecard updates
 - **Quarterly:** Program effectiveness assessment
 - **Annually:** Complete customer re-verification
-

4. CALL MONITORING AND ANALYTICS

4.1 Zero-Tolerance Monitoring System

Real-Time Call Failure Monitoring

TeleConnx employs immediate email alerting for ALL failed call attempts, providing instant visibility into potential robocalling activity.

Monitored Failure Codes:

- SIP 404 (Not Found) - Number not assigned
- SIP 480 (Temporarily Unavailable) - Not in service
- SIP 484 (Address Incomplete) - Invalid number format
- SIP 603 (Decline) - Number on Do-Not-Call or blocking service
- Any non-standard termination responses

Alert Response Timeline:

- **0-1 minute:** Automated email alert generated
- **Within 15 minutes:** Initial pattern review
- **Within 1 hour:** Customer contacted if failure rate exceeds normal thresholds
- **Within 4 hours:** Full investigation completed and documented

Why This Detects Robocalling:

- Legitimate callers typically have <5% failure rates
- Robocallers using purchased/scraped lists show 20-50%+ failure rates
- "Number not assigned" patterns indicate outdated or fabricated number lists
- Immediate detection prevents continuation of problematic campaigns

Answer Seizure Ratio (ASR) Monitoring

- **Continuous Tracking:** ASR calculated for every customer in real-time
- **Baseline Establishment:** Normal ASR patterns established per customer
- **Alert Thresholds:**
 - ASR below 1%: Immediate investigation and possible suspension
 - ASR below 5%: Enhanced monitoring triggered
 - ASR 20% below customer baseline: Customer notification required

Volume and Pattern Monitoring

- **Call Volume Thresholds:**
 - Burst detection: >100 calls/minute triggers review
 - Daily limits: Customer-specific based on established business model
 - Sudden increases: >200% of baseline triggers immediate review
- **Duration Analysis:**
 - Short duration threshold: <6 seconds
 - High percentage (>10%) of short calls triggers investigation
 - Consistent 1-2 second calls indicate possible robocalling
- **Time-of-Day Monitoring:**
 - Calls outside TCPA hours (before 8 AM or after 9 PM local time)
 - Unusual patterns for customer's business type
 - Night/weekend spikes inconsistent with legitimate business

4.2 Analytics Platform and Pattern Detection

Data-Driven Analysis

Rather than machine learning, TeleConnx employs deterministic, rule-based analytics that provide clear, auditable detection criteria:

- **Historical Baseline Comparison**
 - 30-day rolling average calculations per customer
 - Day-of-week pattern analysis
 - Seasonal adjustment factors
 - Clear deviation thresholds trigger alerts
- **Cross-Customer Pattern Detection**
 - Identify similar failure patterns across multiple customers
 - Detect number rotation schemes
 - Flag shared upstream sources of problematic traffic
- **Industry Threat Intelligence Integration**
 - Daily updates from Industry Traceback Group
 - FCC consumer complaint database correlation
 - Known bad actor number ranges
 - Confirmed robocaller tactics and patterns

Alert Priority Matrix

Critical Priority (Immediate Response Required):

- Traceback request received
- ASR drops below 1%
- Confirmed invalid caller ID presentation
- Law enforcement or regulatory contact

High Priority (Response within 1 hour):

- Failed call rate >50%
- Multiple "number not assigned" to same NPA-NXX
- Time-of-day violations (TCPA hours)
- Sudden traffic to new geographic area

Medium Priority (Response within 4 hours):

- ASR below 5% but above 1%
- Volume spike >200% of baseline
- Duration patterns suggesting robocalling
- Customer complaint received

Standard Priority (Response within 24 hours):

- Gradual volume increases requiring baseline adjustment
- New destination country detected
- ASR trending downward but still acceptable

4.3 Alert Response Protocol

1. Immediate Actions (0-5 minutes):

- Automated email/SMS alert to monitoring team
- Call traffic can be suspended within 30 seconds if critical
- Automatic CDR preservation initiated

2. Initial Investigation (5-60 minutes):

- Review specific failure patterns
- Check customer's recent history
- Determine if suspension warranted
- Contact customer if patterns indicate violations

3. Full Investigation (1-4 hours):

- Complete CDR analysis
- Document all findings
- Determine root cause
- Implement corrective actions

4. Follow-up Actions (4-24 hours):

- Customer remediation plan if required
 - Update monitoring thresholds if needed
 - Report to authorities if illegal activity confirmed
 - Document lessons learned
-

5. UPSTREAM AND DOWNSTREAM PROVIDER MANAGEMENT

5.1 Downstream Carrier Partners

TeleConnx delivers traffic to the following major carriers:

- **Bandwidth Inc.**
 - Service Type: Outbound traffic termination
 - Relationship: Primary carrier partner
- **BulkVS**
 - Service Type: Inbound traffic handling
 - Relationship: Secondary carrier partner

These carriers verify TeleConnx's RMD certification status as part of their own compliance obligations.

