

Robocall Mitigation Program Description

Provider: TCG Tech Services

FCC FRN: 0038714036

Provider role: Voice Service Provider

Effective date: 8/4/2026

TCG Tech Services provides interconnected VoIP voice services to business customers. We maintain this Robocall Mitigation Program to prevent the origination of illegal robocalls and unlawful caller-ID spoofing using our network. This program applies to all calls originated by our customers or otherwise originated on our network.

1. STIR/SHAKEN

TCG Tech Services has NOT implemented STIR/SHAKEN on the IP portions of its network because we are We authenticate calls in accordance with our implemented STIR/SHAKEN procedures and use reasonable measures to preserve and transmit caller-ID authentication information.

2. Customer vetting and account controls

Before activating a new customer, and when renewing or materially modifying an account, we use risk-based procedures designed to prevent illegal calling. These procedures include, as applicable:

- Verifying the customer's identity, business name, address, authorized representative, and contact information;
- Evaluating the customer's proposed use of service, expected calling patterns, telephone-number use, and website or other business presence;
- Requiring customers to certify that their use will comply with applicable law, including prohibitions on illegal robocalling and unlawful caller-ID spoofing;
- Screening customers and principals against available risk indicators, including credible complaints, enforcement notices, and adverse public information;
- Reviewing higher-risk customers, high-volume calling, traffic anomalies, sudden calling-volume increases, short-duration or high-answer-seizure calls, and suspicious caller-ID patterns before or after activation; and
- Denying, suspending, restricting, or terminating service when we identify unlawful activity, an unacceptable compliance risk, or a material breach of our service agreement.

Our customer agreements prohibit illegal robocalls, unlawful spoofing, traffic pumping, and use of our services in violation of federal, state, local, or other applicable law. They require customers to provide accurate account information, cooperate with investigations and traceback requests, maintain required consent or other legal authority for their calling, and permit TCG Tech Services to block traffic and suspend or terminate service when necessary to mitigate suspected illegal activity.

3. Traffic monitoring, analytics, and blocking

TCG Tech Services monitors originating traffic using [internal monitoring tools / vendor name(s)] to identify potentially illegal robocall activity. Our monitoring evaluates indicators including abnormal calling volume, call attempts, answer-seizure ratios, short call duration, calling bursts, sequential or rotating caller IDs, invalid or unassigned caller IDs, unexpected international traffic, consumer complaints, traceback information, and other anomalous traffic patterns.

When our monitoring, a complaint, a traceback request, or a law-enforcement or regulatory notice identifies suspected illegal traffic, we investigate promptly. Depending on the facts and risk, we may block identified calls or caller IDs, impose rate or volume limits, require additional customer verification or documentation, suspend the account, terminate service, and preserve relevant records. We periodically review the effectiveness of our monitoring and blocking procedures and adjust controls as warranted.

4. Know-your-upstream-provider procedures

We do not receive upstream voice traffic. Before accepting traffic from an upstream provider, and on an ongoing basis, we use risk-based diligence to evaluate the provider and the traffic it sends. This may include verifying the provider's identity and contact information; confirming its Robocall Mitigation Database status where applicable; reviewing its business purpose, traffic profile, STIR/SHAKEN practices, mitigation procedures, and history of complaints or enforcement concerns; and monitoring traffic for anomalous or unlawful calling patterns.

Our upstream-provider agreements does not include provisions requiring compliance with applicable robocall, spoofing, traceback, and cooperation obligations. We may block, suspend, or terminate traffic from an upstream provider when it presents a credible risk of illegal robocalls, fails to cooperate with an investigation, or otherwise breaches these requirements.

5. Tracebacks, complaints, and enforcement cooperation

TCG Tech Services will respond fully within 24 hours to traceback requests from the FCC, law enforcement, and the Industry Traceback Group or other registered industry traceback consortium. We will cooperate with these entities in investigating and stopping illegal robocalls that use our service.

We maintain procedures to receive, document, investigate, and resolve complaints and compliance escalations. We retain relevant customer, call-detail, signaling, and investigation records in accordance with applicable legal and operational requirements. Our designated robocall-mitigation contact is [Name, Title, Department, Address, Telephone, Email].

6. Governance, training, and review

Responsibility for this program rests with [Name/Title or Compliance Department]. Relevant personnel receive training on customer onboarding, suspicious-traffic escalation, traceback response, and enforcement of account restrictions. We review this program and our mitigation controls periodically and whenever material changes occur in our network, services, customers, traffic sources, laws, or identified risks. We will update our Robocall Mitigation Database filing within 10 business days of a change to required information.

7. Program commitment

TCG Tech Services is committed to implementing and complying with the practices described in this program. These practices are designed to significantly reduce the origination of illegal robocalls on our network. We will not knowingly, or through negligence, originate unlawful robocall campaigns.