

ClearWave Nexus, LLC.

1. Company Identification and Filing Information

This Robocall Mitigation Plan (the “Plan”) is submitted by Clearwave Nexus (the “Company,” “we,” “us,” or “our”) to the Federal Communications Commission (“FCC”) for inclusion in the Robocall Mitigation Database (“RMDB”) maintained under 47 C.F.R. § 64.6305. The Company certifies that it has implemented the STIR/SHAKEN authentication framework where technically feasible and has otherwise instituted an effective robocall mitigation program designed to prevent the origination of illegal robocalls on its network.

Legal Entity Name	Clearwave Nexus
Doing Business As (DBA)	Clearwave Nexus
Principal Business Address	600 17th Street, Suite 2800, Denver, CO 80202, United States
Main Telephone Number	1-800-832-5594
Website	https://clearwavenexus.net
Primary Compliance Contact	Andrew Collins, Chief Compliance Officer
Compliance Contact Email	Inquire@clearwavenexus.net
Secondary Contact Email	Andrew.c@clearwavenexus.net
Traceback / Law Enforcement Email	Inquire@clearwavenexus.net
Provider Category (47 CFR § 64.6300)	Voice Service Provider / Intermediate Provider
RMDB Filing Type	Robocall Mitigation Plan and STIR/SHAKEN Certification

2. Executive Summary

Clearwave Nexus is committed to safeguarding the integrity of the United States voice network and protecting consumers from illegal robocalls, spoofed caller ID, and other forms of telephone-based fraud. Consistent with the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (“TRACED Act”), the FCC’s implementing rules at 47 C.F.R. §§ 64.6300–64.6308, and the

industry best practices established by ATIS, NANC, the Industry Traceback Group (“ITG”), and STI-GA, the Company has adopted, implemented, and maintains the comprehensive program described in this Plan.

This Plan describes: (a) the Company’s deployment of STIR/SHAKEN call authentication technology; (b) the non-STIR/SHAKEN mitigation measures the Company employs across all portions of its network where STIR/SHAKEN cannot yet be applied; (c) the Company’s Know-Your-Customer (“KYC”), Know-Your-Upstream-Provider (“KYUP”) and traffic-vetting procedures; (d) the Company’s cooperation with the FCC, FTC, state attorneys general, law enforcement, and the ITG; and (e) the Company’s internal governance, training, recordkeeping, and continuous-improvement obligations.

The Company affirms, as required by 47 C.F.R. § 64.6305(b)(2) and (c)(2), that it will take responsibility for any calls it originates on its network and will cooperate fully in tracing back the origin of suspected illegal robocalls.

3. Scope and Definitions

3.1 Scope

This Plan applies to all voice traffic that Clearwave Nexus originates, carries, terminates, or otherwise handles, including but not limited to interconnected VoIP service, one-way VoIP service, wholesale origination services, transit/intermediate services, and any traffic exchanged with domestic or foreign providers via SIP or TDM interconnection.

3.2 Definitions

- “STIR/SHAKEN” means the Secure Telephone Identity Revisited / Signature-based Handling of Asserted information using toKENs authentication framework standardized by ATIS-1000074, ATIS-1000080, and related specifications.
- “Illegal robocall” means any call that violates the Telephone Consumer Protection Act (47 U.S.C. § 227), the Truth in Caller ID Act (47 U.S.C. § 227(e)), the Telemarketing Sales Rule (16 C.F.R. Part 310), or any other applicable federal or state law.
- “ITG” means the Industry Traceback Group, the consortium registered with the FCC pursuant to 47 C.F.R. § 64.1200(n)(2) as the official traceback consortium.
- “KYC” means Know-Your-Customer due-diligence procedures designed to verify the identity, legitimacy, and lawful intent of each customer that originates voice traffic on the Company’s network.
- “KYUP” means Know-Your-Upstream-Provider due-diligence procedures applied to all upstream voice providers from which the Company accepts traffic.
- “STI-CA / STI-PA” means the Secure Telephone Identity Certification Authority and Policy Administrator, currently operated by iconectiv, LLC under contract with STI-GA.