5.2 Customer Verification Requirements

As TeleConnx maintains a closed customer base and passes traffic on behalf of our direct customers, our focus is on:

- **Customer Compliance:** Ensuring our direct customers comply with our robocall mitigation requirements
- **Traffic Monitoring:** Real-time monitoring of all customer traffic patterns
- **Enforcement:** Swift action on any violations detected

5.3 Robocall Mitigation Database (RMD) Compliance

- TeleConnx maintains current certification in the FCC's RMD
 - Our certification is available for verification by carrier partners
 - We update our RMD filing annually or when material changes occur
-

6. CUSTOMER COMPLIANCE MANAGEMENT

6.1 Ongoing Customer Monitoring

Daily Monitoring

- Call completion ratios
- Short duration call percentages
- Geographic calling patterns
- Time-of-day distributions

Weekly Reviews

- Complaint analysis
- Traceback request correlation
- Volume trend analysis
- Number rotation patterns

Monthly Assessments

- Comprehensive traffic analysis
- Compliance scorecard update
- Customer communication review
- Risk rating adjustment

6.2 Terms of Service Enforcement

Progressive Enforcement Protocol

1. First Incident

- Immediate notification to customer
- Investigation initiated within 1 hour
- Remediation plan required within 24 hours
- Enhanced monitoring for 30 days

2. Second Incident

- Written warning with cure period (48 hours)
- Service restrictions imposed
- Executive-level attestation required
- Enhanced monitoring for 90 days

3. Third Incident

- Immediate service suspension
- Comprehensive audit required
- Remediation plan with third-party verification
- Board-level review for service restoration

4. Continuing Violations

- Permanent service termination
- Reporting to relevant authorities
- Industry database notification

6.3 Do-Not-Call Registry Compliance

- Daily DNC list synchronization required
- Customer must demonstrate scrubbing processes
- Random audits of calling lists
- Immediate suspension for confirmed DNC violations

6.4 TCPA Compliance Requirements

- Written consent documentation requirements
 - Opt-out mechanism verification
 - Time-of-day calling restrictions enforcement
 - Caller ID accuracy requirements
-

7. TRACEBACK RESPONSE PROCEDURE

7.1 Designated Contacts

Primary Contact:

- Name: Mr. W. Peter Howell
- Email: w.peter.howell@teleconnx.com
- Phone: +1 (719) 789-0799
- Availability: 24/7

Secondary Contact:

- Name: Mr. Marko Ratko
- Email: marko.ratko@teleconnx.com
- Phone: +381 60 7179424
- Availability: 24/7

7.2 Response Timeline Commitment

- **Initial Acknowledgment:** Within 2 hours
- **Preliminary Information:** Within 4 hours
- **Complete Response:** Within 24 hours
- **Follow-up Actions:** Within 48 hours

7.3 Traceback Response Protocol

1. Acknowledge receipt with ticket number
2. Immediately preserve all relevant records
3. Suspend customer if patterns indicate violation
4. Gather comprehensive call detail records
5. Review customer's compliance history
6. Identify upstream/downstream providers
7. Prepare response using Industry Traceback Group template
8. Document all findings and actions taken
9. Implement preventive measures
10. Follow up with ITG on outcomes

7.4 Information Provided in Traceback Response

- Complete CDR for identified calls
 - Customer identification and contact information
 - Upstream provider details if applicable
 - Actions taken (suspension, termination, etc.)
 - Historical compliance issues if any
 - Preventive measures implemented
-



8. COOPERATION WITH LAW ENFORCEMENT

8.1 Law Enforcement Response Procedures

- Designated law enforcement liaison appointed
- 24/7 response capability for urgent requests
- Subpoena and warrant compliance process
- Evidence preservation protocols

8.2 Proactive Reporting

We proactively report to appropriate authorities:

- Confirmed illegal robocalling operations
- Suspected TCPA violations
- Fraudulent calling campaigns
- Technical Caller ID spoofing

