

Robocall Mitigation Plan

OpenPhone Technologies, Inc. (DBA: Quo)

OpenPhone Technologies, Inc. (“Quo”) submits this Robocall Mitigation Plan in compliance with **47 C.F.R. § 64.6305(d)(2)(ii)-(iii)** for inclusion in the FCC Robocall Mitigation Database.

Quo is a non-facilities-based interconnected VoIP provider that originates outbound voice traffic through its upstream carrier partner, Twilio Inc. Quo does not operate its own transmission facilities.

1. STIR/SHAKEN Implementation

Quo routes all outbound voice traffic through its upstream provider, Twilio Inc. Twilio implements STIR/SHAKEN authentication in accordance with FCC rules and industry standards.

Quo does not directly sign calls. However:

- All outbound voice traffic is routed through Quo’s upstream provider, Twilio Inc., which represents that it implements STIR/SHAKEN authentication in accordance with FCC requirements.
- Quo verifies customer identity prior to service activation.
- Quo assigns and manages telephone numbers through authorized carrier channels.
- Customers are not permitted to transmit calls using unauthorized or spoofed caller ID information.

Quo requires customers to use only telephone numbers that are either:

- Assigned by Quo, or
- Properly ported with verified authorization.

2. Know Your Customer (KYC) Practices

Quo employs layered identity verification controls prior to enabling outbound voice capabilities.

Account Creation Controls

- Users must verify a non-VoIP phone number via One-Time Passcode (OTP).
- Users must provide valid payment credentials (name, card number, expiration date, CVC, billing address, ZIP code).
- Payments are screened using Stripe Radar fraud detection.
- Quo applies internal payment risk rules to detect suspicious payment patterns.

Risk Scoring & Fraud Screening

- User information is screened through Sift fraud detection software.
- Accounts are assigned risk scores (low, medium, high).
- High-risk accounts are flagged for enhanced review.

Enhanced Verification

When risk signals are triggered, Quo may:

- Restrict outbound calling or messaging
- Limit call/text velocity
- Require government-issued identification
- Require additional business documentation
- Suspend or terminate the account

Outbound A2P messaging to U.S. numbers requires completed and approved campaign registration.

3. Voice Traffic Monitoring and Analytics

Quo employs automated and manual monitoring systems to detect patterns consistent with illegal robocalling.

Automated Monitoring Controls

Quo monitors for:

- Unusual outbound call volume spikes
- High call velocity patterns
- Short-duration, high-volume call activity
- High complaint indicators
- Geographic inconsistencies
- Traffic inconsistent with customer profile or use case

Accounts that exceed internal risk thresholds may be automatically:

- Rate-limited
- Temporarily suspended
- Flagged for manual review
- Permanently terminated

4. Acceptable Use & Fair Use Enforcement

Quo's Terms of Service and Fair Use Policy prohibit:

- Cold calling without proper consent
- Prerecorded voice calls in violation of law
- Use of automated dialing systems in violation of the TCPA
- Any unlawful telemarketing activity
- Scams, impersonation, or fraudulent schemes

Quo reserves the right to:

- Impose usage limits
- Block outbound traffic
- Suspend accounts
- Terminate service without notice when required to comply with carrier or regulatory obligations

5. Dedicated Fraud & Compliance Team

Quo maintains a dedicated fraud and compliance team operating seven (7) days per week.

Responsibilities include:

- Reviewing automated alerts and flagged traffic
- Investigating complaint-driven escalations
- Reviewing high-risk account activity
- Conducting manual document verification
- Coordinating with upstream carriers on abuse reports

Quo maintains a target 24-hour SLA for investigation of escalated high-risk activity and traceback-related inquiries.

6. Complaint Monitoring & Traceback Cooperation

Quo:

- Cooperates with the FCC, law enforcement, and the Industry Traceback Group.
- Responds fully and within 24 hours to traceback requests.
- Takes immediate mitigation action when credible evidence of illegal robocalling is identified.

Mitigation may include:

- Traffic suspension
- Account termination
- Preservation of relevant records
- Cooperation with enforcement authorities

7. Upstream Carrier Coordination

Quo's upstream voice provider is Twilio Inc.

Quo cooperates with Twilio and other industry partners to:

- Investigate suspected illegal robocall traffic
- Identify originating customers
- Enforce carrier-level requirements
- Comply with mitigation directives

Quo honors carrier-imposed restrictions when necessary to prevent illegal traffic from propagating.

8. Ongoing Evaluation & Improvement

Quo continuously evaluates:

- Effectiveness of traffic monitoring thresholds
- Emerging robocall tactics
- Regulatory guidance updates
- Industry best practices

Quo updates its controls and mitigation strategies as necessary to reduce the risk of illegal robocall origination.