

RIA NETWORKS, LLC

ROBOCALL MITIGATION PLAN

October 2026

Contents

1. Introduction and Regulatory Framework	3
2. Company Information	3
3. Call Authentication – STIR/SHAKEN	3
4. Know Your Customer (KYC) & Know Your Upstream Provider (KYUP)	3
5. Accepting Traffic Only from Providers Listed in the RMD	4
6. Network Monitoring, Analytics, and Call Blocking.....	4
7. Emergency Calls and Public Safety.....	5
8. Mandatory Blocking Following Commission Notification	5
9. Traceback Cooperation	5
10. Contractual Controls	6
11. Prior Enforcement Disclosure	6
12. Certifications, Updates, and Annual Recertification.....	6

1. Introduction and Regulatory Framework

This Robocall Mitigation Plan (the “Plan”) describes the policies, procedures, technical controls, and contractual safeguards that RIA NETWORKS, LLC (“RIA” or the “Company”) applies to prevent its network and services from being used to originate or transmit illegal robocalls and unlawfully spoofed calls.

The Plan is filed with the Federal Communications Commission (“FCC”) in the Robocall Mitigation Database (“RMD”) to address RIA’s obligations under 47 C.F.R. § 64.6305, 47 C.F.R. § 64.1200(k) and (n), and the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act. The practices described in this Plan are reasonably designed to significantly reduce illegal robocall traffic, and RIA follows these practices in its operations.

RIA operates as a wholesale originating voice service provider. The mitigation measures in this Plan apply to all calls RIA originates on its network.

2. Company Information

Legal Name	RIA NETWORKS, LLC
FCC Registration Number (FRN)	0038947511
Service	Wholesale voice origination and SMS services provided to business and platform customers. RIA does not serve residential end users.
Business Address	9211 Forest Hill Ave #200, Richmond, VA 23235
Telephone	+1 904 445 1010
Principal / CEO	Henry Perez
Subsidiaries/Affiliates	None

3. Call Authentication – STIR/SHAKEN

RIA certifies, pursuant to 47 C.F.R. § 64.6305(d)(1)(iii), that it has not yet implemented STIR/SHAKEN on its network.

As a newly registered voice service provider, RIA is completing the registration, certification, and technical steps needed to implement STIR/SHAKEN. RIA expects to complete implementation after obtaining its Operating Company Number (OCN), registering with the STI Policy Administrator (STI-PA), obtaining its Service Provider Code (SPC) token, and securing a certificate from an approved STI Certification Authority (STI-CA). RIA will update its RMD certification and this Plan within 10 business days of completing implementation.

Until implementation is complete, all calls RIA originates are subject to the robocall mitigation measures described in this Plan.

4. Know Your Customer (KYC) & Know Your Upstream Provider (KYUP)

4.1 Onboarding Due Diligence

Before entering into a service agreement, RIA obtains and reviews the following information from each prospective customer:

- Legal business name, entity type, physical business address, and main telephone number.
- Type of business and the voice services the customer provides or intends to use.
- Contact details for key personnel, including name, title, email, telephone, and, where available, LinkedIn profile.
- Federal Tax ID (EIN) or foreign equivalent.
- FCC Registration Number (FRN) and FCC Form 499 Filer ID, where applicable.
- Robocall Mitigation Database registration status and Operating Company Number (OCN), where applicable.
- Regulatory profile, including whether the customer originates calls, acts as a gateway for foreign-originated traffic, engages in telemarketing, has implemented STIR/SHAKEN, and maintains its own robocall mitigation plan.
- Whether the customer has been identified by the ITG as a non-cooperative voice service provider or is subject to any FCC enforcement action.

4.2 Validation

RIA validates the information received by cross-checking it against independent sources, including the customer's website and public and social media presence, FCC Form 499 and FRN records, and the RMD, where RIA confirms that the customer is listed, has not been de-listed, and that the business described matches its RMD filing. RIA may request additional documentation at any time as a condition of onboarding or continued service.

4.3 Ongoing Review

RIA refreshes KYC information for active customers on a recurring basis, and whenever there is a material change, a triggering event, or an elevated-risk indicator identified through traffic monitoring. Continued service depends on the customer's timely and complete cooperation with these requirements.

5. Accepting Traffic Only from Providers Listed in the RMD

In accordance with 47 C.F.R. § 64.6305(g)(1)–(4), RIA accepts calls directly from another provider only if that provider's filing appears in the RMD. RIA verifies RMD status before activating any interconnection and periodically re-verifies that all directly connected providers remain listed. If a provider is removed from the RMD, RIA stops accepting its traffic promptly upon learning of the removal.

