

FILING FOR THE FCC ROBOCALL MITIGATION DATABASE

Robocall Mitigation Program Description

Rojo Services LLC dba Rojoring.com
Non-Interconnected VoIP · Originating Voice Service Provider

LEGAL ENTITY	Rojo Services LLC	DBA	Rojoring.com
ENTITY TYPE	Delaware LLC	EIN	81-2901270
FCC FRN	0038442240	USAC FORM 499	Active · Non-Interc. VoIP
DNC SAN	On file with the Commission	FILER ROLE	Originating Voice Service Provider
STIR/SHAKEN	Partial – Upstream-Signed (Option 2)	PRINCIPAL OFFICE	J-5 Calle J, Guaynabo, PR 00966
OFFICER	Robert J. Johnson · President	PHONE / EMAIL	(636) 346-2037 · rob@rojoring.com

Rojo Services LLC dba Rojoring.com operates a non-interconnected VoIP platform delivering permission-based ringless voicemail at carrier-grade scale. This document is filed in the FCC Robocall Mitigation Database pursuant to 47 C.F.R. § 64.6305(b) and describes the technical and operational measures by which Rojo Services LLC prevents the origination of illegal robocalls across every call originated through its platform.

§ 0 Compliance Stack at a Glance

Consent Verification	Industry-standard third-party consent certification provider; per-recipient certificate produced on demand
Litigator Suppression	Industry-standard Active Litigator List integration via real-time API
Federal DNC Access	National DNC Registry — Subscription Account Number on file with the Commission (active)
STIR/SHAKEN Attestation	Upstream-signed via authorized voice carriers under their SPC tokens (iconectiv STI-PA)
Caller-ID Authentication	Per-customer ownership verification; LOA on file for every assigned number
Traceback Channel	Cooperates with Industry Traceback Group (ITG); 24-hour response SLA; rob@rojoring.com monitored 24/7; ITG Member Inquiry submitted
Identity / MFA	Multi-factor authentication enforced for all production access
Data Encryption	TLS 1.2+ in transit; AES-256 at rest; access-controlled audit log
Records Retention	Consent records and campaign telemetry retained 5+ years; suppression list retained indefinitely

§ 1 Program Posture & Scope

Rojo Services LLC ("Rojo Ring" or "the Company") originates non-interconnected VoIP voice traffic — pre-recorded direct-to-voicemail messages — on behalf of vetted, contracted business customers. Every delivery is treated as a "call" subject to the Telephone Consumer Protection Act ("TCPA"), 47 C.F.R. § 64.6305, the FTC Telemarketing Sales Rule where applicable, and all applicable state laws. The program below applies to one hundred percent of voice traffic originated through the platform.

The Company carries no traffic that is not consent-based and accepts no customer that cannot produce documented prior express consent (and, for telemarketing, prior express written consent) on a per-recipient basis. The Company maintains a continuous commitment to respond fully and within twenty-four hours to traceback requests from the Commission, law enforcement, the Industry Traceback Group, downstream carriers, and state attorneys general.

§ 2 Know-Your-Customer (KYC) & Vetting

The platform is offered by application only. No customer may originate a single voicemail until manual review is complete. Every applicant is subject to the following review prior to activation and on a continuing basis thereafter:

2.1 BUSINESS-ENTITY VERIFICATION

Verified against state Secretary of State records and federal records — legal entity name, date of formation, state of organization, EIN/Tax ID, and principal address.

2.2 PRINCIPAL IDENTIFICATION

Government-issued identification collected for each principal and controlling owner.

2.3 SANCTIONS & RESTRICTED-PARTY SCREENING

OFAC SDN, Denied Persons, and Debarred Parties screening at onboarding and quarterly thereafter.

2.4 REGULATORY HISTORY REVIEW

Each applicant reviewed for open or recent FCC, FTC, or state-AG enforcement action related to telemarketing, robocalling, or unfair-and-deceptive practices. Relevant actions disqualify or specially condition the applicant.

2.5 INTENDED-USE REVIEW

The Company reviews intended verticals, sample scripts, target geography, estimated volume, and the customer journey at which consent is captured.

2.6 LIST-SOURCING ATTESTATION

Each applicant must document the source of every recipient list and the method by which consent is captured. Lists from data brokers, scraped sources, skip-traces, or any source for which per-recipient consent records cannot be produced are disqualifying.

2.7 ACCEPTABLE USE POLICY

Each applicant accepts the Rojo Ring Acceptable Use Policy at application, with IP-and-timestamp audit log. The AUP is binding through the Terms of Service.

