

Coastal Redwood Networks

Robocall Mitigation Plan

Filing entity: Coastal Redwood Networks | **FRN:** 0033709890 | **OCN:** 709K

Date: April 2026 | **Website:** www.coastalredwood.net

I. Introduction and Provider Role

Coastal Redwood Networks ("Coastal Redwood" or "the Provider") is a U.S.-based communications service provider that carries and processes voice traffic between other providers. Coastal Redwood acts as a gateway provider, receiving traffic from foreign originating and intermediate providers at its U.S.-based facilities before transmitting downstream, and as a non-gateway intermediate provider for traffic exchanged between domestic providers. Coastal Redwood has a STIR/SHAKEN implementation obligation in both capacities and holds its own Service Provider Code (SPC) token and digital certificate.

Coastal Redwood is not a voice service provider or originating provider. Coastal Redwood does not furnish voice service to end users, does not assign telephone numbers to subscribers, and does not originate calls on behalf of end-user callers. Its customers are carriers and service providers, not end users.

This Robocall Mitigation Plan describes the specific reasonable steps Coastal Redwood has taken to avoid carrying or processing illegal robocall traffic, consistent with 47 CFR § 64.6305 and related Commission rules. Coastal Redwood commits to responding to all traceback requests from the Federal Communications Commission, law enforcement, and the Industry Traceback Group (ITG), and to cooperating fully with such entities in investigating and stopping illegal robocalling activity.

II. STIR/SHAKEN Implementation Status

Coastal Redwood has implemented STIR/SHAKEN authentication on the IP portions of its network. Coastal Redwood holds its own SPC token and digital certificate, registered with the STIR/SHAKEN Policy Administrator (iconectiv), obtained in summer 2023 and maintained in good standing since. All calls authenticated by Coastal Redwood are signed using Coastal Redwood's own certificate; Coastal Redwood does not sign calls using any third party's certificate, and Coastal Redwood does not enter into third-party authentication agreements under the framework established by the Eighth Report and Order.

Pass-Through of Upstream Signatures

When a call arrives already signed by an upstream provider holding its own STIR/SHAKEN certificate, Coastal Redwood passes the existing Identity header and signature through unchanged. Coastal Redwood does not strip, replace, or re-sign calls that already carry a valid upstream signature.

Attestation Policy

For calls that Coastal Redwood itself signs, attestation level is determined by the information available about the calling party and the status of telephone number ownership validation, consistent

with the criteria in ATIS-1000074 and the STI-GA guidance on improper attestation:

- **A-attestation (Full Attestation)** is applied when Coastal Redwood has completed its ownership validation process for the specific telephone number used in the call, the validation is within its 30-day validity window, and the party whose ownership was validated is the party for whom the call is being signed.
- **B-attestation (Partial Attestation)** is applied when Coastal Redwood has a direct authenticated relationship with the subscriber initiating the call, but does not have an in-window verified association with the specific telephone number being presented.
- **C-attestation (Gateway Attestation)** is applied when Coastal Redwood is signing a call for which it does not have a direct authenticated relationship with the subscriber initiating the call. This is the default attestation for gateway signing of foreign-originated traffic where Coastal Redwood's customer relationship is with the foreign carrier rather than the end-caller, and where telephone number ownership has not been independently validated. C-attestation is expressly contemplated by ATIS standards for gateway and intermediate providers signing previously-unsigned calls.

Telephone Number Ownership Validation

Ownership validation is performed via an automated call-and-code challenge-response process: Coastal Redwood places a call to the number under validation and requires the holder to enter a code proving control of the endpoint. A successful validation is maintained for 30 days, after which re-validation is required for continued A-attestation signing. Validations may be revoked at any time based on new information, including traceback findings or counter-claims of ownership.

Customers with large number inventories that cannot practically be validated through call-and-code are better served by holding their own STIR/SHAKEN certificate; in those cases their calls arrive at Coastal Redwood's network already signed and are passed through unchanged.

Handling of Unsigned Traffic

When a call arrives at Coastal Redwood's network unsigned and the customer does not hold its own STIR/SHAKEN certificate, Coastal Redwood applies the attestation level supported by the information available about the call and the calling party, per the policy above. This includes Coastal Redwood's obligations as a non-gateway intermediate provider with a STIR/SHAKEN implementation obligation under the Sixth Report and Order.

III. Customer Onboarding and Know-Your-Customer

Coastal Redwood conducts know-your-customer ("KYC") diligence on every new customer before provisioning service. KYC is performed with the goal of establishing a well-founded picture of the customer's legitimacy and intended use of the service; no single document satisfies verification, and the determination is based on the totality of available information and the degree of trust it supports.

