

Robocall Mitigation Plan (RMP)

Provider / Filing Entity: Apollo Networks, Inc.

Also known as (DBA / trade / affiliated branding): Apollo Networks; Apollo Managed Services LLC

FRN: 0031067994

Registered Address: 836B N Broadway, North Massapequa, NY 11758

Primary Contact: Zack Magee

Email: zmagee@apollonetworks.com

Phone: 516-584-4000

Date: February 4, 2026

1) Purpose and Scope

This Robocall Mitigation Plan (“Plan”) describes the policies, procedures, and technical controls used by Apollo Networks, Inc. (including its associated branding as Apollo Networks and Apollo Managed Services LLC) to prevent, identify, and mitigate unlawful robocalls and other illegal or suspicious voice traffic originating on or transiting its network.

This Plan applies to all voice services offered by Apollo Networks, Inc., including any services delivered to end users via provider-provisioned devices and associated telephone numbers.

2) Service Model and Risk Controls

Apollo Networks operates a controlled provisioning model designed to materially reduce robocall risk:

1. **No open signup / no self-service onboarding.** Apollo Networks does not provide open, automated, or anonymous signups for voice service. All customers are reviewed and approved manually prior to activation.
2. **Provider-provisioned endpoints only.** Apollo Networks provides end users with managed phones/devices.
3. **No SIP credential disclosure / no customer trunks.** Apollo Networks does not provide customers or end users with SIP usernames/passwords, SIP trunk credentials, IP-auth trunk parameters, or similar access methods that could be used to attach customer-controlled dialers or originate mass outbound calling outside of provider-managed endpoints.

4. **No programmable or bulk-dialing interfaces.** Apollo Networks does not provide outbound campaign tools, dialer integrations, or bulk outbound APIs intended for automated robocalling activity.
5. **Upstream carrier origination.** Apollo Networks originates calls via vetted upstream carrier partner(s) and does not enable customer-managed SBCs or customer-provided trunk origination into the PSTN.

These controls restrict unauthorized high-volume dialing and reduce the likelihood of illegal robocalling originating from Apollo Networks services.

3) Customer Onboarding and Manual Vetting

Apollo Networks manually vets all customers prior to activation and does not offer anonymous or self-service signups. As part of onboarding, Apollo Networks reviews customer legitimacy and intended use, including validating reliable contact information, confirming an accountable authorized representative, and evaluating whether the stated use case and expected calling behavior are consistent with lawful voice communications. Apollo Networks employees, or authorized subcontractors thereof, install all endpoints at all client sites and secure all endpoints such that SIP credentials cannot be obtained.

Vetting steps may include (as applicable):

- Confirmation of business legitimacy (e.g., business presence, nature of operations, references, and consistency of contact information)
- Confirmation of an accountable authorized representative and reliable contact path
- Review of the customer's intended use case and expected calling patterns (e.g., normal business calling vs. high-risk or atypical outbound use)
- Screening for red flags associated with illegal robocalling (e.g., unexplained need for high-volume outbound calling, short-term/anonymous behavior, evasion of accountability, inconsistent or unverifiable details)

Third-party vendor use: Apollo Networks **does not use third-party vendors** for KYC, identity analytics, behavioral analytics, traffic scoring, or robocall analytics as part of customer onboarding. All onboarding review and approval decisions are performed internally using information provided by the customer and internally maintained account/provisioning records.

Apollo Networks reserves the right to request additional information, deny service, delay activation, or impose restrictions where risk cannot be adequately mitigated.

(Note: Apollo Networks does not represent that it performs government-ID based KYC for all customers.)

4) STIR/SHAKEN Implementation

Apollo Networks is a voice service provider serving end users through a hosted PBX model and uses upstream carrier partners for PSTN origination and termination. Apollo Networks has not implemented the STIR/SHAKEN authentication framework on any portion of its own network and is not certifying to full or partial STIR/SHAKEN implementation. Apollo Networks does not currently authenticate calls using its own SPC token and STI certificate. To the extent call authentication may be applied within the overall call path, that is performed through upstream carrier arrangements and not through Apollo Networks' own SPC token and certificate.

5) Traffic Monitoring and Detection

Apollo Networks monitors for suspicious calling behavior and investigates anomalies using available operational signals and call records. Indicators of potentially unlawful or unwanted robocalling may include, but are not limited to:

- Sudden spikes in outbound calling volume or call attempt rates
- Abnormally low answer-seizure ratio (high attempts with low answers)
- Very short-duration calls consistent with robocall blasting
- Repetitive dialing patterns, sequential numbering, or large-list behavior inconsistent with stated use
- Complaints from call recipients, enterprises, carriers, traceback groups, or regulators
- Requests or behaviors indicating attempted evasion of accountability (rapid number changes, frequent provisioning changes without justification, etc.)

6) Mitigation and Enforcement Actions

When Apollo Networks detects or reasonably suspects illegal, unwanted, or suspicious robocall activity, it takes prompt mitigation steps appropriate to the risk, including one or more of the following:

- **Outbound restrictions** (rate limiting or feature restriction)
- **Traffic blocking** for specific numbers, routes, or calling behaviors associated with suspected abuse
- **Immediate suspension** of service pending investigation in urgent or high-risk cases

- **Termination** of service for confirmed illegal robocalling, refusal to cooperate, repeat violations, or material misrepresentations during onboarding
- **Number-level actions** such as disabling outbound calling from specific DIDs where warranted

Apollo Networks documents mitigation actions taken and retains relevant records consistent with its policies and applicable obligations.

7) Complaint Intake and Traceback Cooperation

Apollo Networks maintains channels to receive and respond to complaints and traceback inquiries regarding suspected illegal robocalls.

Complaint / Traceback Contact:

- **Email:** zmagee@apollonetworks.com
- **Phone:** 516-584-4000

Apollo Networks will:

- Review complaints and correlate them to CDRs and account activity where feasible
- Investigate the originating account/endpoints as applicable
- Implement mitigation actions as appropriate
- Cooperate with industry traceback efforts and provide relevant records consistent with applicable law and contractual obligations

8) Recordkeeping

Apollo Networks maintains records sufficient to support investigation and mitigation of suspected robocalls, which may include:

- Customer onboarding and account approval artifacts (as collected)
- Endpoint provisioning records and assigned numbering information
- Call detail records (CDRs) and operational logs used for monitoring/investigations
- Documentation of mitigation actions and account enforcement decisions

Retention is managed in accordance with Apollo Networks' internal retention practices and any applicable legal requirements.

9) Governance and Plan Maintenance

Apollo Networks reviews this Plan periodically and updates it as needed to reflect changes in services, threat conditions, and regulatory expectations. Responsibility for Plan implementation and escalation rests with company leadership and operations.

Responsible Party: Zack Magee

Email: zmagee@apollonetworks.com

Phone: 516-584-4000