

# JNB TEK, LLC

## ROBOCALL MITIGATION PLAN

*Updated August 26, 2026*

|                       |                                                                               |
|-----------------------|-------------------------------------------------------------------------------|
| <b>Provider</b>       | JNB Tek, LLC                                                                  |
| <b>RMD Role</b>       | Voice Service Provider without a STIR/SHAKEN implementation obligation        |
| <b>Business Model</b> | Non-facilities-based retail VoIP reseller serving end-user business customers |

### I. Background and Regulatory Framework

The Federal Communications Commission (FCC or Commission) requires voice service providers, including VoIP resellers such as JNB Tek, LLC (JNB), to maintain an appropriate robocall mitigation program and to file and maintain a certification and written robocall mitigation plan in the Commission's Robocall Mitigation Database (RMD). This plan supersedes JNB's February 2024 robocall mitigation plan and describes JNB's current practices as of the update date above.

JNB's program is designed to take reasonable, effective steps to avoid originating illegal robocall traffic; to know its customers and exercise due diligence so that its services are not used to originate illegal calls; to identify and respond to suspicious calling activity; and to respond fully and timely to traceback requests. JNB will cooperate with the Commission, law enforcement, and the industry traceback consortium in investigating and stopping illegal robocallers that use its services.

JNB maintains this plan as a living compliance document. JNB will review the accuracy of its RMD filing at least annually, will recertify its filing on or before March 1 as required by 47 C.F.R. § 64.6305(h), and will update required RMD information within ten business days of a material change as required by 47 C.F.R. § 64.6305(d)(5).

*Authorities: 47 C.F.R. §§ 64.6305(a), 64.6305(d)(1)-(5), 64.6305(h); 47 C.F.R. § 64.1200(n); Improving the Effectiveness of the Robocall Mitigation Database, FCC 24-135; Wireline Competition Bureau Public Notice, DA 26-72 (Jan. 22, 2026).*

### II. JNB's Business Model and Role in the Call Chain

JNB is a managed services provider and voice service provider focused on small and medium-sized business customers. JNB provides retail voice service directly to end-user business customers. JNB does not offer wholesale origination or transit service to other voice service providers, does not operate as a gateway provider, and does not operate as a non-gateway intermediate provider for third-party wholesale traffic.

JNB is a non-facilities-based reseller. It does not control the underlying network infrastructure on which PSTN interconnection and the technological STIR/SHAKEN authentication function are performed. JNB obtains underlying voice connectivity, numbering, and related network functions from established wholesale carrier partners, including Bandwidth, Inc. Accordingly, based on JNB's current network-control facts, JNB identifies its RMD call-chain role as a "Voice Service Provider without a STIR/SHAKEN implementation obligation."

The Commission has clarified that the STIR/SHAKEN implementation obligation rests with the provider that controls the network infrastructure necessary to implement STIR/SHAKEN. The Commission has also recognized that resellers that lack such control may nevertheless participate voluntarily in caller-ID authentication arrangements with their wholesale providers. If JNB's network architecture or level of infrastructure control materially changes, JNB will reevaluate this classification and update its RMD filing as required.

*See 47 C.F.R. § 64.6305(d)(4)(vi); Call Authentication Trust Anchor, Eighth Report and Order, FCC 24-120, paras. 17-20 & n.88 (discussing resellers that lack control of the infrastructure necessary to implement STIR/SHAKEN and rely on wholesale providers for authentication).*

### III. Know-Your-Customer (KYC) and Customer Due Diligence

JNB takes affirmative, effective measures to prevent new and renewing customers from using its services to originate illegal calls. JNB's business model materially reduces anonymous or high-risk onboarding because JNB ordinarily sells, installs, configures, and supports its services directly for identifiable business customers in its service area.

As part of onboarding and, as appropriate, when service is renewed, materially expanded, transferred, or otherwise re-evaluated, JNB collects and reviews information reasonably sufficient to establish the identity and legitimacy of the customer and the intended use of the service. Depending on the circumstances, JNB may collect or verify:

- Customer legal or operating business name and physical service location;
- Primary business contact person, telephone number, and email address;
- Company website, public business presence, or other indicators that the customer is a legitimate operating business;
- The physical location at which JNB equipment or service is deployed and the nature of the customer's operations;
- The telephone numbers assigned to or ported for the customer and the customer's authority to use those numbers; and
- The expected calling use case, particularly if a requested configuration would enable unusually high-volume, automated, prerecorded, or other atypical outbound calling.

