Junxionet LLC

Robocall Mitigation Plan

Robocall Mitigation Program Description submitted to the Federal Communications Commission Robocall Mitigation Database pursuant to 47 CFR § 64.6305

Legal Business Name	Junxionet LLC
FCC Registration Number (FRN)	0039048897
Business Address	8673E Dry Creek Rd, Unit 1012, Centennial, CO 80112, United States
Previous Business Name(s)	Junction Networks
Other DBAs / Other FRNs	None / None
Principals, Affiliates, Subsidiaries, Parents	None
Role in the Call Chain	Voice Service Provider (originating provider) without a STIR/SHAKEN obligation
STIR/SHAKEN Implementation	No STIR/SHAKEN implementation on Junxionet's own network (Certification Option 3)
Robocall Mitigation Contact	Jayson Owens, Chief Operating Officer, Operations
Contact Telephone / Email	(303) 276-7090 / support@junxionet.net
Effective Date / Version	October 22, 2026 / Version 1.0

1. Purpose and Scope

This Robocall Mitigation Plan (the "Plan") describes the specific, reasonable steps Junxionet LLC ("Junxionet" or the "Company") takes to avoid originating, carrying, or processing illegal robocall traffic, consistent with 47 CFR § 64.6305 and 47 CFR § 64.1200(n). The Plan applies to every call originated by Junxionet customers using telephone numbers, SIP trunking, or hosted phone system services provided or managed by Junxionet, and it is binding on all Junxionet personnel and contractors who provision, support, or administer customer voice services.

2. Company Overview and Role in the Call Chain

Junxionet is a small telecommunications reseller and consulting company. Junxionet deploys, hosts, manages, and supports cloud and premises-based business phone systems (including 3CX) and associated SIP trunking for business customers, primarily in the hospitality sector (hotels and related properties), along with property management system (PMS) integrations and managed session border controller (SBC) services.

Role in the call chain. Junxionet acts as a voice service provider for its business customers' outbound calls, which are handed off to Junxionet's underlying facilities-based carrier(s) for completion. Junxionet does not operate as a gateway provider, does not accept voice traffic from

foreign providers, and does not offer wholesale, transit, or carrier-to-carrier services. Junxionet does not accept calls from other voice service providers or intermediate providers for onward routing.

Customer profile. Junxionet serves only verifiable businesses and verifiable individuals (such as sole proprietors and independent professionals) conducting business within the United States. It does not offer general residential consumer service, does not serve customers located outside the United States, and does not offer services designed for high-volume outbound calling. Junxionet declines prospective customers whose primary intended use is outbound telemarketing, autodialed or prerecorded-message campaigns, lead generation, or call-center dialing.

3. STIR/SHAKEN Implementation Status

Junxionet has not implemented the STIR/SHAKEN caller ID authentication framework on its own network. Junxionet does not hold its own Operating Company Number (OCN) or direct numbering resources. Telephone numbers used by Junxionet customers are assigned by, and calls are delivered through, Junxionet's underlying carrier(s), which are listed in the Robocall Mitigation Database and which are responsible for STIR/SHAKEN authentication of calls they originate on their networks.

All calls Junxionet originates are subject to this Plan regardless of authentication status. Junxionet will reassess its STIR/SHAKEN status whenever its network, numbering access, or role in the call chain changes, and will update its Robocall Mitigation Database certification accordingly.

4. Know Your Customer (KYC) Protocols

Before any telephone number is assigned or any outbound calling is enabled, Junxionet completes the following verification steps for every new customer. No service is activated until verification is complete, documented, and approved by a member of Junxionet's executive leadership (Chief Executive Officer, Chief Operating Officer, or other C-suite officer).

4.1 Identity Verification

Business customers. Junxionet verifies:

- **Legal entity.** Full legal business name, entity type, and confirmation of active, good-standing registration with the applicable Secretary of State.
- **Tax identification.** Federal Employer Identification Number (EIN), cross-checked against the legal business name provided.
- **Authorized representative.** Name, title, direct phone number, and business email of the individual authorized to contract for service, verified through direct contact with the business.

Individual customers. For individuals conducting business in their own name, Junxionet verifies:

- **Identity.** Full legal name verified against a valid, unexpired government-issued photo identification.
- **Business activity.** The nature of the business conducted, supported by documentation such as a business license, DBA or assumed-name filing, professional license, website, or invoices.
- **Tax identification.** A valid U.S. taxpayer identification number (EIN, or ITIN for sole proprietors), handled and stored securely.

