

COMPLIANCE CONTROL DOCUMENT

RMD Plan, KYC Onboarding and Traceback Rules

NebulaNectar Networks, LLC

RMD / ROBOCALL MITIGATION

CUSTOMER KYC

TRACEBACK RESPONSE

Company profile	Details
Business name	NebulaNectar Networks, LLC
Status	Active
Initial filing date	September 25, 2023
Entity type	Domestic Limited Liability Company
Entity sub-type	Domestic LLC
Formed in	New Mexico
Record number	7375166
Registered agent	NORTHWEST REGISTERED AGENT LLC
Agent address	1209 Mountain Road PL NE, STE N, Albuquerque, NM 87110
CEO / authorized officer	Manash Gupta
CEO email	manash@nebulanectar.network
Rates contact	rates@nebulanectar.network
NOC contact	noc@nebulanectar.network
Billing contact	billing@nebulanectar.network
Legal contact	manash@nebulanectar.network
Telephone	833-330-6249
EIN	42-1938254

Document purpose: establish a repeatable, auditable process for preventing illegal robocall traffic, screening customers and upstream providers, preserving traceback evidence, and responding to regulators, law enforcement, and industry traceback requests.

1. Executive Summary

NebulaNectar Networks, LLC is adopting this control plan for its U.S. telecommunications activities. The plan is designed for use in the FCC Robocall Mitigation Database (RMD), customer onboarding, upstream-carrier onboarding, and traceback response. It applies to officers, employees, contractors, vendors, and any business unit involved in selling, provisioning, routing, monitoring, or supporting voice services.

The plan has three connected controls:

- RMD and robocall mitigation: identify the company's role in the call path, prevent illegal traffic, document controls, and keep the RMD filing accurate.
- KYC onboarding: verify the legal identity, ownership, authority, business purpose, traffic profile, caller-ID rights, and compliance posture of every customer and relevant upstream provider.
- Traceback response: preserve records, identify the customer and route, respond through official channels, and take proportionate corrective action without deleting or altering evidence.

Important filing condition: The RMD language in this document assumes NebulaNectar Networks, LLC is a non-facilities-based reseller that does not control the network infrastructure necessary to implement STIR/SHAKEN. If the company operates an originating switch, controls call authentication facilities, originates calls on its own network, or later changes its network model, the RMD position must be reviewed and revised before filing or continuing to rely on the limitation.

This document is an operational compliance policy and is not a substitute for legal advice. The CEO or designated compliance officer must verify that each factual statement is true before submitting it to the FCC or a carrier.

2. RMD and Robocall Mitigation Plan

2.1 Regulatory position

NebulaNectar Networks, LLC will maintain an RMD filing and an appropriate robocall mitigation program. The company will not treat an implementation limitation as an exemption from RMD filing, customer due diligence, mitigation, recordkeeping, or traceback cooperation.

If the operational facts are accurate, the company may describe its STIR/SHAKEN position as follows:

NebulaNectar Networks, LLC is a non-facilities-based telecommunications reseller and does not own or control the network infrastructure necessary to implement STIR/SHAKEN on the underlying voice network. The company obtains voice capacity from upstream facilities-based providers that control the relevant SIP infrastructure, signing systems, and applicable Service Provider Code (SPC) token. Therefore, NebulaNectar Networks, LLC is relying on the lack-of-control basis described in 47 C.F.R. § 64.6305(d)(2)(i). This position is limited to STIR/SHAKEN implementation; it does not eliminate the company's RMD filing or robocall-mitigation obligations.

The company must maintain documentation supporting this position, including its network diagram, carrier agreements, routing model, evidence of which party controls call authentication, and any applicable carrier attestations. If the company becomes facilities-based or obtains control over signing infrastructure, it must reassess this position immediately.

2.2 Governance and accountability

Function	Primary accountability	Minimum responsibility
CEO / authorized officer	Manash Gupta	Approve the policy, certify accurate filings, allocate resources, and approve high-risk exceptions.
Compliance owner	Designated by CEO	Maintain RMD filing, KYC files, risk decisions, training, audits, and regulatory communications.
NOC / technical operations	Designated technical lead	Monitor traffic, preserve CDR/SIP data, enforce blocks, validate routes, and support tracebacks.
Customer operations	Designated account owner	Collect KYC documents, verify use cases, maintain customer contacts, and enforce contract controls.
Legal contact	manash@nebulanectar.network	Receive legal/regulatory notices and coordinate formal responses.