4. STIR/SHAKEN Implementation

4.1 Implementation Status

Clearwave Nexus has completed full STIR/SHAKEN deployment in the Internet Protocol (“IP”) portions of its voice network in accordance with 47 C.F.R. § 64.6301. The Company is registered with the STI Policy Administrator (“STI-PA”), has been issued a Service Provider Code (“SPC”) token, and obtains and rotates STI certificates from an approved STI Certification Authority. The Company signs originating calls and verifies terminating calls using a production-grade Signing/Verification Service (“STI-AS/STI-VS”) integrated with its session border controllers and softswitch platform.

4.2 Attestation Methodology

Consistent with ATIS-1000074 and the STI-GA Token Access Policy, the Company applies the following attestation levels:

- Full Attestation (“A”): assigned when Clearwave Nexus (i) is the originating service provider, (ii) has a direct authenticated relationship with the customer placing the call, and (iii) has established a verified association between the customer and the specific telephone number used as the calling party.
- Partial Attestation (“B”): assigned when the Company is the originating service provider and has a direct authenticated relationship with the customer, but cannot verify the customer’s right to use the specific calling number (e.g., where the customer brings its own DID range).
- Gateway Attestation (“C”): assigned when the Company is the entry point of the call into its IP network from another carrier (including international or TDM-originated traffic) and cannot verify the call’s origin.

The Company never applies an attestation higher than the level supported by its actual KYC data. Misuse of A-level attestation is grounds for immediate termination of the originating customer under Section 7 of this Plan.

4.3 Calling Number Verification (Number Vetting)

Before assigning Full Attestation, Clearwave Nexus verifies the calling party number against the following authoritative sources, as applicable: (i) numbers directly allocated to the Company by the North American Numbering Plan Administrator (“NANPA”) or Pooling Administrator and assigned to a verified customer; (ii) numbers ported into the Company’s network via an authenticated LOA and a successful LNP port; (iii) numbers leased or sub-allocated to the Company under a written agreement with the responsible organization. Bring-Your-Own-Carrier (“BYOC”) numbers receive at most B-level attestation absent independent verification through an authoritative source such as a Letter of Authorization plus carrier confirmation, or a Delegated Certificate under ATIS-1000092.

4.4 STI Certificates and Key Management

- Certificates are obtained from an STI-PA-approved STI-CA and renewed prior to expiration.
- Private signing keys are stored in FIPS 140-2/140-3 validated hardware security modules (HSMs) or in equivalently protected key vaults with strict role-based access control and audit logging.
- SPC tokens are refreshed in accordance with STI-PA policy and the Company's Trust Anchor list is automatically updated.
- Key rotation, revocation, and incident-response procedures are documented in the Company's internal STIR/SHAKEN Operations Runbook and tested at least annually.

4.5 Verification on Terminating Calls

For traffic terminated on the Company's network, the STI-VS validates each received SIP Identity header, checks the certificate chain to the STI-PA Trust Anchor, evaluates the attestation level and origination identifier ("OrigID"), and produces a "verstat" outcome (TN-Validation-Passed, TN-Validation-Failed, or No-TN-Validation). Results are: (a) logged for traceback support; (b) made available to downstream analytics, blocking, and labeling partners; and (c) preserved for at least 24 months.

4.6 Non-IP Portions of the Network

To the extent any portion of the Company's network remains non-IP, the Company qualifies for, and operates consistent with, the extension under 47 C.F.R. § 64.6304. For such non-IP segments, the Company: (i) maintains and follows the robocall mitigation program described in Section 5 below; (ii) is actively working to upgrade those segments to IP or to implement an approved out-of-band STIR/SHAKEN solution (e.g., ATIS-1000096) as a Caller ID Authentication framework working group solution becomes commercially available; and (iii) tracks and reports its non-IP traffic volumes and conversion milestones to senior management on a quarterly basis.

4.7 Foreign-Originated and Gateway Traffic

For any traffic the Company accepts as a Gateway Provider as defined in 47 C.F.R. § 64.6300(g), the Company complies with all gateway-provider obligations including (i) authenticating unauthenticated foreign-originated calls bearing North American Numbering Plan numbers within the Company's IP network, (ii) responding to traceback requests from the ITG within 24 hours, (iii) blocking traffic when required by an FCC Enforcement Bureau notice, and (iv) maintaining and submitting an updated certification to the RMDB reflecting its gateway-provider status.

