

ROBOCALL MITIGATION PLAN

Pursuant to 47 CFR § 64.6305
and the TRACED Act of 2019

Provider Name:	Bluespan Wireless LLC (d/b/a Bluespan)
Document Date:	February 26, 2026
Version:	2.0
Classification:	Voice Service Provider
STIR/SHAKEN Status:	Non-Implementation

Prepared for filing in the FCC Robocall Mitigation Database (RMD)

This document contains confidential business information.

I. Introduction and Provider Overview

This Robocall Mitigation Plan (“RMP” or “Plan”) is established by Bluespan Wireless LLC, doing business as Bluespan (“Provider” or “Company”), in accordance with the requirements set forth by the Federal Communications Commission (“FCC”) under 47 CFR § 64.6305, the Telephone Robocall Abuse Criminal Enforcement and Deterrence Act of 2019 (TRACED Act), and all subsequent FCC orders, public notices, and guidance pertaining to robocall mitigation obligations, including the January 2024 expanded filing requirements, the January 2025 Report and Order establishing enhanced RMD filing requirements, and the November 2024 Eighth Report and Order addressing third-party STIR/SHAKEN authentication.

This Plan documents the specific, reasonable steps the Provider has taken and continues to take to avoid originating illegal robocall traffic on its network, and supersedes all prior versions of the Provider’s Robocall Mitigation Plan.

Provider Description

Bluespan Wireless LLC, doing business as Bluespan, is a Wireless Internet Service Provider (WISP) operating in rural Arizona. In addition to broadband internet access services, the Provider offers voice services to its customer base. Voice services are delivered via locally-managed Private Branch Exchange (PBX) systems interconnected to the Public Switched Telephone Network (PSTN) through upstream wholesale voice providers. The Provider utilizes two upstream wholesale carriers: Voyant Communications, LLC (d/b/a Vitelity) and VoIP Innovations, LLC.

The Provider resells voice services for consumption by end users — primarily small businesses and residential customers within the Provider’s broadband service area. The Provider does not operate as an intermediate provider, gateway provider, or wholesale originating carrier. The Provider does not originate traffic on behalf of other voice service providers or resellers.

II. STIR/SHAKEN Implementation Status

As certified in the FCC’s Robocall Mitigation Database, the Provider has not implemented the STIR/SHAKEN authentication framework on any portion of its network.

Basis for Non-Implementation

Pursuant to 47 CFR § 64.6305(d)(2)(i), the Provider lacks control over the network infrastructure necessary to implement STIR/SHAKEN. Specifically:

- The Provider does not own or operate PSTN switching infrastructure, Session Border Controllers (SBCs) with STIR/SHAKEN signing capability, or direct interconnections to other carriers.
- All outbound calls originated by the Provider’s end users traverse the Provider’s PBX(s) and are delivered to the PSTN via SIP trunks provided by the Provider’s upstream wholesale carriers: Voyant Communications, LLC (d/b/a Vitelity) and VoIP Innovations, LLC.
- The upstream wholesale carriers control the network infrastructure at the point of PSTN origination and are responsible for STIR/SHAKEN call authentication and attestation for traffic they originate onto the public network on the Provider’s behalf.

- The Provider does not have the ability to obtain an SPC token, generate a STIR/SHAKEN certificate, or perform call signing at any point in its call path.

The FCC has confirmed that the STIR/SHAKEN implementation requirement does not apply to providers that lack control of the network infrastructure necessary to implement the framework, and that in the context of a wholesale provider originating calls for a reseller, it is the wholesale provider that bears the STIR/SHAKEN implementation obligation (FCC 24-120, Eighth Report and Order, ¶ 14 n.64).

Notwithstanding this exemption from STIR/SHAKEN implementation, the Provider maintains this comprehensive robocall mitigation program as required by 47 CFR § 64.6305(a).

