

ROBOCALL MITIGATION PLAN

[YOUR COMPANY NAME]

FCC Registration Number (FRN): [YOUR FRN NUMBER]

Effective Date: April 21, 2026

1. Company Information

Company Name: [YOUR COMPANY NAME]

FCC Registration Number (FRN): [YOUR FRN NUMBER]

Role: Mobile Virtual Network Operator (MVNO)

Network Provider: AireSpring

Service Type: IoT/M2M (Machine-to-Machine) Services

Contact for Robocall Mitigation Compliance:

Name: [COMPLIANCE CONTACT NAME]

Title: [TITLE]

Email: [EMAIL ADDRESS]

Phone: [PHONE NUMBER]

2. Nature of Service & Traffic Characterization

[YOUR COMPANY NAME] is a Mobile Virtual Network Operator providing IoT and Machine-to-Machine (M2M) communications services. Our network traffic consists exclusively of automated, device-to-device communications for purposes including but not limited to:

- Remote device monitoring and telemetry
- Industrial automation and control systems
- Fleet tracking and asset management
- Smart utility metering
- Connected device management

As an IoT/M2M provider, our traffic is generated by registered, authenticated devices and does not involve human-initiated telephone calls in the traditional sense. Our traffic profile significantly reduces the risk of robocall-type abuse compared to traditional voice carriers.

3. STIR/SHAKEN Compliance

As an IoT/M2M MVNO that does not originate traditional voice calls, the STIR/SHAKEN authentication framework may not be technically applicable to our traffic type. However, we commit to the following:

- We will monitor FCC guidance on STIR/SHAKEN applicability to IoT/M2M traffic and implement signing/attestation requirements as they become applicable.
- To the extent our network passes any voice traffic, we will work with our underlying carrier (AireSpring) to ensure such traffic is appropriately authenticated.
- We will implement STIR/SHAKEN capabilities upon FCC mandate or as technically feasible.

4. Robocall Mitigation Measures

Because we cannot fully implement STIR/SHAKEN at this time (due to the IoT/M2M nature of our service), we are implementing the following reasonable robocall mitigation practices as required by the FCC:

4.1 Customer Onboarding & Know Your Customer (KYC)

- All customers and device accounts must execute a service agreement that prohibits use of our network for illegal robocalling or unlawful autodialers.
- We conduct identity verification for all new customers prior to service activation.
- Customer and device registration information is maintained and available for law enforcement and FCC inquiry.

4.2 Acceptable Use Policy (AUP) Enforcement

- Our Terms of Service and Acceptable Use Policy expressly prohibit use of our network for illegal robocalling, spoofing, or any violation of the Telephone Consumer Protection Act (TCPA).
- Violations of the AUP are grounds for immediate service suspension and termination.

4.3 Traffic Monitoring

- We will implement monitoring procedures to identify unusual traffic patterns that may indicate misuse of our IoT/M2M network for voice or robocall abuse.
- Anomalous traffic events will be investigated and, where warranted, referred to law enforcement.

4.4 Traceback Cooperation

- We commit to responding to all traceback requests from the USTelecom Industry Traceback Group (ITG) within the timeframes required by FCC rules.
- We will cooperate fully with law enforcement and the FCC in any investigation of illegal robocalling originating from our network.

4.5 Upstream & Downstream Obligations

- We will not accept traffic from any provider that is not registered in the FCC Robocall Mitigation Database.
- We will require downstream customers and resellers to maintain their own robocall mitigation obligations.

5. Point of Contact for Law Enforcement & FCC

The following individual is designated as the point of contact for all law enforcement and FCC inquiries relating to robocall mitigation:

Name: [COMPLIANCE CONTACT NAME]

Title: [TITLE]

Email: [EMAIL ADDRESS]

Phone: [PHONE NUMBER]

Mailing Address: [COMPANY ADDRESS]

This contact will respond to traceback requests, law enforcement inquiries, and FCC investigation requests within the timeframes required by applicable rules.

6. Recordkeeping

[YOUR COMPANY NAME] will maintain records sufficient to demonstrate compliance with this Robocall Mitigation Plan, including:

- Customer contracts and identity verification records
- Device registration and authentication logs
- Traffic monitoring reports and anomaly investigations
- Traceback requests and responses
- Any complaints received regarding robocall or illegal calling activity

Records will be retained for a minimum of two (2) years and made available to the FCC or law enforcement upon lawful request.

7. Plan Review & Updates

This Robocall Mitigation Plan will be reviewed at least annually and updated as necessary to reflect:

- Changes in our service offerings or traffic profile
- New or updated FCC rules and guidance
- Technological developments in call authentication
- Lessons learned from traceback or enforcement actions

Any material changes to this plan will be reflected in an updated filing in the FCC Robocall Mitigation Database.

8. Certification

I, the undersigned, am an authorized representative of [YOUR COMPANY NAME] and hereby certify that the information provided in this Robocall Mitigation Plan is true and accurate to the best of my knowledge, information, and belief. I further certify that [YOUR COMPANY NAME] is committed to complying with all applicable FCC rules regarding robocall mitigation.

Signature: _____

Printed Name: _____

Title: _____

Date: _____

Company: [YOUR COMPANY NAME]

FRN: [YOUR FRN NUMBER]