2.3 Preventive controls

- 1 Accept traffic only from upstream providers whose business identity, RMD status where applicable, contact information, routing authority, and compliance posture have been reviewed.
- 2 Accept customers only after the KYC process in Section 3 is completed, the service agreement is signed, the intended traffic is approved, and the customer has supplied an emergency and compliance contact.
- 3 Require customers to use lawful caller-ID information and to maintain the right to use every displayed number. Prohibit spoofing, impersonation, misleading caller-ID, and traffic designed to evade analytics or carrier controls.
- 4 Prohibit illegal or deceptive campaigns, including impersonation of government agencies, banks, insurers, technology companies, law enforcement, delivery services, or other trusted brands; account takeover; payment fraud; and campaigns that materially misrepresent the purpose of a call.
- 5 Use network controls appropriate to the service, including rate and CPS limits, concurrent-channel limits, destination controls, abnormal-volume alerts, caller-ID velocity checks, complaint review, and blocking or quarantine procedures.
- 6 Maintain a documented escalation path for suspected fraud, high complaint rates, unusual answer-seizure patterns, invalid caller-ID, repeated short-duration traffic, unexplained traffic spikes, or customer refusal to provide source details.

2.4 Ongoing monitoring and records

- Retain customer, route, carrier, account, CDR, SIP, authentication, complaint, block, and traceback records for the period required by contract, applicable law, or the company's retention schedule. Do not delete records relevant to an open investigation.
- Review traffic at onboarding, after material changes, on a risk-based periodic schedule, and whenever complaints, traceback requests, carrier warnings, or abnormal analytics indicate elevated risk.
- Maintain an RMD change log. Update the RMD filing promptly and no later than the FCC-required update window after a change to required filing information.
- Use access controls, audit logs, backups, and least-privilege permissions for compliance and network records.

2.5 Prohibited conduct

Prohibited conduct	Required action
Submitting false, incomplete, or misleading RMD or KYC information	Reject, correct, document the decision, and escalate to the CEO / compliance owner.

Prohibited conduct	Required action
Accepting traffic from an unapproved or unverified source	Quarantine or block the traffic pending review; preserve evidence.
Allowing a customer to rotate numbers to avoid complaints or traceback	Suspend the affected service and investigate all related numbers and accounts.
Coaching a customer to conceal the true source or campaign purpose	Terminate the account or relationship and preserve the communication record.
Ignoring an official traceback request or knowingly delaying a response	Escalate immediately; respond within the internal 24-hour target.

3. Customer KYC Onboarding Rules

3.1 Onboarding principle

No customer may be provisioned for U.S. voice service until NebulaNectar Networks, LLC has identified the customer, verified the business purpose, assessed the traffic risk, confirmed the customer's authority to use caller-ID resources, and obtained a signed agreement containing compliance, audit, suspension, and traceback obligations.

3.2 Required onboarding package

Category	Required information or document
Legal identity	Legal entity name, DBA names, formation jurisdiction, formation date, state/entity ID, EIN or tax documentation, principal and mailing addresses.
Ownership and control	CEO or authorized officer, directors/managers, beneficial owners, ownership percentages, government-issued identification where appropriate, and authority to sign.
Telecom identifiers	FCC FRN, RMD filing number, OCN, 499A/499Q information, section 214 information where applicable, carrier or reseller status, and upstream-provider details.
Business profile	Website, business email, phone, business description, customer type, operating countries, physical operating location, and expected monthly spend.
Traffic profile	Originating countries, destination, campaign type, conversational or dialer use, expected ACD, ASR, CPS, channels, daily/monthly minutes, and calling hours.
Caller-ID authority	DID inventory or source, proof of authorization to display the numbers, attestation expectations, and process for validating customer-owned numbers.
Compliance controls	DNC process, consent process, complaint handling, internal fraud controls, STIR/SHAKEN status, RMD plan, traceback contact, and 24-hour contact number.
Commercial records	Signed MSA/order form, pricing and billing terms, payment method, credit information if applicable, and authorized technical contacts.

3.3 Verification procedure

- 1 Create a unique customer record and assign an onboarding owner. Record the date received, reviewer, source of each document, and any missing item.
- 2 Compare the legal name, address, state record, EIN, website, email domain, phone number, officer, and payment information for consistency. Investigate material discrepancies before approval.
- 3 Verify that the customer is authorized to use the proposed DIDs, caller-ID numbers, brand names, campaign scripts, and traffic source. Reject unverifiable or third-party claims.

- 4 Assess whether the customer is an enterprise end user, reseller, wholesaler, dialer, lead generator, call center, or other intermediary. Require additional downstream and source information for intermediaries.
- 5 Review the traffic profile for consistency with the requested product. A customer requesting conversational service but describing mass autodialing, prerecorded messages, or high-volume short-duration traffic must be escalated before approval.
- 6 Perform a risk decision: approve, approve with conditions, hold for clarification, or reject. Record the reason and any conditions, including initial limits, test periods, or restricted destinations.
- 7 Provision only after the agreement, KYC package, risk decision, and technical approval are complete. Retain the full approval record in the customer file.