5. Robocall Mitigation Program (Non-STIR/SHAKEN Measures)

In addition to STIR/SHAKEN, Clearwave Nexus maintains a layered, defense-in-depth robocall mitigation program. The elements below collectively constitute the Company's "robocall mitigation program" as required by 47 C.F.R. § 64.6305(a)(1) and (b)(1).

5.1 Know-Your-Customer (KYC) Procedures

Before activating service for any new originating customer, the Company performs and documents the following due-diligence steps:

1. Collect and verify legal entity information, including legal name, jurisdiction of formation, business address, EIN/Tax ID, and articles of incorporation or equivalent.
2. Collect and verify beneficial-ownership information for any individual owning 25% or more of the customer, including government-issued identification.
3. Verify the identity of the principal contact via independent means (e.g., callback to a publicly listed number, video verification, or notarized attestation).
4. Screen the customer, its principals, and beneficial owners against the OFAC Specially Designated Nationals list, the FCC's public lists of providers removed from the RMDB, and the ITG's list of known bad actors.
5. Require the customer to describe, in writing, the use case for the voice service, projected call volume, average call duration, anticipated calling pattern (inbound vs. outbound), dialing technology, and source of consent for any outbound campaigns.
6. Require the customer to provide a written attestation that it will comply with the TCPA, Truth in Caller ID Act, TSR, and all applicable state telemarketing laws, and that it will not originate or transmit illegal robocalls.
7. Document, retain, and re-verify all KYC information at least every twelve (12) months or upon any material change in the customer's ownership, use case, or traffic profile.

5.2 Know-Your-Upstream-Provider (KYUP) Procedures

Before accepting traffic from any upstream voice provider, the Company verifies that the provider: (i) is listed in good standing in the FCC RMDB; (ii) has filed an appropriate STIR/SHAKEN certification and robocall mitigation plan; (iii) has not been the subject of an FCC Enforcement Bureau "mandatory blocking" notice under 47 C.F.R. § 64.1200(k)(4); and (iv) executes a written interconnection agreement that incorporates the robocall mitigation, traceback, and indemnification provisions referenced in Section 8 of this Plan.

5.3 Customer Contract Provisions

All customer contracts include, at a minimum: (a) a prohibition on the origination or transmission of illegal robocalls, spoofed caller ID used to defraud or harm, or calls in violation of the TCPA, TSR, or Truth in Caller ID Act; (b) a representation that the customer has obtained all consents required under the TCPA and TSR; (c) the Company's right to suspend or terminate service immediately upon a reasonable, good-faith belief that the customer is originating illegal traffic; (d) cooperation obligations for traceback requests; and (e) indemnification of the Company against losses arising from the customer's violation of these provisions.

5.4 Traffic Analytics and Monitoring

- Continuous, automated monitoring of call detail records (CDRs) and SIP signaling for indicators of illegal robocalling, including but not limited to: short-duration call ratios, average completion rate (ACR) anomalies, high call-attempt rates from a single endpoint, repeated calls to the same destination, calling-number rotation patterns, neighbor-spoofing patterns, FCC “Do-Not-Originate” (DNO) list hits, and invalid, unallocated, or unassigned calling numbers.
- Use of commercially recognized analytics platforms and reputation data, including risk scoring of originating customers, to flag anomalous behavior.
- Automated alerting to the Network Operations Center and Compliance team upon detection of suspicious patterns, with documented escalation procedures.
- Periodic (no less than quarterly) review of analytics rule sets to incorporate new robocall typologies and FCC/FTC consumer-complaint trends.

5.5 Call Blocking and Number Validation

- The Company blocks calls purporting to originate from numbers that are invalid, unallocated, unassigned, or appear on the FCC-administered or customer-provided Do-Not-Originate list, consistent with 47 C.F.R. § 64.1200(k)(1)–(3).
- The Company blocks calls upon receipt of a written notification from the FCC Enforcement Bureau under 47 C.F.R. § 64.1200(k)(4) directing the Company to block the identified traffic, and submits the required certification of compliance within the timeframe specified by the FCC.
- Where the Company offers analytics-based blocking to its subscribers, it does so on an opt-out or opt-in basis as permitted by 47 C.F.R. § 64.1200(k)(3), with transparent disclosure, a no-charge mechanism, and a clearly documented process for redress under 47 C.F.R. § 64.1200(k)(11).

