

## Robocall Mitigation Program Description

Provider: DFWCloudphones DBA Advanced Communications Group

Date: December 16, 2025

DFWCloudphones DBA Advanced Communications Group ("the Provider") is a voice service provider offering cloud-based VoIP telecommunications services. The Provider is committed to preventing illegal and unlawful robocalls from originating on or transiting its network in compliance with Federal Communications Commission (FCC) rules, including those established under the TRACED Act and 47 CFR § 64.6305.

### STIR/SHAKEN Implementation Status

#### Robocall Mitigation

The Provider has implemented a comprehensive robocall mitigation program that includes specific, reasonable steps to avoid originating, carrying, or processing illegal robocall traffic. All calls on the Provider's network are subject to this program. Key elements include:

##### Know Your Customer (KYC) Procedures

The Provider maintains robust processes to vet new and renewing customers to prevent them from using the service to originate illegal robocalls:

- Collection and verification of customer identity, business information, physical address, contact details, and intended use of service.

- Review of customer-provided documentation (e.g., business licenses, EIN, or equivalent).

- Prohibition on anonymous or prepaid sign-ups without verification.

- Contracts explicitly prohibit the origination of illegal robocalls, unlawful spoofing, or violations of the Telephone Consumer Protection Act (TCPA).

- Ongoing monitoring of customer traffic patterns, with suspension or termination for suspected abuse.

##### Know Your Upstream Providers

The Provider only accepts traffic from reputable upstream providers and carriers that are registered in the FCC's Robocall Mitigation Database (RMD). Traffic from unregistered or blocked providers is refused. Upstream agreements include requirements for compliance with robocall mitigation standards.

##### Call Analytics and Monitoring

The Provider employs real-time call analytics and monitoring systems to identify and block suspected illegal traffic:

- Analysis of call detail records (CDRs) for anomalous patterns (e.g., high-volume short-duration calls, unusual calling patterns).

- Rate limiting on new accounts and high-risk traffic.

- Integration with industry traceback consortium requests, with a commitment to respond fully and within 24 hours.

- Use of honeypots or similar tools to detect potential abuse (where applicable).

- No third-party analytics vendors are currently utilized, but internal systems and manual reviews are in place.

##### Response to Traceback and Enforcement

The Provider commits to cooperating fully with the Industry Traceback Group, FCC, law enforcement, and other authorities on traceback requests and investigations into suspected illegal robocalls.

##### Additional Measures

- Blocking of known high-risk number ranges or patterns associated with illegal robocalls.

- Customer education on legal calling practices.

- Regular internal reviews and updates to the mitigation program to align with evolving FCC guidance and industry best practices.

The Provider has no history of formal FCC, law enforcement, or regulatory actions related to illegal robocalls or deficient mitigation efforts.

This program is designed to effectively mitigate illegal robocalls while the Provider works toward full STIR/SHAKEN implementation. The Provider will update this description as needed to reflect enhancements.

##### Contact for Robocall-Related Issues:

Scott Springer CEO 13099 St. Orlin Way Forney Texas 75126 2145872256 [scott@dfwcloudphones.com](mailto:scott@dfwcloudphones.com)]