

Robocall Mitigation Plan (RMP)

Company Name: CONNECTWEBX

1. Introduction

CONNECTWEBX is committed to full compliance with the Federal Communications Commission (FCC) regulations regarding robocall mitigation and caller ID authentication. This Robocall Mitigation Plan outlines the procedures, policies, and technologies implemented to prevent illegal robocalls and ensure network integrity. This plan is prepared in accordance with the latest FCC Robocall Mitigation Database (RMD) rules effective February 5, 2026, including all recent updates and enforcement requirements.

2. Regulatory Compliance Overview (2026 Updates)

CONNECTWEBX acknowledges and complies with the latest FCC requirements:
Key 2026 Updates Included in this Plan

- Mandatory update of RMD information within 10 days of any change
- Annual RMD recertification required (deadline: March 1 each year)
- Increased penalties:
 - o \$10,000 per violation for false/inaccurate filings
 - o \$1,000 per violation for failure to update data timely
- Mandatory accuracy and completeness of all RMD submissions
- Potential removal from RMD for non-compliance (leading to traffic blocking)
- Multi-factor authentication (MFA) required for RMD portal access
- Providers must block traffic from entities not listed in RMD CONNECTWEBX maintains strict internal controls to comply with all above obligations.

3. STIR/SHAKEN Implementation Status Fully Implemented

CONNECTWEBX has implemented the STIR/SHAKEN framework and:

- Uses its own SPC token and certificate
- Signs outbound calls with appropriate attestation levels
- Maintains compliance with FCC authentication standards

4. Robocall Mitigation Program

CONNECTWEBX has implemented the following mitigation measures:

4.1 Know Your Customer (KYC) Procedures

- Verification of customer identity (business registration, ID, address)
- Screening against fraud databases and blacklists
- Risk profiling before service activation

4.2 Traffic Monitoring & Analytics

- Continuous monitoring of call patterns (volume, frequency, destinations)
 - Detection of suspicious traffic spikes or abnormal behavior
 - Automated flagging and investigation of high-risk accounts
- #### **4.3 Call Blocking & Filtering**
- Blocking of:
 - o Invalid, spoofed, or malformed caller IDs
 - o Known scam or illegal robocall sources
 - Use of industry traceback data and third-party analytics tools

4.3 Traceback Cooperation

CONNECTWEBX

- Responds to traceback requests within 24 hours
- Cooperates with industry traceback groups and regulators
- Maintains logs for investigation and enforcement

4.4 Enforcement Actions If suspicious or illegal activity is detected:

- Immediate suspension of customer accounts
- Investigation and documentation
- Permanent termination for confirmed violations

5. Network Safeguards

CONNECTWEBX ensures:

- Secure SIP signaling and authentication
- Prevention of unauthorized access or traffic injection
- Rate limiting and fraud detection systems

6. Data Accuracy & RMD Maintenance

CONNECTWEBX maintains strict compliance with FCC database requirements:

- All RMD information is accurate, complete, and current
- Updates are made within 10 business days of any change
- Internal compliance team reviews data regularly Annual recertification to be done timely.

7. Internal Compliance Governance

CONNECTWEBX has established:

- A designated Compliance Officer
- Regular compliance audits
- Staff training on robocall regulations
- Documentation of all mitigation processes

8. Record keeping & Documentation

CONNECTWEBX maintains:

- Customer verification records
- Call detail records (CDRs)
- Traffic monitoring logs
- Incident and enforcement reports. All records are retained per regulatory requirements and made available upon request.

9. Third-Party Relationships If applicable,

CONNECTWEBX:

- Ensures all partners comply with FCC rules
- Maintains written agreements for call authentication

10. Certification Statement

CONNECTWEBX certifies that:

- It has implemented a robocall mitigation program compliant with FCC rules
- All information submitted to the Robocall Mitigation Database is true, accurate, and complete
- It will update its filing within the required timeframe and comply with annual recertification obligations

11. Contact Information

Company Name: CONNECTWEBX

Contact Person: Heather Stockman

Title: C E O

Email:

heather@connectwebx.com

Phone: 3126670029

12. Conclusion

CONNECTWEBX is committed to preventing illegal robocalls and maintaining full compliance with evolving FCC regulations. This plan reflects the latest 2026 requirements and will be continuously updated to meet regulatory changes.