Documentation Collected

At onboarding, Coastal Redwood collects the customer's legal entity name, business registration, business address, Employer Identification Number or Taxpayer Identification Number where applicable (foreign carriers without a U.S. TIN are an expected exception), government-issued

identification for responsible officers, company website information, and references from other carriers or industry contacts. Customers are required to certify that they are not the subject of any active Commission, law enforcement, or regulatory action related to illegal robocalling, spoofing, or deficient Robocall Mitigation Database filings.

Foreign Customers

Foreign customers are required to maintain a current filing in the FCC's Robocall Mitigation Database when they will send traffic using North American Numbering Plan caller ID through Coastal Redwood. Legitimacy is established through a combination of independently verifiable business information, reference checks with known industry contacts, and overall reputational footprint. New foreign entities lacking an established operating history are not onboarded.

Customer Obligations by Contract

Coastal Redwood's Master Services Agreement, Acceptable Use Policy, and Terms of Service require customers to:

- Attest to compliance with all laws and regulations applicable to their traffic, including but not limited to the Telephone Consumer Protection Act (and its Do-Not-Call and prior-express-consent provisions) where applicable, and analogous obligations under other regulatory regimes where the TCPA does not apply (for example, the Fair Debt Collection Practices Act for debt-collection traffic);
- Cooperate fully with any traceback request forwarded by Coastal Redwood, including timely identification of the originating party and cooperation with any resulting investigation;
- Perform their own know-your-customer diligence on their downstream customers as a condition of sending traffic into Coastal Redwood's network;
- Pass accurate caller ID information and refrain from stripping or altering signaling in ways that would interfere with downstream traceback or authentication;
- Refrain from originating or carrying illegal traffic of any kind.

Graduated Onboarding

New customers are onboarded with graduated capacity during an initial trust-building period. Volume limits start below the customer's projected steady-state capacity and are expanded as traffic patterns and traceback history are observed. The duration and steps of the ramp are set on a per-customer basis based on customer profile, reference quality, and declared use case.

IV. Know-Your-Upstream-Provider (Gateway Obligations)

In Coastal Redwood's gateway provider capacity, know-your-upstream-provider obligations are satisfied through a combination of contractual commitments, onboarding verification, and ongoing cooperation requirements, consistent with 47 CFR § 64.1200(n)(4).

Upstream clients are verified at onboarding against publicly available databases for regulatory flags, including the Commission's published list of de-listed and prohibited providers, the STI-GA's revoked-token list where applicable, and general business-legitimacy and reputational sources. Foreign upstream clients are required to maintain a current filing in the Robocall Mitigation Database

when sending traffic using NANP caller ID.

Upstream contracts require full cooperation with any traceback request Coastal Redwood forwards, pass-through of accurate caller ID and signaling information, and know-your-customer diligence on the upstream provider's own downstream customers. Violations of these contractual obligations are grounds for suspension or termination of the upstream relationship.

V. Traffic Monitoring and Analytics

Content Analysis for Voice Broadcast Traffic

For all customers whose traffic includes pre-recorded voice broadcast messages, Coastal Redwood requires that each distinct message be submitted to an internal analysis endpoint and verified before broadcast. The endpoint applies large-language-model-based content analysis to identify scam, fraud, and other indicators of illegal calling patterns. This approach replaced an earlier keyword-based system and has demonstrated improved detection of content that evades simple term matching. The analysis system is built and operated in-house. Verification is required once per distinct message; the same verified message may be reused across calls without re-verification until the message content changes.

Completion-Rate Monitoring

Coastal Redwood tracks call completion rates on a continuous basis, segmented by customer, caller ID, and media IP address. Degradation in completion rates — particularly patterns consistent with downstream carriers applying their own blocking — is treated as a signal requiring investigation. When such a signal is observed, calls may be rerouted across alternate wholesale carriers to isolate whether the cause is network-related or traffic-related, and the affected traffic is flagged for review to determine root cause.

This methodology benefits from the observation that recipients who answer a call and subsequently determine it to be fraudulent or unwanted often report it to their own provider, who in turn may begin blocking the traffic. Coastal Redwood's completion-rate monitoring captures the resulting downstream blocking as a signal, providing a practical mechanism to identify both illegal traffic and traffic that, while technically legal, has generated recipient complaints.

Capacity Controls

Traffic capacity is governed by port allocations across the network. These allocations serve both capacity management and mitigation purposes: traffic bursts that would exceed allocated capacity are rejected rather than carried, eliminating the risk of a customer using Coastal Redwood to push large volumes of illegal traffic before detection mechanisms can respond. This architectural constraint is considered a material element of the robocall mitigation posture.