All customers. Junxionet also requires:

- **U.S. physical address.** A verifiable physical address within the United States (not a P.O. box or virtual mailbox only), confirmed against public records, site visit, or installation address.
- **Billing.** A billing method in the customer's own name. Anonymous, prepaid, or untraceable payment methods are not accepted.

4.2 Intended Use and Caller ID Authorization

- **Intended use.** The customer must describe its business purpose for voice service, its expected number of users, and its expected outbound call volume. This information is used to size trunk capacity and to establish the traffic baseline described in Section 6.
- **Right to use numbers.** For ported numbers, Junxionet requires a signed Letter of Authorization (LOA) and a copy of a recent bill from the losing carrier. Customers may display as caller ID only numbers assigned to them by Junxionet or numbers they have documented authority to use.
- **Proportional number assignment.** Number assignments are limited to what the customer's documented operations reasonably require. Requests for large or sequential blocks of numbers, or for frequent number rotation, require documented business justification and C-suite approval.

4.3 Red Flags and Enhanced Review

Any of the following results in enhanced review by a C-suite officer, and service is denied if the concern cannot be resolved:

- Refusal or inability to provide verification information, or information that does not match public records.
- Intended use involving outbound marketing, autodialing, prerecorded or artificial-voice messages, debt collection campaigns, or lead generation.
- Requests to display caller ID numbers the customer cannot show authority to use.
- Requested call capacity or number quantity far exceeding the customer's documented operations.
- Prior termination by another voice provider for robocall, fraud, or acceptable-use violations, or appearance in any traceback or enforcement action known to Junxionet.

4.4 Renewing and Existing Customers

Junxionet re-verifies customer information at each contract renewal, upon any change in ownership, legal name, business name, address, or authorized contact, and upon any material increase in requested numbers or call capacity. Customer verification records are retained for the life of the account and for at least two (2) years after service ends.

5. Acceptable Use and Terms of Service

Junxionet's acceptable use terms are written directly into its customer service agreement, which every customer must execute before service is activated. The service agreement prohibits the following:

- Making or initiating any call that violates the Telephone Consumer Protection Act (47 U.S.C. § 227), the FCC's implementing rules (47 CFR § 64.1200), the Telemarketing Sales Rule, or any applicable state law.

- Transmitting misleading or inaccurate caller ID information with the intent to defraud, cause harm, or wrongfully obtain anything of value, in violation of the Truth in Caller ID Act (47 U.S.C. § 227(e)) and 47 CFR § 64.1604.
- Displaying any calling number the customer is not assigned or authorized to use.
- Using artificial or prerecorded voice messages, or automatic telephone dialing systems, without the prior express consent required by law.
- Calling numbers on the National Do Not Call Registry or any internal do-not-call list in violation of law.
- Reselling, sublicensing, or providing Junxionet voice service to any third party for outbound calling without Junxionet's prior written approval.
- Using the service for fraud, harassment, impersonation of government agencies or businesses, or any other unlawful purpose.

Enforcement rights. The service agreement reserves Junxionet's right to immediately suspend or terminate service, in whole or in part and without prior notice, when Junxionet reasonably believes a customer is violating the service agreement or originating illegal robocall traffic. Junxionet may also block specific numbers, routes, or destinations; disclose customer information to the FCC, law enforcement, and the Industry Traceback Group (ITG) in response to traceback or lawful requests; and recover from the customer any fines, costs, or damages arising from the customer's violations. Customers must cooperate fully with any Junxionet investigation.

6. Call Monitoring and Analytics

Junxionet uses the following tools and methods to prevent, detect, and stop illegal robocall traffic and unauthorized use of customer phone systems.

6.1 Preventive Controls on Every Phone System

- **Caller ID enforcement.** Outbound caller ID is configured by Junxionet at the trunk and extension level and is restricted to numbers assigned to or verified for that customer. End users cannot set arbitrary caller ID.
- **Capacity limits.** Simultaneous outbound call capacity on each SIP trunk is sized to the customer's documented needs, limiting the volume any compromised or misused system can generate.
- **Destination restrictions.** International dialing is disabled by default and enabled only for the specific country codes a customer requires. Premium-rate and high-risk destinations are blocked.
- **System security.** Customer phone systems are hardened against compromise that could be used to generate illegal calls: strong unique SIP credentials, platform anti-hacking and IP blocking controls, restricted administrative access with multi-factor authentication where supported, and timely application of software updates and security patches.

