

Narrate Inc. Robocall Mitigation Program

Filed by: Narrate Inc. (d/b/a EloLabs, FeatherAI, and Elo GPT)

1. Company Overview

EloLabs is a cloud-based AI communications platform operated by Narrate Inc., serving verified business entities in the United States. The platform enables organizations to manage outbound and inbound voice, SMS, and email communications with their contacts. For outbound voice communications, EloLabs originates calls through upstream voice service providers who handle STIR/SHAKEN call authentication on their networks.

All outbound communications are subject to the platform's compliance controls, including DNC screening, time-of-day restrictions, federal and state regulatory compliance, opt-out enforcement, and human-initiated sending where legally required.

2. Customer Vetting and Onboarding

- All customers must complete a formal business verification (KYC) process before gaining platform access, confirming they are a legitimate, verified business entity.
 - Customers sign a service agreement that explicitly prohibits illegal robocalling, spoofing, or any communications that violate the TCPA or FCC regulations.
 - The platform's Terms of Service include explicit TCPA compliance requirements and robocalling prohibitions applicable to all users.
 - Customers who violate these terms are subject to immediate suspension and termination of service.
-

3. Technical Robocall Mitigation Controls

EloLabs implements the following technical measures to prevent illegal robocalls from originating through its platform:

Compliance Screening:

- All outbound communications are screened against the platform's compliance protocols prior to delivery.
- Campaign creation requires structured configuration, including channel selection, compliance profile assignment, and contact type designation. Compliance profile options are defined and constrained by the platform based on applicable regulatory requirements — customers may only select from pre-approved configurations that meet established legal standards and may not define

or modify compliance parameters outside of what the platform permits.

Do Not Call (DNC) Compliance:

- Non-opt-in outbound communications are screened against the National Do Not Call Registry via third-party DNC verification services.
- Screening encompasses federal DNC, state-level DNC lists, and additional regulatory flags.
- Per-campaign compliance profiles determine which DNC categories are enforced, ensuring appropriate blocking based on the nature and context of each communication.

Consent and Opt-Out Management:

- For contacts with documented opt-in consent, the platform verifies and manages the opt-in audit trail to ensure consent validity.
- The platform maintains contact-level opt-out tracking — contacts who have opted out are blocked from receiving further communications, and opt-out requests are honored promptly.

Human-in-the-Loop Sending, where legally required:

- For non-opt-in communications, the platform does not function as an automated dialer — each message or call is individually triggered by a human operator in accordance with applicable law.

Time-of-Day Restrictions:

- The platform enforces calling window restrictions in compliance with TCPA and applicable state regulations.
- No outbound calls are initiated before 8:00 AM or after 9:00 PM in the recipient's local time zone.
- State-specific calling hour restrictions are enforced at the campaign level.

Caller ID Integrity:

- All outbound calls originate from phone numbers legitimately assigned to and owned by the customer, or provisioned through the platform's upstream carrier.
- The platform does not permit caller ID spoofing or any manipulation of originating phone number information.

10DLC Compliance:

- All SMS messaging is conducted through 10DLC-registered campaigns in compliance with carrier requirements for application-to-person (A2P) messaging.

4. Monitoring and Enforcement

- EloLabs operates an automated anomaly detection system that analyzes call logs to identify unusual patterns, volume spikes, and potential misuse.
 - Customers found to be in violation of the platform's acceptable use policy or applicable law are subject to immediate service suspension and account termination.
 - EloLabs commits to fully cooperating with any traceback requests from the FCC, law enforcement, the Industry Traceback Group, or upstream carriers.
-

5. What EloLabs Does Not Provide

- Anonymous or untraceable calling capabilities
- Caller ID spoofing functionality
- Bulk autodialing to purchased or scraped number lists
- Call origination on behalf of unverified or anonymous users