2.8 KNOW-YOUR-UPSTREAM-PROVIDER

The Company verifies that each upstream voice carrier is currently listed in the FCC Robocall Mitigation Database, monitored continuously for delisting events.

§ 3 Consent Verification & Recordkeeping

The Company requires per-recipient documented consent at the time of every delivery.

3.1 THIRD-PARTY CONSENT CERTIFICATION

The Company integrates with **TrustedForm** by ActiveProspect to certify prior express written consent on a per-recipient basis. Each opt-in is captured at source and stored as a verifiable TrustedForm certificate URL.

3.2 CONSENT RECORD CONTENTS

Each recipient record stores: (i) timestamp; (ii) source publisher and source URL; (iii) IP address and user agent; (iv) full consent language presented at opt-in; (v) business name presented to the consumer; (vi) campaign category and channel of contact for which consent was captured; and (vii) the TrustedForm certificate identifier.

3.3 CONSENT LANGUAGE REVIEW

All consent language is reviewed by Rojo Ring compliance before campaign activation — explicit reference to pre-recorded and ringless-voicemail outreach, identification of authorized parties, no misleading phrasing.

3.4 ON-DEMAND PRODUCTION

For any recipient, the Company produces the full consent record — TrustedForm certificate, source attribution, opt-in path — within twenty-four hours of any request from a downstream carrier, the Industry Traceback Group, the Commission, the FTC, or any state attorney general.

3.5 RETENTION

Consent records, list-source documentation, scripts, send schedules, and opt-outs are retained for at least five years, and longer for any campaign under inquiry.

§ 4 Suppression & Do-Not-Call Compliance

Every outbound delivery is filtered through the following layered suppression stack, enforced in series at send time:

LAYER	DESCRIPTION
Federal DNC Registry	National Do Not Call Registry scrub via the Company's active federal Subscription Account (SAN on file with the Commission). Recipient lists scrubbed within 31 days of every send.
State DNC Registries	Per-state DNC scrubs for every state operating its own registry, including Indiana, Missouri, Wyoming, Texas, and any other state with a published list. Stricter state calling-hour rules layered concurrently.
Blacklist Alliance	Real-time integration with the Blacklist Alliance Active Litigator List for TCPA-litigator and serial-complainant suppression.
Platform-Wide Internal	Any opt-out received by any channel — voice, IVR keypress, text reply, /opt-out web form, regulator forward, ITG forward — added to a platform-wide list and suppressed across every customer indefinitely.
Internal Blacklist	Rojo Ring-maintained blacklist seeded from prior complaints, carrier abuse reports, regulator forwards, and historical bad-reputation data.
Customer-Specific DNC	Each customer maintains and scrubs against its own opt-out list as a contractual obligation under the AUP. Customer opt-outs sync to the platform-wide suppression list within 24 hours.

Opt-out requests received by any channel are processed within twenty-four hours, propagated platform-wide, and honored indefinitely. No customer may re-contact a number that has opted out, by any means, including segmentation or re-branding.

§ 5 Quiet Hours & Throttling

The platform enforces, by default and without customer override:

- A delivery window of **8:00 a.m. to 9:00 p.m.** in the recipient's local time, derived from area-code and time-zone signaling.
- Stricter state-specific calling-hour rules layered automatically.
- Per-recipient daily frequency caps.
- Per-customer rate ceilings tuned to downstream-carrier ingestion tolerances.

None of these limits can be overridden without documented compliance review and written approval by the Rojo Ring compliance team.

§ 6 STIR/SHAKEN Authentication

The Company has filed under **Option 2 — Partial STIR/SHAKEN Implementation** pursuant to 47 C.F.R. § 64.6305. The Company itself does not directly hold a Service Provider Code (SPC) token. All IP-originated voice traffic carried on

the Rojo Ring platform is signed under STIR/SHAKEN by authorized upstream voice carriers under their SPC tokens issued by the STI Policy Administrator (iconectiv). The Company verifies the STIR/SHAKEN posture of every upstream carrier and confirms the upstream's listing in the FCC Robocall Mitigation Database on a continuing basis.

For traffic segments that cannot be signed in IP, the Company relies on **47 C.F.R. § 64.6302** and applies the full mitigation program described herein — including layered suppression, traffic analytics, throttling, and traceback response — to ensure all such calls remain subject to a robocall-mitigation program consistent with 47 C.F.R. § 64.6305(a). Caller-ID numbers used on the platform are restricted to numbers the originating customer legitimately controls or has been assigned, verified at customer onboarding through ownership documentation, verification-call confirmation, or integration with the customer's number-management system.