6.2 Traffic Monitoring and Analysis

Junxionet reviews phone system and carrier call detail records (CDRs) and system reports, together with traffic reports and fraud alerts provided by its underlying carrier(s), and compares each customer's activity against the baseline established at onboarding. The following patterns trigger investigation:

- **Volume spikes:** outbound call volume significantly above the customer's historical baseline (for example, three times the trailing 30-day average), or outbound activity outside the customer's normal business hours.
- **Short call durations:** a high proportion of very short calls (for example, average duration under 15 seconds across a significant volume of calls).
- **Low completion rates:** elevated rates of failed, unanswered, or rejected calls, including calls to invalid, unallocated, or disconnected numbers.
- **Sequential or patterned dialing:** calls placed to sequential or near-sequential numbers, or a single caller ID placing calls to large numbers of unique destinations.
- **Caller ID anomalies:** any attempt to present an unauthorized, invalid, or unassigned calling number.
- **Unusual destinations:** calls to international, premium-rate, or high-cost destinations inconsistent with the customer's documented use.
- **External notices:** complaints, carrier fraud alerts, call-labeling notices, or any notice from the FCC, law enforcement, or the ITG.

6.3 Response Procedures

When suspicious activity is identified, Junxionet will: (1) open a documented ticket in its ticketing system; (2) investigate the affected system and traffic; (3) where illegal or unauthorized traffic is probable, immediately suspend the affected outbound calling, credentials, or trunk; (4) contact the customer's authorized representative; and (5) restore service only after the cause is resolved and the customer has confirmed compliance with its service agreement. Customers found to be knowingly originating illegal robocalls are terminated.

Junxionet will also comply with any Notice of Suspected Illegal Traffic issued by the FCC's Enforcement Bureau under 47 CFR § 64.1200(n), including promptly investigating the identified traffic, taking required steps to effectively mitigate it, and reporting the results to the Enforcement Bureau within the required timeframe.

7. Know Your Upstream and Downstream Providers

Junxionet does not accept voice traffic from other providers for onward routing. Junxionet routes customer traffic only through underlying carriers that (a) are listed in the FCC Robocall Mitigation Database with an active certification, (b) have contractually committed to comply with applicable robocall mitigation and caller ID authentication rules, and (c) respond to traceback requests. Junxionet verifies each carrier's Robocall Mitigation Database listing before beginning service and at least quarterly thereafter, and will cease routing traffic through any carrier whose certification is removed from the database.

8. 24-Hour Traceback Commitment

Junxionet LLC commits to respond fully and within 24 hours to all traceback requests from the Federal Communications Commission, law enforcement agencies, and the industry traceback consortium (the Industry Traceback Group), and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

To meet this commitment, Junxionet will:

- Maintain a designated Robocall Mitigation Contact (Section 10) and monitor support@junxionet.net and (303) 276-7090 for traceback requests, with a backup contact designated when the primary contact is unavailable.
- Maintain an active registration with the ITG traceback portal and respond through the portal or by the method the requesting entity specifies.
- Within 24 hours of receipt, identify the customer that originated the traced call using CDRs and account records, and provide the requesting entity with the source information requested.
- Retain call detail records for no less than twelve (12) months to support traceback investigations.
- Investigate the identified customer, take the actions described in Section 6.3, and report the outcome to the requesting entity on request.

9. Program Administration and Compliance

- **Accountability.** The Chief Operating Officer is responsible for administering this Plan and handling robocall mitigation matters. Customer KYC approvals and exceptions may be granted by any C-suite officer.
- **Training.** All personnel who provision or support customer voice services are trained on this Plan at onboarding and annually.
- **Database accuracy.** Junxionet will update its Robocall Mitigation Database certification and CORES registration within ten (10) business days of any change in the information they contain, and will complete annual recertification by March 1 of each year.
- **Plan review.** This Plan is reviewed at least annually and whenever Junxionet's services, network, carriers, or role in the call chain change, or the governing rules change.
- **Records.** Customer verification records, investigation tickets, and traceback responses are retained for at least two (2) years.

10. Robocall Mitigation Contact

Jayson Owens, Chief Operating Officer, Operations

Junxionet LLC, 8673E Dry Creek Rd, Unit 1012, Centennial, CO 80112

Telephone: (303) 276-7090 | Email: support@junxionet.net

11. Officer Certification

I certify that I am an officer of Junxionet LLC, that I am authorized to make this certification on its behalf, that all calls Junxionet originates are subject to this Robocall Mitigation Plan, and that the information in this Plan is true and correct to the best of my knowledge.

_____ _____

Jayson Owens
Chief Operating Officer, Junxionet LLC

Date: October 22, 2026