8.3 Evidence Preservation

- Automatic 90-day preservation upon violation detection
- Extended preservation upon law enforcement request
- Chain of custody procedures
- Secure evidence storage protocols

8.4 Regulatory Cooperation

- FCC enforcement bureau cooperation
 - FTC Do-Not-Call Registry enforcement support
 - State attorney general office collaboration
 - Industry working group participation
-

9. INTERNATIONAL TRAFFIC MANAGEMENT

9.1 International Traffic Policy

No International Voice Traffic:

- TeleConnx does not accept or handle any international voice traffic
- All voice services are restricted to US domestic traffic only
- No international customers for voice services
- No origination or termination of calls from outside the United States

9.2 Service Restrictions

Voice Services - US Only:

- All voice traffic must originate within the United States
- All voice traffic must terminate within the United States
- Automatic rejection of any international call attempts
- No international gateway services provided

Non-Voice Services:

- Canadian customer utilizes hosted PBX services only (no voice traffic)
- PBX hosting does not involve call origination or termination through TeleConnx network

9.3 Enforcement and Monitoring

Blocking Measures:

- Network-level blocking of all international origination attempts
- Automatic rejection of international country codes
- Real-time alerts for any attempted international traffic
- Immediate investigation of any international call attempts

Compliance Benefits:

- Eliminates risk of international robocall origination
- Removes exposure to high-risk international jurisdictions
- Simplifies STIR/SHAKEN implementation (US-only traffic)
- Reduces regulatory complexity

10. REMEDIATION MEASURES

10.1 Customer Remediation Requirements

Before service restoration after suspension:

1. **Root Cause Analysis**
 - Detailed investigation report
 - Identification of failure points
 - Timeline of violations
2. **Corrective Action Plan**
 - Specific technical measures implemented
 - Process improvements documented
 - Staff training completed
 - Third-party audit if required
3. **Compliance Attestation**
 - C-level executive attestation
 - Legal counsel review
 - Compliance officer certification
 - Board resolution if repeat offender
4. **Enhanced Monitoring Agreement**
 - Accept increased surveillance
 - Lower thresholds for future violations
 - Performance bond if required
 - Monthly compliance reporting

10.2 Network Remediation

- Implement additional filtering rules
 - Enhance analytics algorithms
 - Update threat intelligence databases
 - Strengthen authentication requirements
-

11. STAFF TRAINING AND AWARENESS

11.1 Training Program Components

- Initial robocall mitigation training for all staff
- Role-specific advanced training
- Annual refresher courses
- Updates on new regulations and threats

11.2 Training Topics

- TRACED Act requirements
- STIR/SHAKEN protocols
- Traceback procedures
- Customer vetting processes
- Monitoring system operation
- Escalation procedures
- Documentation requirements

11.3 Training Documentation

- Individual training records maintained
- Certification tracking system
- Performance assessments
- Continuous improvement feedback

11.4 Awareness Initiatives

- Monthly threat intelligence briefings
 - Industry conference participation
 - Regulatory update newsletters
 - Best practices sharing sessions
-

12. RECORD KEEPING AND REPORTING

12.1 Required Documentation

Retention Period: Minimum 24 months

- All traceback requests and responses
- Customer investigations and outcomes
- Call detail records for flagged traffic
- Compliance violations and remediation
- Training records and certifications
- Provider verification documentation
- Law enforcement interactions
- Regulatory filings and correspondence

12.2 Record Format and Security

- Electronic storage with encryption
- Automated backup procedures
- Access controls and audit logs
- Readily retrievable format
- Secure disposal procedures

12.3 Regulatory Reporting

- Annual RMD certification update
- Quarterly compliance reports (internal)
- Incident reports as required
- Response to FCC data requests

12.4 Performance Metrics Dashboard

- Real-time monitoring statistics
 - Traceback response times
 - Customer compliance scores
 - Provider performance ratings
 - Training completion rates
 - Incident resolution metrics
-

13. PROGRAM GOVERNANCE AND REVIEW

13.1 Governance Structure

- **Executive Sponsor:** CEO/President
- **Program Owner:** Chief Compliance Officer
- **Day-to-Day Management:** Network Operations Manager
- **Review Committee:** Quarterly executive review

13.2 Regular Review Schedule

- **Daily:** Traffic pattern analysis
- **Weekly:** Customer compliance review
- **Monthly:** Program effectiveness assessment
- **Quarterly:** Provider verification, Executive review
- **Annually:** Comprehensive program audit, Regulatory update incorporation