JNB does not market its retail voice service as an anonymous bulk-dialing, lead-generation, or wholesale termination platform. Customer requests that would materially change an account's normal calling profile or enable unusual automated or high-volume outbound calling are subject to additional review before JNB enables or continues the requested configuration.

JNB retains customer and service records reasonably sufficient to identify the customer associated with its accounts, SIP credentials, telephone numbers, and calling activity. These records support both JNB's ongoing due diligence and its ability to cooperate promptly with traceback and law-enforcement requests.

*See 47 C.F.R. § 64.1200(n)(4) (requiring affirmative, effective measures for new and renewing customers, including knowing customers and exercising due diligence); 47 C.F.R. § 64.6305(d)(2)(ii).*

### IV. Acceptable Use, Caller-ID, and Customer Enforcement Controls

JNB's customer agreements and acceptable-use requirements prohibit use of JNB's services for illegal, abusive, fraudulent, deceptive, or misleading activity. Prohibited uses include unlawful telemarketing or prerecorded/automated calling, unlawful spoofing or manipulation of caller-ID information, and other calling activity that violates applicable federal or state law, including the Telephone Consumer Protection Act and the Truth in Caller ID Act.

JNB reserves the right to investigate suspected misuse and to restrict, suspend, or terminate service when necessary to protect the network, comply with law, or stop suspected illegal calling activity. Depending on the circumstances, JNB may also require the customer to provide additional documentation concerning its calling practices or its authorization to use a telephone number before service is restored or continued.

### V. Telephone-Number Authorization and STIR/SHAKEN Authentication

JNB controls the caller-ID numbers that its retail customers are authorized to present through JNB-provided service. Customer telephone numbers are either assigned through JNB's wholesale carrier arrangements or ported to the applicable carrier platform for the customer. JNB does not permit customers to arbitrarily present telephone numbers with which JNB has no documented relationship. If a customer requests use of a caller-ID number not assigned or ported through JNB's normal service, JNB requires documentation establishing the customer's right to use that number before such use is authorized.

JNB does not independently operate the underlying originating network infrastructure on which the technological act of STIR/SHAKEN signing occurs. JNB participates in caller-ID authentication through its wholesale carrier arrangements. For traffic carried by Bandwidth, JNB provides the customer and

telephone-number authorization information needed to support authentication, and a JNB-associated STIR/SHAKEN certificate is provisioned within Bandwidth's platform for the applicable outbound signing arrangement. Bandwidth performs the technological signing function on the network infrastructure it controls.

JNB will provide its wholesale carrier partners with information reasonably necessary to determine the appropriate attestation for calls associated with JNB's customers and telephone numbers and to support traceback to the originating end user. JNB will not knowingly authorize a customer to use a calling number for which JNB lacks a reasonable basis to conclude that the customer is entitled to use the number.

*See FCC 24-120, paras. 17-20 & n.88; ATIS reseller use cases discussed therein. JNB's RMD implementation-status certification should remain consistent with its actual level of control over the network infrastructure and its current wholesale authentication arrangement.*

## **VI. Network Monitoring, Analytics, and Identification of Suspicious Traffic**

JNB monitors its own service records and relies in part on network-level fraud and traffic-monitoring capabilities made available through its wholesale carrier partners. JNB does not separately contract with a dedicated third-party robocall analytics vendor. Its mitigation practices may use information from JNB's PBX/SIP systems, account records, customer history, and wholesale carrier reports or controls to identify anomalous or suspicious calling patterns.

Indicators that may prompt review include, as applicable:

- A sudden or unexplained increase in outbound call volume;
- Large numbers of short-duration, unanswered, or failed calls;
- Sequential or repetitive dialing patterns inconsistent with the customer's normal business use;
- Unusual changes in destination patterns or calling hours;
- Repeated complaints, traceback inquiries, carrier fraud alerts, or downstream blocking reports associated with a customer or number;
- Attempts to use unauthorized caller-ID numbers or otherwise circumvent JNB's caller-ID controls; and
- Other activity inconsistent with the customer's known business purpose or historical calling profile.