3.4 Risk tiers and review frequency

Tier	Typical indicators	Controls and review
Standard	Known business, consistent documents, clear use case, moderate volume, direct enterprise or established carrier relationship.	Approve after normal KYC. Review at least annually and upon material change.
Elevated	New entity, reseller/intermediary, high CPS or channels, unclear caller-ID authority, unusual campaign, cross-border source, or incomplete history.	Enhanced documents, staged testing, lower initial limits, senior approval, and quarterly review.
Prohibited / unacceptable	Impersonation, fraud indicators, unverifiable identity, refusal to disclose source, false documents, illegal campaign, repeated complaints, or traceback non-cooperation.	Reject or suspend. Do not provision or restore service without documented remediation and executive approval.

3.5 Contractual onboarding requirements

- Customer warrants that it will use the service only for lawful communications and will not transmit illegal robocalls, spoofed caller-ID, deceptive traffic, or traffic that violates applicable federal or state law.
- Customer must maintain accurate KYC information and notify NebulaNectar Networks, LLC of material changes before using the service under the changed facts.
- Customer must respond promptly to source, script, consent, caller-ID, and traceback inquiries and must identify the actual end user or campaign owner when requested.
- NebulaNectar Networks, LLC may rate-limit, quarantine, block, suspend, or terminate traffic or service when necessary to protect consumers, the network, upstream providers, or regulatory compliance.
- Customer must not transfer, resell, or sub-allocate service unless the agreement expressly permits it and the downstream relationship is disclosed and approved.

4. Traceback Response Rules

4.1 Objective and service level

NebulaNectar Networks, LLC will maintain a documented process to respond to traceback requests from the FCC, law enforcement, the Industry Traceback Group or its designated consortium, upstream carriers, and other authorized compliance partners. The internal target is to acknowledge a request within four hours and provide a complete, accurate response within 24 hours, or sooner if the request specifies an earlier deadline.

A traceback request is a compliance event, not an accusation by itself. The company must cooperate, preserve evidence, avoid speculation, and provide verified facts. A request must never be ignored because the call was not originated directly by the company or because the company relies on an upstream carrier.

4.2 Intake and triage

Step	Rule	Target
1. Receive	Accept requests through official email, portal, ticket, or other verified channel. Confirm sender identity and preserve the original request.	Immediate
2. Log	Create a unique ticket. Record receiving time, deadline, requesting entity, telephone number, date/time, originating number, called number, and all attachments.	Within 1 hour
3. Assign	Assign a compliance owner and technical investigator. Notify the CEO or designated escalation contact for high-risk matters.	Within 2 hours
4. Acknowledge	Confirm receipt and provide the company ticket number, responsible contact, and expected response timing.	Within 4 hours
5. Investigate	Trace the call through customer, account, DID, IP, SIP headers, CDR, route, carrier, and downstream records. Identify the closest responsible source supported by evidence.	Same business day
6. Respond	Provide complete and accurate information, identify any uncertainty, and state corrective action taken or pending. Never alter records to fit a requested conclusion.	Within 24 hours
7. Close	Document final status, blocks, suspension, customer notification, upstream notification, evidence location, and any follow-up monitoring.	After response

4.3 Minimum evidence to preserve and review

- Customer legal name, account ID, authorized contacts, KYC file, MSA, order form, and current risk tier.
- Calling number, called number, date/time with time zone, call duration, disposition, account, campaign, DID assignment, and route.
- CDR, SIP signaling, ingress and egress IP addresses, trunk information, user agent, asserted and preferred identity fields, diversion or forwarding information, and authentication data available to the company.
- Upstream carrier, reseller, dialer, end-user, or downstream provider associated with the call; include the communication path and relevant contact information.
- Customer script, campaign description, consent or lead source information, complaint history, prior blocks, analytics alerts, and any related numbers or accounts.
- Emails, tickets, portal messages, attachments, screenshots, carrier notices, and the final response. Preserve originals and maintain a chain-of-custody note for exported records.

4.4 Corrective action matrix

Finding	Minimum action
Unable to identify the customer or source	Place traffic on hold, escalate to the upstream carrier, preserve records, and do not restore until identity is verified.
Credible fraud, impersonation, or illegal robocall evidence	Immediately block affected numbers and traffic, suspend the responsible account where appropriate, notify the compliance owner, and document the action.
Customer explanation is incomplete or inconsistent	Request source details, script, consent, and caller-ID authority. Maintain restrictions until resolved.
Upstream carrier or customer caused the issue and cooperates	Apply a documented remediation plan, monitor traffic, and retain the incident in the customer/carrier file.
Repeated event, refusal to cooperate, or false information	Terminate or permanently block the relationship unless executive approval documents a lawful and effective remediation basis.