13.3 Update Procedure

1. Monitor regulatory changes and industry best practices
2. Assess program effectiveness metrics
3. Incorporate lessons learned from incidents
4. Update documentation and procedures
5. Communicate changes to all stakeholders
6. Conduct training on updates
7. File updated program with RMD as required

13.4 Continuous Improvement Process

- Regular benchmarking against industry standards
 - Participation in industry working groups
 - Technology investment in detection capabilities
 - Feedback incorporation from all stakeholders
-

14. TECHNOLOGY AND TOOLS

14.1 Current Technology Stack

All Systems Developed and Maintained In-House

- **Call Analytics Platform:** Custom-built proprietary analytics system
 - Real-time pattern analysis for unusual calling behaviors
 - Baseline establishment and deviation detection per customer
 - Automated threshold monitoring with configurable alerts
 - No reliance on third-party analytics services
- **STIR/SHAKEN Implementation:**
 - **Signing Platform:** Asterisk with STIR/SHAKEN module
 - **Certificate Management:** Telonium service integration
 - **Authentication:** Native Asterisk SIP identity header handling
- **CDR Storage and Analysis:**
 - **Database:** MySQL
 - **Custom Analysis Tools:** Proprietary SQL queries and scripts
 - **Real-time Processing:** Automated analysis of CDR data
 - **Alert Generation:** Custom email alerting based on SQL triggers
- **Monitoring and Alerting:**
 - **Custom Monitoring Scripts:** Proprietary pattern detection algorithms
 - **Email Alert System:** Automated notifications for all failure conditions
 - **Real-time Dashboard:** Internal monitoring displays
 - **ASR Calculation:** Custom queries against MySQL CDR database
- **Customer Portal:** Not applicable - Direct customer communication model

Key Advantages of Custom Platform:

- Complete control over detection algorithms
- Immediate customization capability for new threat patterns
- No dependency on third-party vendor limitations
- Full audit trail and transparency of all detection logic
- Cost-effective solution tailored to specific needs

14.2 Planned Enhancements

- Additional pattern detection algorithms based on emerging threats
 - Enhanced SQL query optimization for faster analysis
 - Expanded automated response capabilities
 - Integration with Industry Traceback Group APIs when available
-



15. COMPLIANCE ATTESTATION

This Robocall Mitigation Program is hereby certified as accurate and complete, representing TeleConnx Inc.'s commitment to preventing illegal robocalling on our network.

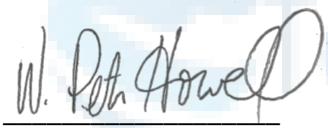
Attestation:

By signing below, I attest that:

1. This program is fully implemented and operational
2. All statements herein are true and accurate
3. TeleConnx Inc. is committed to full regulatory compliance
4. This program will be updated as regulations evolve

Chief Executive Officer

Name: William P Howell

Signature: 

Date: 09/15/2025

APPENDICES

Appendix A: Definitions and Acronyms

- **ASR:** Answer Seizure Ratio
- **CDR:** Call Detail Record
- **ITG:** Industry Traceback Group
- **KYC:** Know Your Customer
- **RMD:** Robocall Mitigation Database
- **SHAKEN:** Signature-based Handling of Asserted Information Using toKENS
- **STIR:** Secure Telephone Identity Revisited
- **TCPA:** Telephone Consumer Protection Act
- **TRACED Act:** Telephone Robocall Abuse Criminal Enforcement and Deterrence Act

Appendix B: Contact Information

- **FCC Robocall Response Team:** robocall@fcc.gov
- **Industry Traceback Group:** traceback@ustelecom.org
- **Internal Escalation:** compliance@teleconnx.com



Appendix C: Reference Documents

- FCC Report and Order 20-136
- FCC Second Report and Order 21-62
- 47 CFR Part 64, Subpart HH
- Industry Traceback Group Policies and Procedures
- ATIS STIR/SHAKEN Standards

Appendix D: Forms and Templates

- Traceback Response Template
- Customer Violation Notice Template
- Remediation Plan Template
- Compliance Attestation Form

Document Control:

- Version: 2.0
- Effective Date: 09/15/2025
- Review Date: 12/15/2025
- Owner: Compliance Department
- Distribution: FCC, Internal Use, RMD Filing

This document is proprietary and confidential. It is filed with the FCC's Robocall Mitigation Database as required by federal regulations.

