

ROBOCALL MITIGATION PROGRAM DESCRIPTION

Quasar Data Center

1. Company Information

Quasar Data Center (“Company”) is a non-facilities-based interconnected VoIP provider offering hosted VoIP, SIP-based communications, and related telecommunications services to business customers. The Company provides service under its own branding utilizing underlying carrier and platform partners for PSTN connectivity.

FCC Registration Number (FRN): 0038466470

Principal Business Address: 1001 Texas St. Suite 310, Houston, Texas 77002

Contact Email: dgraytan@quasardata.com

2. Service Description

Quasar Data Center provides interconnected VoIP services, including hosted PBX and SIP-based voice communications. The Company does not operate its own physical telecommunications network infrastructure and instead relies on upstream carrier and platform providers for PSTN interconnection.

All voice services provided by the Company are subject to applicable federal regulations governing interconnected VoIP providers, including robocall mitigation obligations under 47 CFR § 64.6305.

3. STIR/SHAKEN Implementation

The Company does not directly implement STIR/SHAKEN authentication across its network. Instead, Quasar Data Center relies on underlying carrier and platform providers for STIR/SHAKEN call authentication and signaling integrity.

Accordingly, the Company certifies it has not implemented STIR/SHAKEN on its own network and does not hold a direct obligation for STIR/SHAKEN signing infrastructure.

4. Robocall Mitigation Program

Quasar Data Center maintains a robocall mitigation program reasonably designed to prevent, detect, and mitigate the origination of illegal robocall traffic. This program includes:

- Customer identity verification (Know Your Customer / KYC) prior to service activation
 - Prohibition of unlawful, fraudulent, or unsolicited robocalling activity
 - Monitoring of outbound call traffic for suspicious patterns or abuse indicators
 - Investigation and remediation of reported or detected abusive traffic
 - Ability to suspend or terminate services of customers engaged in prohibited activity
 - Maintenance of internal abuse response procedures
 - Cooperation with traceback requests from the FCC, law enforcement, and the Industry Traceback Group
 - Commitment to respond to traceback requests within 24 hours
-

5. Traceback Cooperation

The Company commits to fully cooperate with all traceback requests from the Federal Communications Commission, law enforcement agencies, and authorized industry traceback consortiums. Quasar Data Center will investigate and take appropriate remedial action, including traffic blocking, suspension, or termination of service to prevent further illegal traffic.

6. Customer Use Policy

All customers are prohibited from using Quasar Data Center services for illegal robocalling, spoofing, or any telecommunications fraud. The Company reserves the right to suspend or terminate service for any customer found to be in violation of these policies.

7. Network Architecture

Quasar Data Center operates as a non-facilities-based VoIP provider. The Company relies on upstream carrier and platform partners for PSTN connectivity, routing, and STIR/SHAKEN implementation.

While the Company does not own or operate the underlying telecommunications network, it maintains direct responsibility for customer-level compliance and robocall mitigation controls.

8. Abuse Contact

Abuse and compliance reports may be submitted to:

Email: abuse@quasardata.com

Response Time: Within 24 hours

9. Certification

Quasar Data Center certifies that this robocall mitigation program is reasonably designed to prevent the origination of illegal robocall traffic and that the Company will comply with all applicable requirements under 47 CFR § 64.6305.