6. Network Monitoring, Analytics, and Call Blocking

RIA monitors traffic across its network on a continuous basis using the analytics and reporting tools of its own switch, supported by internal review. RIA's monitoring and enforcement include:

- Detection of abnormal traffic patterns through calls-per-second and session limits and anomaly detection.
- Analysis of key metrics, including answer-seizure ratio (ASR), average call duration, short-duration calling, invalid or unassigned ANIs, and excessive call-failure rates.
- Application of a Do-Not-Originate (DNO) filter to block calls purporting to originate from numbers that should never originate calls.
- Blocking of media and source IP addresses associated with suspicious or unlawful campaigns, or identified through FCC or Industry Traceback Group (ITG) notices.
- Reputation and reported-scam screening to identify and block high-risk sources.
- Use of SIP response code 603+ where RIA blocks calls based on reasonable analytics, in accordance with 47 C.F.R. § 64.1200(k)(9).

RIA combines automated controls with periodic internal review, as appropriate to its network operations. When illegal robocalling or caller ID spoofing is suspected, RIA promptly identifies the responsible party and takes timely action, including suspension or blocking of the offending traffic. Calls carrying valid STIR/SHAKEN Identity headers are passed without alteration.

7. Emergency Calls and Public Safety

Where applicable to its services, RIA will not block calls to 911 and will make all reasonable efforts to avoid blocking calls from Public Safety Answering Points (PSAPs) or government emergency numbers. RIA reviews these safeguards whenever it changes its call blocking rules.

8. Mandatory Blocking Following Commission Notification

Upon receiving an FCC Notification of Suspected Illegal Traffic under 47 C.F.R. § 64.1200(n)(2), RIA will promptly investigate the identified traffic, block it where RIA determines that it is illegal, and report to the Commission within 14 days of the notification, or within the deadline stated in the notification, the results of its investigation and the steps taken. RIA will also take reasonable steps to prevent its network from being used to transmit substantially similar traffic from the same source in the future.

9. Traceback Cooperation

RIA participates in the industry traceback process and responds fully within 24 hours to traceback requests from the Commission, law enforcement, and the Industry Traceback Group (ITG), consistent with 47 C.F.R. § 64.6305(a)(2). RIA uses the ITG's secure traceback portal to review and verify traffic records, identify the source of flagged calls, and support investigations into illegal robocalls originating through its service. The designated contact listed below receives and acts on traceback requests and suspicious-traffic inquiries. RIA also cooperates with other providers and industry bodies, sharing information about suspicious traffic to support timely investigation and mitigation.

Name	Henry Perez
Title / Department	Manager / CEO
Business Address	9211 Forest Hill Ave #200, Richmond, VA 23235
Telephone	+1 904 445 1010
Email	compliance@rianetworksllc.com

10. Contractual Controls

Every RIA customer must execute a Master Service Agreement (MSA) and comply with all applicable federal, state, and international laws and regulations governing telecommunications services, including those related to robocalls, caller ID authentication, and consumer protection. RIA's Acceptable Use Policy (AUP) prohibits the use of its services for any unlawful, fraudulent, abusive, or deceptive activity, including the origination or transmission of illegal robocalls and caller ID spoofing.

Under its MSA and AUP, RIA may suspend, restrict, or terminate service, in whole or in part, immediately and without prior notice where it reasonably determines that such action is necessary because of an AUP violation, suspected or actual fraud, a legal or regulatory obligation (including FCC requirements), or to protect its network, its customers, or third parties.

11. Prior Enforcement Disclosure

Pursuant to 47 C.F.R. § 64.6305(d)(2)(iv), RIA states that, at no time in the prior two years, has RIA been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing relating to illegal robocalls, spoofing, or a deficient RMD certification or mitigation program.

12. Certifications, Updates, and Annual Recertification

RIA certifies that:

- All calls it originates and/or transmit on its network are subject to this robocall mitigation program.
- No prior certification of RIA has been removed by Commission action, and RIA has not been prohibited from filing in the RMD.
- The information in this Plan and in its RMD filing is true, accurate, and complete.

RIA will update its RMD filing, including this Plan, within 10 business days of any change to the required information, as required by 47 C.F.R. § 64.6305(d)(5), and will recertify on or before March 1 of each year that the information in its RMD filing is true and correct, as required by 47 C.F.R. § 64.6305(h). RIA reviews

this Plan periodically and updates it as needed to reflect changes in its operations, network, vendor relationships, or applicable FCC requirements.