



Company Name: Flynode Wireless, LLC

Company Address 601 Brickell Key Drive, Suite 700, Miami, Florida, 33131, USA

Company Phone #: 9544198043

Robocall Mitigation Plan

Updated February 2026

Purpose and Scope

This Robocall Mitigation Plan (“Plan”) describes the policies and procedures Flynode Wireless, LLC (“Provider”) uses to prevent, detect, and mitigate illegal robocall traffic on the voice services it supports, consistent with 47 C.F.R. § 64.6305 and related FCC robocall mitigation requirements.

The Plan applies to the Provider’s to all voice traffic that the Provider carries/processes across its network for its customers. The Provider does not provide end-user voice service.

Traffic carried over the Provider’s network is not originated by the Provider; calls are originated by the Provider’s customers and/or their downstream end users and are routed through the Provider for transport, interconnection, and delivery to the next carrier upstream. This Plan governs the Provider’s controls for customer onboarding and due diligence, as applicable, traffic monitoring, escalation, enforcement actions, and traceback cooperation for traffic carried and/or processed on behalf of its customers.

Provider Role and Call Flow

The Provider offers SIP trunking and DID provisioning to wholesale/reseller customers and other voice service providers. The Provider operates as a non-gateway intermediate provider and primarily carries/processes customer traffic; it does not provide end-user voice service.

High Level Call Flow

- Outbound direction: Calls are originated by the Provider’s wholesale customers and/or their downstream end users and delivered to the Provider over SIP trunks. The Provider then processes and routes the traffic to upstream interconnection partners for delivery toward the PSTN and/or the next provider in the call path.
- Inbound direction (to Provider-provisioned DIDs): Calls destined to DIDs provisioned by the Provider are received from upstream interconnection partners and delivered via SIP trunks to the applicable wholesale customer for termination to its downstream end users.

In this role, the Provider maintains provisioning/routing controls for the services it provides, monitors carried traffic for suspicious patterns and applies appropriate enforcement actions as described herein.

STIR/SHAKEN Implementation

The Provider certifies that its voice network is entirely IP-based, and the Provider maintains an in-house STIR/SHAKEN signing capability and its interconnection practices are intended to preserve and pass

through authenticated caller ID information, including any upstream Identity header and attestation, to the next provider in the call path, except where technical interoperability or security needs require otherwise.

For certain unauthenticated SIP calls received directly from an originating provider, the Provider can authenticate and sign the calls using its own signing certificate. In those scenarios, the Provider assigns attestation based on the information available to it and its ability to verify the calling party's identity and authority to use the associated telephone number(s), consistent with applicable FCC rules, orders, and guidance.

To the extent the Provider originates any calls on its own network (e.g., operational/test traffic), those calls are authenticated and signed using the Provider's signing certificate via its in-house signing platform.

Know Your Customer

The Provider takes affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence to ensure its services are not used to transmit illegal traffic.

As part of standard onboarding, and renewal review, as applicable, the Provider may obtain and verify customer identity and authority information such as the customer's legal name and/or DBA, formation documents, business address, website, contact information, authorized signer, and designated compliance contacts. The Provider documents the customer's requested services and intended use case, for example, expected call volumes/CPS, target destinations, and whether call center, dialer, or marketing traffic is involved.

The Provider also verifies that the customer is properly registered with the FCC as applicable, including confirming FRN and Robocall Mitigation Database status, where required. Customer agreements prohibit illegal robocalls, spoofing, and other abusive activity; require accurate and up-to-date customer information; require traceback cooperation; and authorize monitoring and enforcement actions, including rate-limiting, blocking, suspension, and termination.

Enhanced review may be triggered by higher-risk indicators including, but not limited to, foreign traffic into the U.S., unusually high-volume requests, unverifiable identity information, prior complaints or blocking signals, or traffic patterns inconsistent with the stated use case. In those situations, the Provider may require additional documentation and apply tighter initial controls, such as staged ramp-up, CPS caps, and/or route limitations. Customer records are refreshed periodically and re-verified.

Traffic Analysis and Monitoring

To help identify abnormal activity, the Provider uses its own SBC to monitor traffic call flow. This may include secure access to authorized users, key performance metrics such as ASR and ACD, limiting customers to an approved quantity of channels, and applying bursting controls to help reduce uncontrolled spikes and misuse. The Provider does not rely on a third-party monitoring vendor for these functions but will work with other providers in the call flow to address fraud or abuse indicators detected on their networks.

If suspicious or potentially illegal traffic is detected, the Provider typically contacts and warns the

customer and may block the connection to stop the activity. If the issue requires further escalation, the Provider will cooperate with the appropriate authorities as needed.

Know Your Upstream Providers

The Provider maintains an inventory of its upstream interconnection and transport partners and appropriate points of contact for operational support, fraud and/or abuse coordination, and traceback requests. The Provider reviews upstream network feedback, including blocking or other abuse indicators, and coordinates with upstream partners as needed to investigate and mitigate suspicious or unlawful traffic. Upstream relationships and routing are reviewed periodically and updated when material changes occur.

Traceback Commitment and Ongoing Efforts

The Provider remains committed to cooperating with the Commission, law enforcement, and the traceback consortium by responding fully and within 24 hours to call traceback requests and supporting efforts to investigate and stop illegal robocall activity.

The Provider also maintains and continually improves its robocall mitigation practices, including:

- Updating its RMD filing and associated plan information within 10 business days when required filing information materially changes.
- Periodically reviewing and updating its mitigation program to address emerging threats and relevant regulatory developments.
- Participating in industry initiatives and forums, as applicable, to support best practices for combating illegal robocalls.
- Providing customers with a method to report suspected robocall-related concerns and, where applicable, sharing general guidance on avoiding illegal robocalls.

Person of Contact

Name: Jose Figueroa

Title: CEO

Email: jose@flynode.us

Phone: 954-419-8043

This program demonstrates Flynode Wireless, LLC's commitment to protecting consumers, upholding industry standards, and contributing to the elimination of illegal robocalls.