

Provider: [Leads to Scale LLC]

FRN: [0037441110]

Role(s) in call path: Originating voice service provider
(and, if applicable, reseller/wholesale)

Primary contact (RMD & law enforcement): [Name, Title,
Email, Phone]

Address: [Street, City, State, ZIP]

OCN (if any): [#####]

1) Program overview (required)

[Company] implements a multi-layer program to prevent, detect, and remediate illegal or spoofed robocalls originating on its network. This includes customer vetting (KYC), traffic monitoring & analytics, caller ID authentication (STIR/SHAKEN where applicable), traceback cooperation, and rapid remediation/blocking. This program satisfies 47 C.F.R. § 64.6305 requirements and supports our RMD certification.

2) STIR/SHAKEN deployment status (required)

- Status to certify in RMD: Partial STIR/SHAKEN (change to Complete if 100% of your IP-originated calls are authenticated end-to-end).
- Implementation: We sign SIP-originated traffic that we originate or pass to participating downstream carriers using our STI-PA credentials (or through an authorized third party). Where calls traverse TDM or unauthenticated segments, we apply mitigation controls described below.
- If “Complete”: Replace the above with “All SIP calls we originate are authenticated with our STI-PA certificate; we verify inbound signatures on termination.”
(Providers must select full/partial/none in RMD and certify that all originated calls are subject to a mitigation program.)

Note: As the FCC tightens filings, providers claiming partial/complete

should have their own STI-PA token/certificate or a compliant third-party arrangement that authenticates all originated SIP calls.

3) Know-Your-Customer (KYC) & onboarding (required)

Before enabling origination, we verify:

- Business identity & legitimacy: legal name, EIN, formation records, corporate address, website, officers, industry, and service use-case.
- Contact verification: working phone/email for operational and abuse contacts.
- Consent basis & calling practices: scripts, lead sources, opt-in method (and proof), vertical (e.g., informational vs. telemarketing), target geography.

- Risk signals: prior enforcement actions, reputation checks, ITG traceback history, and foreign origination risk.
- Number resources: assignment source, CNAM alignment, Do-Not-Originate (DNO) screening, any high-risk ranges.
Customers must accept our AUP and Robocall/Spam Policy; high-risk use-cases face tighter limits or rejection. (KYC and reasonable steps to avoid illegal calls are explicit elements of compliant programs.)

4) Caller ID authentication & attestation

- Attestation policy:
 - A (Full) when we have a direct authenticated relationship with the caller and assigned/validated the number.
 - B (Partial) for verified customer with a number we did not assign but validated to the customer.

- C (Gateway) not used for origination unless unavoidable; flagged for additional analytics.
-
- DNO & high-risk lists: We block known Do-Not-Originate numbers and known invalid/unallocated ranges at ingress.
- Display alignment: We require accurate A-number and brand display; CNAM consistency is encouraged/verified when feasible. (These practices align with FCC expectations for authenticated caller ID and mitigation.)

5) Traffic monitoring, analytics & controls (required)

We continuously monitor originated traffic for red flags, including:

- Abnormal answer/seizure ratios (ASR), short-duration spikes, high calls-per-second (CPS),

repetitive patterns, sequential dialing, and unusual call windows.

- Complaints, carrier spam labels, honeypot hits, and traceback notifications.

Controls applied: per-customer CPS limits, concurrent session caps, geo/ANI throttles, destination blocks, and dynamic rate limiting.

Suspicious traffic triggers automated alerts and manual review. (Ongoing monitoring and analytics are core program elements.)

6) Remediation, blocking & enforcement (required)

If we detect illegal or abusive traffic:

1. Immediate containment: suspend affected trunks/routes; block suspect A-numbers/ranges; implement tighter CPS/caps.
2. Customer contact & cure: notify the customer; require proof of consent or corrected practices.

3. Escalation: repeated or egregious issues lead to account termination and upstream/peer notification as appropriate.
4. Recordkeeping: retain event logs, CDR samples, and correspondence for at least 24 months (or longer if required by law/enforcement request).
(Providers must take reasonable steps and be able to demonstrate mitigation when filing in RMD.)

7) Traceback & law-enforcement cooperation (required)

We fully cooperate with the USTelecom Industry Traceback Group (ITG), FCC, FTC, and state AGs. We respond promptly to traceback requests, provide CDRs/headers as permitted by law, and take immediate mitigation when notified of illegal traffic. (Traceback cooperation is an explicit requirement tied to RMD obligations.)

8) Handling foreign-originated traffic / wholesale

- We do not accept anonymous open SIP peering.
- Any foreign or wholesale intake requires documented KYC, upstream attestation visibility where possible, and contractual obligations mirroring this Program. High-risk sources face stricter limits or refusal.

9) Complaint intake & redress

We maintain abuse/reporting mailboxes and a web form. Complaints are triaged within 1 business day, correlated to CDRs/analytics, and resolved via the remediation ladder above. Proven erroneous blocking can be appealed via our abuse desk; validated legal traffic is unblocked rapidly.

10) Customer education & contractual terms

Customers receive guidance on lawful calling (e.g., consent, revocation, opt-out, time-of-day limits) and caller ID best practices. Our MSA/AUP prohibits illegal robocalls, snowshoeing, neighbor spoofing, and violations of federal/state telemarketing rules.

11) Governance, audits & updates

This Program is reviewed at least annually and upon material rule changes (e.g., FCC Order FCC 24-135 improving RMD effectiveness). We keep the public/redacted version in the RMD and can provide a confidential unredacted version to regulators upon request.

12) Technical references (public summary)

- STI-PA/CA: [Your provider or third-party signer]
- Softswitch/SBC: [e.g., FreeSWITCH/Kamailio/Acme/etc.]
- Analytics: [in-house rules + vendor tools, if any]
- Upstreams: [Carriers, if public]

Officer Certification (to accompany RMD filing)

I, [Name, Title], certify under penalty of perjury that:

1. All calls originated on [Company]’s network are subject to this robocall mitigation program; and
2. [Company] has [fully/partially/not] implemented STIR/SHAKEN on the IP portions of its network; and
3. Any prior RMD certification has not been removed by the Commission and we are not prohibited from

filing.

Signature: _____ Date:

(Certification language tracked to § 64.6305 & RMD
filing instructions