

James Bouse Enterprises, LLC

d/b/a Brazos WiFi

Robocall Mitigation Plan

March 30, 2026

Introduction. James Bouse Enterprises, LLC d/b/a Brazos WiFi (“Brazos WiFi”), pursuant to Sections 64.6301 and 64.6305 of the Commission’s rules, 47 C.F.R. §§ 64.6301, 64.6305 and the Commission’s “Best Practices” as amended, adopts this Robocall Mitigation Plan (“Plan”). This Plan is current as of its submission date and may be subject to changes as necessary to further comply with amended Commission regulations and requirements. This document sets forth the Provider’s current policies and procedures designed to reduce or eliminate outbound illegal robocalls originating on its network.

Pursuant to Section 64.6305 of the Commission’s rules, 47 C.F.R. § 64.6305, Brazos WiFi commits to take all reasonable steps to avoid originating illegal robocall traffic and shall include a commitment to respond fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls. As set forth below, Brazos WiFi has adapted the North America Numbering Council Call Authentication Trust Anchor Working Group’s *Best Practices for the Implementation of Call Authentication Frameworks* into its Plan.

Company Contact:

James Bouse
Owner
James Bouse Enterprises, LLC
P.O. Box 163
Kurten, Texas 77862
Telephone: 979-999-7000
Email: jim@brazoswifi.com

Business Information. Brazos WiFi is a privately-owned business. The Company’s principals exert full control over Brazos WiFi’s operations. Brazos WiFi is not affiliated with any other entity that provides telecommunications or communications services. James Bouse Enterprises, LLC operates under the assumed name Brazos WiFi and no other assumed names.

Brazos WiFi operates as a non-facilities-based interconnected VoIP provider. Brazos WiFi is not a foreign voice service provider, is not an intermediate or gateway provider, and does not act as a wholesale provider originating calls on behalf of another provider or providers. Brazos WiFi does not maintain an operating company number and does not have direct access to telephone numbers from the North American Numbering Plan Administrator (NANPA) and/or the National Pooling Administrator.

Certification. Brazos WiFi certifies that it has not been prohibited from filing in the Robocall Mitigation Database. Brazos WiFi certifies that it independently reviews its underlying carrier subscriber traffic analytics and does not separately engage a third-party analytics provider. Brazos WiFi certifies further that it has not been subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing. And Brazos WiFi certifies that at no time during the prior two years, has Brazos WiFi 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.

Reasonable Steps to Prevent Robocalling.

Customer and Subscriber Vetting

Brazos WiFi fully vets all subscribers before providing service to the subscriber. Brazos WiFi obtains specific subscriber information including service locations and principals, if commercial subscribers, and verifies location for all subscribers. Further, Brazos WiFi compares information provided by the subscriber against underlying carrier records to verify accuracy and authentication and validate subscriber information. Subscribers are served under a service agreement.

Brazos WiFi monitors its subscribers' traffic for call, originating number, and terminating number irregularities in conjunction with its underlying carriers, and should irregularities be determined, will immediately contact the subscriber as part of its investigatory process.

Telephone Number Validation

Telephone Number Validation refers to the confirmation of the customer or end-user right to use a telephone number in connection with their subscribed voice service(s). In accord with industry best practices, the Provider has procedures in place to confirm the calling customer's right to use a telephone number. Specifically, a subscriber of the Provider's services is permitted to use a telephone number as their caller identity if a number is directly managed by the Provider and/or obtained by the Provider via an underlying partner.

Network Traffic Investigation

Consistent with its commitment above, Brazos WiFi will respond fully to all traceback requests from the Commission, law enforcement, and the industry traceback consortium as soon as possible and at no time exceeding 24 hours from the time of the request and will cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

As a non-facilities-based voice service provider, Brazos WiFi coordinates with its underlying carriers to monitor Brazos WiFi's subscribers' traffic, identify traffic anomalies including, but not limited to, unusually high call volumes to different telephone numbers and disparate geographic areas, over the course of one or more hours, for which Brazos WiFi will investigate, and to immediately block subscriber service if robocalling is suspected. Confirmation of illegal activity will result in immediate subscriber service termination.

The Provider monitors the usage of its network and examines call detail records (CDRs) on a recurring basis for the purpose of detecting suspicious call activity and/or calling patterns. When network usage patterns consistent with illegal robocalls are detected or the Provider otherwise

suspects illegal robocalling or spoofing is taking place on its network, it immediately seeks to identify the party that is originating, terminating, or routing these calls so that it may take appropriate action.

Refusing Traffic from Unlisted Providers.

In conjunction with its underlying carriers, Brazos WiFi refuses to accept traffic from unlisted and de-listed providers from the Commission's Robocall Mitigation Database.

Ongoing Robocall Mitigation.

Brazos WiFi, in conjunction with its underlying carriers, will implement a call authentication protocol for voice calls delivered over the non-IP portions of its network that do not use SIP technology when such a protocol is fully developed and finalized by industry standards and the necessary equipment and software is available on the commercial market.

Brazos WiFi anticipates that its Plan will evolve as it makes Plan enhancements, as underlying carriers enhance their own plans, and as the Trust Anchor and industry generally gain experience in caller ID authentication protocols.