4.5 Communication rules

- Use the official company legal or compliance contact for regulator, law-enforcement, and traceback communications. Do not send sensitive records from an unapproved personal account.
- Respond with facts supported by records. If information is unavailable, say so and describe the steps taken to obtain it. Do not guess, conceal, or attribute responsibility without evidence.
- Do not instruct any customer or vendor to deny a relationship, conceal a source, alter records, or avoid a traceback request. Escalate any such request as a compliance incident.
- Keep a copy of the final response, attachments, delivery confirmation, and any subsequent request for clarification in the ticket.

5. Incident Management, Training, and Audit

5.1 Incident severity

Severity	Examples	Escalation
Critical	Government or financial impersonation, active fraud, widespread spoofing, customer refuses traceback, or credible threat to continued carrier access.	Immediate CEO/compliance/NOC escalation; suspend or block affected traffic; external response within 24 hours.
High	Multiple complaints, repeated invalid caller-ID, abnormal traffic spike, serious KYC discrepancy, or carrier warning.	Same-day investigation; enhanced monitoring and documented management decision.
Moderate	Single complaint with no confirmed violation, missing document, minor traffic deviation, or isolated technical anomaly.	Ticket, corrective action, and review before normal limits are restored.

5.2 Training

Relevant employees and contractors must receive training before receiving access to customer provisioning, routing, monitoring, or traceback systems and at least annually thereafter. Training must cover:

- Recognizing impersonation, spoofing, account takeover, high-risk campaigns, and suspicious customer behavior.
- KYC documentation standards, red flags, approval authority, and prohibited shortcuts.
- RMD filing accuracy, STIR/SHAKEN role classification, carrier obligations, and the company's documented operational position.

- Traceback intake, evidence preservation, response timelines, confidentiality, and escalation.
- Use of network blocks, rate limits, monitoring tools, access controls, and incident tickets.

5.3 Audit and review checklist

Control area	Audit question
RMD accuracy	Do the company name, address, contact, role, implementation status, OCN/FRN information, and mitigation description remain accurate?
Network basis	Does the evidence still support the company's stated lack of control over STIR/SHAKEN infrastructure, if that position is used?
Customer files	Are KYC documents, ownership, business purpose, traffic profile, caller-ID authority, and signed terms complete and current?
Monitoring	Are limits, alerts, complaints, blocks, route changes, and abnormal traffic reviewed and documented?
Tracebacks	Were requests acknowledged, investigated, answered, and closed within the internal target?
Remediation	Are suspended or terminated accounts prevented from returning through related entities, numbers, or undisclosed downstreams?

5.4 Change management

The compliance owner must review this plan before launching a new product, adding a new call path, acquiring or controlling network infrastructure, accepting a new class of customer, materially changing traffic profiles, or receiving a regulatory or carrier notice. The RMD filing and customer controls must be updated when the underlying facts change.

6. Regulatory References and Management Attestation

6.1 Primary references

The following sources should be reviewed against the current FCC rules before each material filing update:

- [1] Federal Communications Commission, Call Authentication Trust Anchor, Sixth Report and Order, 88 FR 40096 (June 21, 2023), including RMD certification, mitigation-plan, STIR/SHAKEN extension, and lack-of-control explanation requirements.
- [2] Federal Communications Commission, Improving the Effectiveness of the Robocall Mitigation Database; Amendment of CORES Registration System, 89 FR 74184 (September 12, 2024), including the broad requirement for providers carrying or processing voice traffic to maintain accurate RMD filings and mitigation plans.
- [3] 47 C.F.R. § 64.6305, Robocall mitigation and certification.
- [4] 47 C.F.R. § 64.6304, Extension of implementation deadline.
- [5] 47 C.F.R. § 64.1200(n), provider obligations concerning robocall mitigation, customer information, and upstream-provider procedures.
- [6] FCC Robocall Mitigation Database information page and filing resources.

Reference	URL
FCC Call Authentication Trust Anchor	https://www.federalregister.gov/documents/2023/06/21/2023-12142/call-auth-entification-trust-anchor
FCC RMD effectiveness proceeding	https://www.federalregister.gov/documents/2024/09/12/2024-20176/improvin-g-the-effectiveness-of-the-robocall-mitigation-database-amendment-of-cores-r-egistration
FCC RMD information page	https://www.fcc.gov/robocall-mitigation-database

6.2 Management attestation

By approving this plan, NebulaNectar Networks, LLC's authorized officer confirms that the company will maintain reasonable controls to avoid originating, carrying, or processing illegal robocall traffic; will keep its RMD information accurate; will cooperate with official traceback requests; and will review the factual basis of any STIR/SHAKEN implementation limitation before relying on it.

Authorized officer	Manash Gupta
Company	NebulaNectar Networks, LLC
Signature	_____
Date	_____

Operational reminder: This plan should be maintained with the company's current carrier list, network diagram, customer KYC checklist, traceback ticket template, suspension matrix, and RMD filing confirmation.