5.6 Suspension and Termination of Bad Actors

Upon a reasonable, good-faith determination that a customer is originating, or has originated, illegal robocall traffic, the Company will (i) issue a notice to cure; (ii) if the customer fails to cure within a commercially reasonable period not to exceed 48 hours, or if the violation is severe or repeated, suspend all originating service; (iii) terminate the customer; and (iv) preserve all related CDRs and KYC records for a minimum of 24 months. Where required by FCC rule or written notice, the Company will block all traffic from the offending customer regardless of the calling number.

6. Traceback Cooperation

Clearwave Nexus is a participating provider in good standing with the Industry Traceback Group, the official traceback consortium designated by the FCC under 47 C.F.R. § 64.1200(n)(2). The Company affirms its obligation under 47 C.F.R. § 64.1200(n)(1) to:

- Respond fully and in good faith to all traceback requests from the FCC, FTC, state attorneys general, and the ITG within 24 hours, or sooner if so requested.

- Identify the upstream provider or originating customer of the call, including any associated KYC records, CDR data, SIP headers, and STIR/SHAKEN PASSporT information.
- Take prompt mitigation action against any originating customer or upstream provider identified as the source of illegal robocall traffic, up to and including suspension and termination of service.
- Maintain a dedicated, monitored contact channel for traceback requests: Inquire@clearwavenexus.net and 1-800-832-5594, available during U.S. business hours with after-hours escalation.
- Retain CDRs, SIP signaling data, STIR/SHAKEN logs, and KYC records for a minimum of 24 months to support traceback and law enforcement requests.

7. Governance, Training, and Oversight

7.1 Responsible Officials

Andrew Collins, Chief Compliance Officer, is the senior officer accountable for the Company's robocall mitigation program and STIR/SHAKEN implementation, and is the Company's primary point of contact for the FCC, ITG, and law enforcement on all robocall-related matters. The Chief Compliance Officer reports directly to the Company's executive leadership and provides quarterly written updates on program performance, incidents, and remediation.

7.2 Written Policies and Procedures

The Company maintains written internal policies and procedures that operationalize this Plan, including a STIR/SHAKEN Operations Runbook, a KYC/KYUP Manual, a Traceback Response Playbook, a Blocking and DNO Procedure, and an Incident Response Plan. These documents are reviewed and updated no less than annually, and after any material change in law, FCC rule, or Company operations.

7.3 Training

- All Company personnel involved in customer onboarding, network operations, compliance, and customer support receive role-appropriate training on the TCPA, Truth in Caller ID Act, TSR, FCC robocall rules, STIR/SHAKEN attestation, and the Company's internal robocall mitigation procedures within 30 days of hire and at least annually thereafter.
- Training completion is tracked and audited by the Compliance team.

7.4 Audit, Recordkeeping, and Continuous Improvement

- Internal audits of the robocall mitigation program are conducted no less than annually. External audits or independent assessments are conducted at the discretion of the Chief Compliance Officer and when material changes occur.

- All KYC records, customer contracts, traceback responses, blocking notices, STIR/SHAKEN signing/verification logs, and CDRs are retained for a minimum of 24 months, or longer if required by applicable law or by a preservation request from law enforcement.
- The Company tracks key program metrics — including traceback response time, traceback-confirmed bad-actor terminations, attestation-level distribution, verstat outcomes, and consumer complaints — and uses those metrics to drive program improvements.

8. Cooperation with the FCC, Law Enforcement, and Industry

Clearwave Nexus will cooperate fully and in good faith with the FCC, the FTC, state attorneys general, federal and state law enforcement agencies, the ITG, STI-GA, STI-PA, and all other authorized governmental or industry bodies in any investigation, enforcement action, traceback, or rulemaking related to illegal robocalls or caller ID spoofing. The Company will respond to lawful process (subpoenas, civil investigative demands, court orders) in accordance with applicable law and within the timeframes required.