Monitoring Cadence and Alert Review

Monitoring is conducted on a continuous, near-real-time basis with no batch-window delay in detection. Response is hybrid: automated responses include rerouting across alternate upstream carriers and flagging affected traffic for review; manual review is applied to determine root cause and to decide on further action, which may include customer notification, throttling, suspension, or termination.

VI. Call Blocking Procedures

Coastal Redwood blocks calls when: (a) information indicates the call is part of an illegal calling campaign identified by the Commission, the ITG, or law enforcement; (b) the Enforcement Bureau has issued a Final Determination Order requiring blocking of traffic from a specific upstream provider; (c) a customer has been suspended or terminated for violation of Coastal Redwood's terms of service; or (d) Coastal Redwood's own monitoring has identified specific traffic as fraudulent, illegal, or otherwise in violation of its acceptable use policy.

Blocking is implemented at Coastal Redwood's session border infrastructure and may be applied at customer-wide, caller-ID-specific, or destination-specific granularity depending on the nature of the identified problem.

Coastal Redwood monitors Commission Enforcement Bureau Final Determination Orders published in EB Docket No. 22-174. When such an Order identifies an upstream provider whose traffic must be blocked, Coastal Redwood implements the required block within the 30-day timeframe set by Commission rules, or sooner where the severity of the identified conduct warrants expedited action.

VII. Traceback Response and Escalation

Traceback Point of Contact

Coastal Redwood has designated the following single point of contact for traceback-related communications:

Coastal Redwood Networks — Network Operations Center (NOC)

Email: traceback@coastalredwood.net

Phone: 724-252-7436

The NOC is staffed as a functional group rather than tied to a single individual, ensuring continuous coverage.

Traceback Response

Coastal Redwood commits to acknowledging and responding to traceback requests within 24 hours of receipt. Response activity includes identification of the upstream provider from which the identified traffic was received, review of call detail records for the identified call, and forwarding of the traceback request to the responsible upstream client under the cooperation obligations imposed by Coastal Redwood's contracts. When Coastal Redwood was the signing party for the identified call, relevant attestation records and telephone number validation records are produced in support of the traceback.

Consistent with the published policies of the Industry Traceback Group, Coastal Redwood does not proactively register with the ITG; the ITG's process provides that a provider is contacted upon the first traceback request transiting its network, using contact information sourced from the Robocall Mitigation Database and downstream partners. Coastal Redwood's traceback point of contact above is listed in its Robocall Mitigation Database filing for that purpose, and Coastal Redwood commits to cooperating fully with any ITG traceback upon receipt.

Graduated Response to Problematic Traffic

When problematic traffic patterns are identified — whether through internal monitoring, downstream completion-rate degradation, or traceback findings — Coastal Redwood applies a graduated response scaled to the severity and persistence of the issue. Initial responses may include notification to the customer requiring investigation, temporary throttling or rerouting of affected traffic, or a requirement that the customer terminate service to a specific downstream client. Persistent or egregious issues result in suspension or termination of the customer relationship. Coastal Redwood reserves the right to skip intermediate steps and move directly to suspension or termination when the severity of the traffic warrants it, including any case in which law enforcement, the Commission, or the ITG has identified the traffic as illegal.

VIII. Record-Keeping

Coastal Redwood retains call detail records, signaling records, and telephone number validation records for a minimum of two years, consistent with the period required to support traceback investigations and regulatory review. Customer onboarding and know-your-customer records are retained for the duration of the customer relationship and for no less than two years following termination. Records supporting STIR/SHAKEN attestation decisions — including the linkage between a signed call, the customer, the telephone number, and the active ownership validation at the time of signing — are maintained in sufficient detail to support any traceback or regulatory inquiry into the basis for a specific attestation.

IX. Certification

Coastal Redwood Networks certifies that the policies and procedures described in this Robocall Mitigation Plan constitute the specific reasonable steps it has taken to avoid carrying or processing illegal robocall traffic, and that it implements these policies and procedures on an ongoing basis. Coastal Redwood further certifies that it responds to all traceback requests from the Federal Communications Commission, law enforcement, and the Industry Traceback Group, and cooperates with such entities in investigating and stopping any illegal robocalling activity that may use its network.

This plan is reviewed and updated as appropriate to reflect changes in Commission rules, industry standards, and Coastal Redwood's own operational practices. Coastal Redwood will update its Robocall Mitigation Database filing within the timeframes required by the Commission's rules in response to any material change.