III. Know Your Customer (KYC) Program

Pursuant to 47 CFR § 64.1200(n)(4), the Provider maintains a Know Your Customer program as an affirmative, effective measure to prevent customers from originating illegal robocalls. The Provider does not offer voice service signup through its website, any self-service portal, or any other automated provisioning method. Voice services are offered exclusively to the Provider's existing broadband internet access subscribers and are provisioned only through direct interaction with the Provider's staff. This approach eliminates the risk of anonymous or fraudulent voice service enrollment and ensures that every voice customer is a known, verified entity. The Provider's KYC procedures include the following:

A. Customer Onboarding and Identity Verification

1. Voice services are offered exclusively to the Provider's existing broadband internet access customers. All voice customers have been previously verified through the Provider's broadband customer onboarding process, which collects and verifies the customer's full legal name (or business name and authorized representative), physical service address within the Provider's wireless service territory, mailing address, and primary contact telephone number and email address.
2. For business customers, the Provider verifies the existence and legitimacy of the business through state business registration records, publicly available business listing databases, and/or other commercially reasonable verification methods.
3. Because the Provider delivers broadband service to a verified physical location via fixed wireless infrastructure, the Provider has a high degree of confidence in the identity and location of each customer. The physical service address is confirmed as part of broadband installation and cannot be falsified, as the Provider's wireless equipment must be directed at a specific location.
4. No voice services are provisioned until the customer's identity has been satisfactorily verified and a service agreement has been executed.

B. Telephone Number Assignment and Validation

Pursuant to the Provider's telephone number validation practices:

- All Direct Inward Dialing (DID) numbers assigned to customers are sourced through the Provider's upstream wholesale carriers and are assigned directly to the customer's account in the Provider's systems.

- Customers may only use telephone numbers that have been assigned to their account by the Provider. The Provider's PBX(s) are configured to restrict outbound Caller ID to numbers assigned to the originating customer's account.
- Customers requesting to port in existing telephone numbers must demonstrate right-to-use through a valid Letter of Authorization (LOA) and a copy of their current telephone service bill showing the number(s) to be ported.
- The Provider does not allow customers to configure arbitrary or unassigned Caller ID numbers for outbound calls.

C. Acceptable Use and Contractual Obligations

All voice service customers are subject to the Provider's Acceptable Use Policy (AUP) and Terms of Service, which expressly prohibit:

- Originating, facilitating, or transmitting illegal robocalls, as defined under the Telephone Consumer Protection Act (TCPA), the TRACED Act, and applicable FCC rules and orders.
- Caller ID spoofing in violation of the Truth in Caller ID Act of 2009 and 47 U.S.C. § 227(e).
- Using the Provider's voice services for any form of telephone fraud, scam, or deceptive telemarketing.
- Transmitting pre-recorded or artificial voice messages to residential telephone lines without the prior express consent of the called party, except as permitted by law.
- Any use of auto-dialing equipment or predictive dialers without appropriate consent from called parties as required by applicable law.

Violation of these terms constitutes grounds for immediate suspension or termination of voice services.

IV. Know Your Upstream Provider Program

Although the Provider operates as an originating voice service provider (not an intermediate provider), and its upstream provider vetting obligations derive from the general requirement under 47 CFR § 64.6305(d)(2)(ii) to describe any procedures in place to know its upstream providers, the Provider nonetheless maintains the following procedures to verify the compliance and legitimacy of its upstream wholesale voice carriers:

1. The Provider has verified that both of its upstream wholesale carriers maintain active, compliant filings in the FCC's Robocall Mitigation Database: (a) Voyant Communications, LLC (d/b/a Vitelity), and (b) VoIP Innovations, LLC.
2. The Provider periodically reviews the RMD to confirm the continued listing and compliance status of both upstream carriers.
3. The Provider understands that its upstream wholesale carriers bear the STIR/SHAKEN implementation obligation for traffic originated on their network infrastructure on the Provider's behalf. The Provider will verify the STIR/SHAKEN implementation status of its upstream carriers through their respective RMD filings.
4. The Provider maintains records of its wholesale voice service agreements with both upstream carriers, including contact information for robocall mitigation and traceback purposes.

In the event that either upstream carrier is removed from the RMD, subjected to FCC enforcement action, or otherwise becomes non-compliant, the Provider will promptly evaluate the situation and, if necessary, migrate affected traffic to the remaining compliant carrier or to an alternative upstream carrier to ensure continuity of compliant voice service delivery.