JNB may adjust the intensity of its review based on the customer's business model, the nature of the traffic, information received from Bandwidth or another wholesale carrier, and any complaint, traceback, or law-enforcement information available to JNB.

*See 47 C.F.R. § 64.6305(d)(2)(ii) (requiring the mitigation plan to describe analytics used to identify and block illegal traffic and to identify any third-party analytics vendors).*

## **VII. Investigation and Mitigation of Suspected Illegal Traffic**

When JNB detects, or receives credible information regarding, traffic that may be illegal or inconsistent with this plan, JNB will promptly investigate. The investigation may include reviewing call-detail records, SIP/account logs, telephone-number assignments, customer records, relevant IP or endpoint information, and information supplied by JNB's wholesale carrier or the requesting agency or traceback entity.

When warranted by the facts, JNB may take one or more of the following measures:

- Contact the customer and require an explanation or supporting documentation;
- Restrict or disable affected outbound calling, SIP credentials, trunks, endpoints, or caller-ID numbers;
- Temporarily suspend the customer's voice service while an investigation is completed;
- Coordinate with Bandwidth or another wholesale carrier to block or mitigate identified traffic at the carrier-network level;
- Terminate the customer's service for confirmed or material violations of law or JNB's acceptable-use requirements; and
- Preserve and provide relevant records in response to lawful Commission, law-enforcement, or traceback requests.

If JNB receives a Commission Notice of Suspected Illegal Traffic or other direction triggering the requirements of 47 C.F.R. § 64.1200(n), JNB will investigate and take the actions required by the rule,

including blocking or ceasing the identified traffic and substantially similar traffic when required. JNB will also observe applicable public-safety safeguards and will not intentionally block emergency calls to 911.

### **VIII. Traceback Response and Cooperation**

JNB commits to respond fully and within the time required by FCC rules to traceback requests from the Commission, civil or criminal law enforcement, and the industry traceback consortium. JNB will maintain a responsible point of contact in its RMD filing and will use its customer, number-assignment, SIP, and call-detail records to identify the originating customer and provide responsive information.

JNB will cooperate with such entities in investigating and stopping illegal robocallers that use JNB's services and will devote sufficient resources to provide complete and timely responses. JNB will also cooperate with its wholesale carrier partners when carrier-level information or mitigation is necessary to complete a traceback or stop unlawful traffic.

*See 47 C.F.R. §§ 64.6305(a)(2), 64.6305(d)(2)(iii), and 64.1200(n)(1).*

### **IX. Plan Administration, RMD Maintenance, and Annual Review**

JNB will review this mitigation plan and the associated RMD certification whenever there is a material change to its business model, call-chain role, network-control facts, wholesale carrier arrangements, caller-ID authentication configuration, KYC practices, analytics or monitoring practices, or robocall-mitigation point of contact. JNB will update its RMD filing within ten business days when information required by 47 C.F.R. § 64.6305(d)(1)-(4) changes.

At least annually, and before completing the annual RMD recertification, JNB will review the information in its RMD filing and this plan for accuracy. JNB will also ensure that the separate RMD certification accurately addresses any formal Commission, law-enforcement, or regulatory investigation or action required to be reported for the prior two years under 47 C.F.R. § 64.6305(d)(2)(iv).

This plan is intended to describe JNB's actual mitigation practices. If JNB changes a practice described here, it will update the plan and its RMD filing as necessary rather than continuing to certify to an outdated description.

### **Selected Authorities**

- 47 C.F.R. § 64.6305 - Robocall mitigation and certification.
- 47 C.F.R. § 64.1200(n) - Voice service provider traceback, mitigation, KYC, and upstream-provider obligations.
- Call Authentication Trust Anchor, Sixth Report and Order and Further Notice of Proposed Rulemaking, FCC 23-18 (Mar. 17, 2023).
- Call Authentication Trust Anchor, Eighth Report and Order, FCC 24-120 (Nov. 21, 2024).
- Improving the Effectiveness of the Robocall Mitigation Database, Report and Order, FCC 24-135 (Dec. 30, 2024).
- Wireline Competition Bureau Announces OMB Approval and Effective Dates for RMD Rules and Provides Filing Guidance, DA 26-72 (Jan. 22, 2026).