

Robocall Mitigation Program — bardan.dev SRL (AlterPhone)

Robocall Mitigation Program — bardan.dev SRL ("AlterPhone")

Filer: bardan.dev SRL (DBA: AlterPhone) **FRN:** 0038388286 **Filing date:** May 7, 2026 **Provider**

role: Voice Service Provider (foreign), without a STIR/SHAKEN implementation obligation

Certification: Option 3 — No STIR/SHAKEN Implementation; complete robocall-mitigation program per 47 CFR § 64.6305(a) **Robocall-mitigation contact:** Marius Bardan, Sole Member, Operations.

str. Onisifor Ghibu 20a, 400185 Cluj-Napoca, Cluj, Romania. +40 755 118 707 —

marius@bardan.dev

1. Description of voice service

bardan.dev SRL operates AlterPhone, a consumer mobile application (iOS / Android) that issues individual end-users a personal second phone number (DID). DIDs are leased from upstream U.S. carriers Twilio and Telnyx; AlterPhone does not hold its own number-block allocations, does not interconnect directly with the PSTN, and does not act as a wholesale or transit provider. The user interface is a single-call dialer; there is no bulk-dialing API, no predictive or auto-dialer functionality, and no campaign-management tooling. The subscriber base consists exclusively of natural persons; no business-to-consumer outbound calling, no telemarketing, no political or fundraising calling is supported by the platform.

Outbound calls to U.S. PSTN destinations are originated by the mobile client over SIP, traverse a Kamailio session-border controller (under bardan.dev SRL operation), and terminate to the PSTN through Twilio or Telnyx. Twilio and Telnyx, as the upstream U.S.-licensed voice service providers, hold the relevant STIR/SHAKEN signing certificates and sign call attestations on AlterPhone's behalf.

2. Practices to prevent customer-initiated illegal robocalls

2.1 Subscriber identity verification (KYC) at sign-up

Every subscriber account is bound to a verified identity at registration. Three sign-up paths are accepted, all of which require ownership of a third-party-verified credential:

- **Phone OTP** — Twilio Verify SMS code to a real handset; the recipient must possess the handset to complete verification.
- **Google OAuth** — verified Google account with verified email.
- **Apple Sign In** — verified Apple ID.

Each verified identity maps to exactly one user record in the authentication system; multi-account-per-identity is rejected at sign-up. Source IP and IP-derived country are recorded at sign-up and at every subsequent sign-in, and stored alongside the account record. Phone-OTP rate limits are enforced per source IP and per destination phone number; suspended phone numbers receive a 403 short-circuit before any SMS is dispatched.

For numbers issued in countries where carrier-side dispatchable- location registration is supported (currently the United States, Puerto Rico, Canada, and the United Kingdom), outbound calling is gated on collection and carrier-validation of an emergency-services address per the carrier's E911 / equivalent program before the line becomes capable of originating outbound calls.

2.2 Architectural constraints on bulk dialing

The product surface is a single-call interactive dialer. The server-side call-initiation endpoint is JWT-authenticated to one user, accepts exactly one destination per request, and enforces per-user rate limits on call initiation. There is no programmatic broadcast or campaign API exposed to subscribers. The platform was not designed for, and does not support, the call patterns that typically generate illegal robocall traffic.

2.3 Per-call records and traceability

Every outbound call writes a record to the `call_history` data store at call setup and updates it at call completion. Each record captures, at a minimum:

- Subscriber identifier (internal user ID).
- AlterPhone DID used as the calling number (E.164).
- Called number (E.164).
- Originating SIP IP and source country at call setup.
- Upstream carrier (Twilio or Telnyx) handling the leg.
- Call-setup timestamp (UTC) and call-completion timestamp.
- Duration and disposition.

Records are retained for at least 24 months. The retention period exceeds the 24-hour traceback-response window required by 47 CFR § 64.6305(b) and supports follow-on Commission, law-enforcement, or industry-traceback enquiries on historical traffic.

2.4 Content controls

In-call media is end-to-end encrypted (SRTP) between the subscriber device and the upstream carrier's media gateway. AlterPhone does not record call audio. Optional, per-user-opt-in transcription (when enabled by the subscriber for their own records) is encrypted at rest. The platform does not generate, broadcast, or assist with recorded-message playback.

2.5 Account suspension and revocation

The platform supports immediate, server-side account suspension. A suspended account loses the ability to originate new calls within seconds across all of the subscriber's devices via JWT-token revocation and an authentication-state cache invalidation pushed to the request-validation layer; new sign-ins for the suspended identity are also rejected. Suspension is used for confirmed abuse, suspected fraud, repeated violations of the AlterPhone Terms of Service, and on receipt of a credible Commission, law-enforcement, or traceback request implicating a subscriber.

2.6 Carrier-side controls

Twilio and Telnix both expose call-anomaly insights (volume, destination distribution, duration patterns) for the AlterPhone sub-account. AlterPhone reviews material anomalies and acts on them including, where appropriate, immediate subscriber suspension under Section 2.5.

3. Practices for identifying and acting on suspicious calls

- **Volume anomalies** — call-rate alerts on per-user thresholds and per-DID thresholds. Threshold violations trigger automatic rate-limit enforcement and a manual-review queue.
 - **Destination concentration** — disproportionate concentration of calls toward a small set of destinations from a single subscriber is flagged for review.
 - **Short-duration high-volume patterns** — the canonical robocall signature (high attempt rate, very short connect duration) is monitored and flagged.
 - **Reported numbers** — destination numbers reported by abuse channels (industry traceback, Commission referrals, end-user reports) are added to a server-side denylist; calls to denylisted destinations from any subscriber are blocked at the SBC.
-

4. Cooperation with the Commission, law enforcement, and the Industry Traceback Group

bardan.dev SRL commits to:

- Respond fully within 24 hours to traceback requests from the Federal Communications Commission, the Enforcement Bureau, the USTelecom Industry Traceback Group, and federal/state law enforcement.
- Provide, on request and subject to applicable privacy law, per-call records (E.164 numbers, timestamps, durations, carrier), subscriber registration data (verified phone/email, sign-up IP and country), and account-status history.
- Take timely investigative action on credible reports of illegal robocall, spoofing, or fraud activity originating from a subscriber, up to and including immediate account suspension under Section 2.5 and termination.
- Cooperate with subpoenas, civil investigative demands, and judicial process directed to bardan.dev SRL.

The robocall-mitigation contact identified at the head of this document is the single point of contact for traceback enquiries and is the same individual identified in the Robocall Mitigation Database filing.

5. Maintenance and updates

- This filing and program description will be updated within 10 business days of any material change to the operational facts recited above, per 47 CFR § 64.6305(d)(5).
 - The program is reviewed at least annually.
 - The certification posture (Option 3 — no STIR/SHAKEN implementation, mitigation-program-only) will be revisited if the origination architecture changes such that bardan.dev SRL acquires or originates calls outside the Twilio / Telnyx upstream signing path.
-

This document constitutes the robocall mitigation program description filed in support of bardan.dev SRL's Robocall Mitigation Database certification under 47 CFR § 64.6305.