

Robocall Mitigation Program Description

Conquest Solutions, LLC
FRN 0031445216 · OCN 413M · 1250 Powers Ferry Common SE, Marietta, GA 30067
Filed pursuant to 47 CFR § 64.6305 · Dated June 22, 2026

1. Provider Profile and Scope

Conquest Solutions, LLC ("Conquest") is a United States voice service provider offering hosted PBX (3CX-based) business communications service and SIP trunk service to business end users. Conquest maintains a direct, contractual relationship with each end-user customer under a written Telecommunications Services Agreement, assigns or ports the telephone numbers used by its customers, and bills those customers directly for service. Conquest does not offer service on a wholesale or resale basis to its customers; resale is expressly prohibited under its customer agreement.

Conquest certifies that all calls it originates are subject to the robocall mitigation program described below, consistent with 47 CFR § 64.6305.

2. STIR/SHAKEN Implementation Status

At the time of this filing, Conquest has not yet completed STIR/SHAKEN caller ID authentication in the IP portions of its own network using its own certificate. Conquest is actively in the process of obtaining its own STIR/SHAKEN certificate and onboarding to a hosted call-signing service so that it may authenticate the calls it originates. Accordingly, Conquest files under the "No Implementation" certification and relies on the reasonable robocall mitigation practices set out in this description for all of the traffic it originates. Upon completing implementation, Conquest will update this certification to reflect its implementation status within ten (10) business days of the change.

3. Reasonable Steps to Avoid Originating Illegal Robocall Traffic

Conquest's mitigation practices are designed to significantly reduce the origination of illegal robocalls across its network. These practices include:

- **Business-only customer base; no resale.** Service is provided only to identified business end users. The customer agreement expressly prohibits resale or transfer of the service to any other person without Conquest's prior written permission, which limits anonymous or layered origination.
- **Contractual prohibition on abusive calling.** The customer agreement prohibits use of the service for auto-dialing, continuous or extensive call forwarding, inbound or outbound call-center operations, telemarketing (including charitable, political solicitation, or polling), and fax broadcasting or blasting on standard plans.

- **Lawful-use requirement with immediate termination.** Customers agree to use the service only for lawful purposes. Conquest reserves the right to terminate service immediately and without advance notice where it believes the service is being used for a prohibited or unlawful purpose, and to forward objectionable material and related records to the appropriate authorities.
- **Usage anomaly detection.** Conquest applies usage thresholds (including a pooled-minute cap per seat on "unlimited" plans) that are used to identify atypical or high-volume calling patterns indicative of abuse, triggering review.
- **Controlled number assignment.** Conquest assigns and controls the telephone numbers used by its customers and manages porting; customers may not transfer or reassign numbers independently, reducing the risk of spoofing or unauthorized number use.
- **Fraud and theft-of-service reporting.** Customers are contractually required to notify Conquest promptly of any suspected theft or fraudulent use of service, supporting rapid detection and response.

4. Know-Your-Customer (KYC) Process

- Every customer is onboarded under a signed written service agreement; Conquest collects and retains the customer's legal business name, service and billing address, authorized contacts, and account information.
- Service is provisioned to an identified business at a known location, establishing a direct, authenticated relationship between Conquest and the calling party.
- Telephone numbers are assigned only to vetted, contracted customers; for ported numbers, Conquest obtains a Letter of Authorization confirming the customer's right to use the number.
- Customer and provisioning records are retained and are available to support traceback and law-enforcement inquiries.

5. Know-Your-Upstream-Provider Compliance (47 CFR § 64.1200(n)(4))

- Conquest obtains underlying transport, origination, and numbering services from established, regulated U.S. carriers and takes reasonable steps to confirm that those providers are themselves participants in STIR/SHAKEN and the robocall-mitigation framework (including listing in the Robocall Mitigation Database where applicable).
- Conquest monitors for indications that an upstream or peer provider is a source of illegal robocall traffic and will investigate, escalate, and, where warranted, cease accepting traffic from or routing traffic to a non-cooperative provider.

6. Traceback Cooperation

Conquest commits to respond fully and within twenty-four (24) hours to all traceback requests from the Federal Communications Commission, law enforcement, and the industry traceback consortium (the USTelecom Industry Traceback Group), and to cooperate with those entities in identifying, investigating, and stopping any illegal robocallers that use Conquest's service to originate calls.

Designated traceback / robocall mitigation contact: Lance Retter, Chief Executive Officer, Conquest Solutions, LLC — (770) 953-2500 ext. 1100 — lance@csatlanta.com.

7. Response When Illegal Traffic Is Identified

- Investigate promptly to identify the originating customer and the nature of the traffic.
- Take graduated action up to and including immediate suspension or termination of the offending customer, as permitted under the customer agreement.
- Preserve relevant records and provide them to the Commission, law enforcement, or the traceback consortium as appropriate.
- Review and tighten onboarding or monitoring controls where a gap is identified.

8. Certification Statement

Conquest Solutions, LLC believes the practices described above are reasonable and can be expected to significantly reduce the origination of illegal robocall traffic on its network, consistent with the "reasonable steps" standard of 47 CFR § 64.6305. The undersigned officer will execute the certification under penalty of perjury within the Robocall Mitigation Database filing system.