V. Traffic Monitoring and Call Analytics

Pursuant to 47 CFR § 64.6305(d)(2)(ii), the Provider describes the following analytics and monitoring practices used to identify and prevent illegal robocall traffic:

A. Call Detail Record (CDR) Monitoring

The Provider monitors call detail records generated by its PBX(s) on a regular basis to detect suspicious or anomalous calling patterns. Specific indicators monitored include:

- Abnormally high call volumes from a single extension or customer account, including large bursts of calls in short timeframes.
- High volumes of short-duration calls or calls with low answer/completion rates, which may indicate robocalling or auto-dialer activity.
- Sequential or patterned dialing of called-party numbers.
- Calls to numbers on the National Do Not Call Registry, invalid or unassigned NPA-NXX combinations, or numbers not assigned by the North American Numbering Plan Administrator.
- Unusual spikes in call volume during non-business hours.
- Calls originating with Caller ID information that does not match numbers assigned to the originating customer's account.

B. PBX-Level Controls

The Provider's PBX(s) are configured with the following technical controls to prevent abuse:

- Concurrent call limits are enforced per customer account/extension to prevent bulk dialing.
- Outbound Caller ID is restricted to numbers assigned to the customer's account; the PBX(s) do not permit customers to set arbitrary Caller ID values.
- International dialing and premium-rate number access are restricted by default and enabled only upon verified customer request.
- Rate limiting controls are in place to prevent excessive call origination volumes that are inconsistent with normal business or residential use.

C. Third-Party Analytics

The Provider relies on the analytics and fraud detection capabilities of its upstream wholesale carriers as an additional layer of monitoring. Both Voyant Communications, LLC (d/b/a Vitelity) and VoIP Innovations, LLC maintain fraud detection systems that monitor for illegal robocall traffic across their networks. The Provider cooperates with both upstream carriers in any fraud investigations and promptly acts on notifications of suspicious traffic originating from the Provider's accounts.

Third-Party Analytics Vendor(s): The Provider currently relies on the analytics and fraud detection systems operated by its upstream wholesale carriers (Voyant Communications, LLC d/b/a Vitelity, and VoIP Innovations, LLC) for network-level call analytics. The Provider does not independently contract with a separate third-party call analytics vendor at this time. Should the Provider engage a third-party analytics vendor in the future, this Plan will be updated within 10 business days to reflect that change, including the name(s) of any such vendor(s).

VI. Traceback Cooperation Commitment

Pursuant to 47 CFR § 64.6305(a)(2) and (d)(2)(iii), the Provider hereby commits to the following:

1. The Provider commits to responding fully and within 24 hours to all traceback requests received from the Federal Communications Commission (FCC), law enforcement agencies, and the Industry Traceback Group (ITG) operated by USTelecom – The Broadband Association.
2. The Provider will cooperate fully with such entities in investigating and stopping any illegal robocallers that may use the Provider's service to originate calls.
3. The Provider has designated a single point of contact for receiving and responding to all traceback requests. The contact information for this designated individual is maintained in the Provider's RMD filing and in the Provider's records, and is available to the FCC, law enforcement, and the ITG upon request.
4. Upon receipt of a traceback request, the Provider will promptly identify the customer account associated with the traffic in question using CDR records and PBX logs, and will provide all responsive information to the requesting entity within the 24-hour timeframe.
5. The Provider will preserve all call detail records, PBX logs, and related documentation relevant to any traceback investigation for a minimum period consistent with FCC requirements and any applicable legal hold obligations.

VII. Enforcement History Disclosure

Pursuant to 47 CFR § 64.6305(d)(2)(iv), the Provider discloses the following:

At no time in the prior two years has the Provider, or any entity with which the Provider shares common ownership, management, directors, or control, been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

Should any such action or investigation arise, the Provider will update this Plan and its RMD filing within 10 business days to include a description of the action or investigation, the agencies involved, the date commenced, the current status, a summary of any findings of wrongdoing, and whether any final determinations have been issued.

VIII. Plan Maintenance and Review

This Robocall Mitigation Plan is a living document that will be reviewed and updated on a regular basis. The Provider commits to the following:

- Annual review of this Plan, at minimum, in conjunction with the annual RMD recertification process.
- Updates within 10 business days of any material change to the Provider's voice service operations, upstream carrier relationships, analytics tools, or compliance procedures.
- Prompt updates in response to new FCC orders, rules, public notices, or guidance affecting robocall mitigation obligations.
- Retention of prior versions of this Plan for a minimum of three years.