9. Certifications and Affirmations

Pursuant to 47 C.F.R. § 64.6305(b) and (c), Clearwave Nexus certifies and affirms as follows:

8. Clearwave Nexus has implemented the STIR/SHAKEN authentication framework in the IP portions of its network in accordance with 47 C.F.R. § 64.6301, and where any portion of its network is not yet capable of STIR/SHAKEN, the Company qualifies for an extension under 47 C.F.R. § 64.6304 and applies the robocall mitigation program described in this Plan to that traffic.
9. Clearwave Nexus has instituted a robocall mitigation program that is reasonably designed to ensure that it is not originating illegal robocall traffic, as described in Sections 4 through 7 of this Plan.
10. Clearwave Nexus is, and will remain, a participating provider in good standing with the Industry Traceback Group, and will respond fully and timely to all traceback requests.
11. Clearwave Nexus will take responsibility for any calls it originates on its network, and will promptly investigate, mitigate, and cooperate in the cessation of any illegal robocall traffic identified on its network.
12. All information contained in this Plan, and all information submitted by Clearwave Nexus to the Robocall Mitigation Database, is true and correct to the best knowledge of the undersigned officer.

10. Public Contact Information

Robocall Mitigation Contact	Andrew Collins, Chief Compliance Officer
------------------------------------	--

Mailing Address	Clearwave Nexus, 600 17th Street, Suite 2800, Denver, CO 80202
Telephone	1-800-832-5594
Email (Compliance / Traceback)	Inquire@clearwavenexus.net
Email (Executive Escalation)	Andrew.c@clearwavenexus.net
Website	https://clearwavenexus.net
Hours of Coverage	24/7 monitored inbox; live response during 8:00 a.m.–6:00 p.m. MT business days, with after-hours on-call escalation

11. Officer Attestation

I, Andrew Collins, in my capacity as Chief Compliance Officer of Clearwave Nexus, having authority to bind the Company, hereby certify under penalty of perjury that I have reviewed this Robocall Mitigation Plan and that the statements made herein are true, accurate, and complete to the best of my knowledge, information, and belief. I further certify that Clearwave Nexus has implemented the practices described herein and will continue to do so for as long as it is required to be listed in the Robocall Mitigation Database.



Andrew Collins

Chief Compliance Officer

Clearwave Nexus

Email: Andrew.c@clearwavenexus.net

Telephone: 1-800-832-5594

Date: 4/29/2026

Appendix A — Regulatory Authority and References

- 47 U.S.C. § 227 (Telephone Consumer Protection Act)
- 47 U.S.C. § 227(e) (Truth in Caller ID Act)
- Pallone-Thune TRACED Act, Pub. L. No. 116-105 (2019)
- 47 C.F.R. §§ 64.6300–64.6308 (Caller ID Authentication and Robocall Mitigation)
- 47 C.F.R. § 64.1200 (Restrictions on Telephone Solicitation; Call Blocking)
- 16 C.F.R. Part 310 (FTC Telemarketing Sales Rule)
- ATIS-1000074 — Signature-based Handling of Asserted information using toKENs (SHAKEN)
- ATIS-1000080 — Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management
- ATIS-1000092 — Delegated Certificates for STIR/SHAKEN
- ATIS-1000096 — STIR/SHAKEN Out-of-Band PASSport Transmission
- STI-GA Token Access Policy and STI-PA Operational Practices
- FCC Sixth Report and Order, FCC 22-37 (Gateway Provider Obligations)
- FCC Seventh Report and Order, FCC 23-18 (Closing the Gaps in STIR/SHAKEN)

Appendix B — Definitions of Attestation Levels

Attestation	Definition and KYC Standard
A — Full	Originating provider has a direct authenticated relationship with the customer AND has verified the customer's right to use the specific calling number.
B — Partial	Originating provider has a direct authenticated relationship with the customer but has NOT verified the customer's right to use the specific calling number.
C — Gateway	Provider is the point of entry into its IP network for a call from another carrier (including international or TDM origination) and cannot verify the call's origin or right to use the calling number.

Appendix C — Document Control

Version	Date	Summary of Change
1.0	May 11, 2026	Initial Robocall Mitigation Plan and STIR/SHAKEN certification adopted for filing with the FCC Robocall Mitigation Database.

End of Document.