§ 7 Traffic Analytics & Anomaly Detection

The platform monitors every campaign in real time for patterns consistent with unlawful robocalling, including: (i) high burst rates; (ii) repeated delivery attempts to a narrow set of numbers; (iii) abnormal disposition-code distributions; (iv) abrupt list-mix changes mid-campaign; (v) matches against known-bad-reputation feeds; and (vi) elevated complaint volume attributable to a specific customer. Flagged traffic is throttled or paused pending compliance review. Every automated flag is reviewed by a human before any non-throttle action is taken.

§ 8 Traceback Response Protocol

The Company participates in the Industry Traceback Group ("ITG"), the FCC-designated traceback consortium operated by USTelecom, and responds to every traceback request from the ITG, downstream carriers, the Commission, the FTC, or any state attorney general within twenty-four hours. The traceback inbox **rob@rojoring.com** is monitored continuously, with on-call alerting to the compliance lead.

T + 0	Inbound traceback hits rob@rojoring.com; on-call compliance lead alerted via PagerDuty and SMS.
T + 4h	Acknowledgment sent to the requesting party with confirmation reference. Internal investigation opened.
T + 12h	Per-call provenance assembled: originating customer, list reference, per-recipient consent record (TrustedForm certificate), script, send window, disposition, carrier route.
T + 24h	Substantive response delivered. If unlawful traffic confirmed, originating customer suspended under the AUP.
T + 48h	Corrective action: suppression list updated, root cause documented, mitigation program updated.

§ 9 Records & Retention

The Company maintains records sufficient to reconstruct full provenance of any individual delivery:

- KYC and contracting records — account life + 7 years
- Per-recipient consent records — account life + 5 years from last campaign
- Campaign metadata and per-attempt delivery telemetry — 5 years
- Suppression and opt-out records — indefinite
- Traceback responses — 5 years
- Audit and training records — 5 years

Records stored in encrypted, access-controlled storage with documented retention schedules.

§ 10 Audit, Training & Continuous Improvement

The Company conducts: annual third-party review of this program by external compliance counsel; quarterly internal audits of consent records, suppression integrity, analytics false-negative rates, and traceback timeliness; annual training for all personnel on the TCPA, FTC TSR, state mini-TCPAs, and the platform's compliance tooling; and annual recertification of this program in the FCC RMD between February 1 and March 1. Updates to the Company's FRN, USAC Form 499 filing, and RMD entry are made within ten business days of any material change.

§ 11 Cooperation Commitment

The Company commits to respond fully and within twenty-four hours to all traceback requests from the Commission, law enforcement, the Industry Traceback Group, and downstream carriers, and to cooperate fully with such entities in investigating and stopping any illegal robocaller using the Rojo Ring platform. The Company certifies that it has not had any prior RMD certification removed by Commission action and has not been prohibited from filing in the Robocall Mitigation Database.

§ 12 Contact Channels for Regulators & Carriers

Compliance & Regulators	rob@rojoring.com
Tracebacks (24/7)	rob@rojoring.com
Recipient Opt-Out (Platform-Wide)	admin@rojoring.com
Recipient Complaints	admin@rojoring.com
Legal & Service of Process	rob@rojoring.com; D.C. agent designated under 47 U.S.C. § 413, on file with USAC
Mailing Address	Rojo Services LLC dba Rojoring.com · J-5 Calle J, Guaynabo, PR 00966 · (636) 346-2037

§ 13 Officer Certification

I, Robert J. Johnson, the duly authorized officer of Rojo Services LLC, certify under penalty of 18 U.S.C. § 1001 and 47 C.F.R. § 1.16 that I have read the foregoing Robocall Mitigation Program Description; that I am authorized to make this filing on behalf of Rojo Services LLC; that all of the information set forth herein is true, complete, and correct to the best of my knowledge and belief; that all calls originated by Rojo Services LLC on its network are subject to the robocall-mitigation program described herein; and that Rojo Services LLC commits to respond fully and within twenty-four hours to all traceback requests from the Commission, law enforcement, the Industry Traceback Group, and downstream carriers, and to cooperate fully in investigating and stopping any illegal robocaller using its service.

OFFICER

Robert J. Johnson

PRESIDENT · ROJO SERVICES LLC

DATE

May 20, 2026

EXECUTED IN GUAYNABO, PUERTO RICO

FRN 0038442240

EIN 81-2901270

SAN ON FILE

ROJORING.COM

FOUNDER · ROBERT J. JOHNSON · PUBLIC PROFILES

 /in/robertjj  @rojo1ang  @DrRojo  @internationalrojo  /brojkk