

1. Service model and STIR/SHAKEN status

Tech Grips, LLC provides managed interconnected VoIP services to business end users as a non-facilities-based reseller. Tech Grips manages customer PBX systems, endpoints, SIP configurations, telephone-number assignments, and customer support.

Tech Grips does not control the wholesale originating network, SPC token, STI certificate, or carrier infrastructure necessary to implement STIR/SHAKEN. Outbound calls are delivered to our wholesale originating provider for wholesale origination onto the public switched telephone network and STIR/SHAKEN authentication.

2. Customer identification and due diligence

Tech Grips does not permit anonymous or unattended self-service registration for voice service.

Before activating a customer, Tech Grips obtains and verifies information including:

- Legal business name and physical address
- State registration or other business-formation information
- Authorized representative's name and contact information
- Business website, telephone number, and stated business activities
- Service locations and intended use of the voice service
- Billing information and executed service agreement

Tech Grips evaluates whether the requested services, telephone numbers, channel capacity, expected traffic volume, and calling destinations are reasonable for the customer's stated business purpose.

Tech Grips may deny, delay, restrict, suspend, or terminate service when information cannot be verified or when the customer presents an elevated fraud or abuse risk.

3. Telephone-number and caller-ID controls

Tech Grips permits customers to transmit only caller-ID numbers that:

1. Were assigned to the customer through Tech Grips or its upstream provider;
2. Were ported for the customer; or
3. Were independently verified as numbers the customer is authorized to use.

Customer PBX outbound routes and caller-ID settings are restricted to an approved allowlist. Arbitrary caller-ID spoofing is prohibited.

Tech Grips retains documentation supporting customer authorization to use telephone numbers when the numbers were not originally assigned through Tech Grips.

4. Acceptable-use restrictions

Tech Grips prohibits:

- Illegal robocalling or spoofing
- Fraudulent, deceptive, abusive, or harassing calls
- Unauthorized telemarketing or automated dialing
- Calls impersonating government agencies, financial institutions, or other third parties
- Use of compromised SIP credentials or unauthorized calling systems
- Attempts to conceal the actual source of telephone traffic

Telemarketing, predictive dialing, high-volume short-duration calling, polling, collections, or call-center activity requires prior written disclosure and approval.

5. Technical security controls

Tech Grips uses controls appropriate to each customer, including:

- Separate SIP credentials or subaccounts for each customer
- Unique, randomly generated credentials
- IP-based access restrictions where practical
- Restricted outbound caller-ID values
- International and high-risk destination restrictions by default
- Concurrent-call limits appropriate to the customer
- PBX firewalling and endpoint-access controls
- Prompt revocation of compromised credentials
- Logging through our custom PBX CDR/CEL records and the wholesale originating provider's call-detail records

6. Monitoring and analytics

Tech Grips uses the wholesale originating provider's call-detail and usage reporting together with our custom PBX's CDR/CEL records to identify potentially unlawful or compromised traffic.

Tech Grips reviews available call records and traffic data for indicators including:

- Sudden or unexplained increases in calling volume
- Large quantities of short-duration calls

- Sequential or highly repetitive dialing
- Calling inconsistent with the customer's business purpose
- Calls originating outside expected hours
- Attempts to use unauthorized caller-ID numbers
- Calls to unusual, premium-rate, international, or high-risk destinations
- Evidence of compromised SIP credentials

Tech Grips does not currently use a separate third-party robocall analytics vendor. Tech Grips uses the account-level records and monitoring procedures described above to identify potentially unlawful or compromised traffic. Network-level STIR/SHAKEN authentication and upstream traffic handling occur within the wholesale originating network outside Tech Grips' control.

7. Upstream-provider diligence

Tech Grips maintains a direct commercial relationship with a wholesale provider that supplies SIP origination and termination services.

Before placing customer traffic into production, Tech Grips verifies that its upstream provider maintains an active Robocall Mitigation Database filing and requires reseller compliance with applicable FCC requirements.

Tech Grips periodically reviews the upstream provider's regulatory status, applicable terms, and abuse-reporting procedures.

8. Investigation, suspension, and termination

Tech Grips investigates credible complaints, usage anomalies, traceback requests, or indications of unlawful traffic.

Depending on the circumstances, Tech Grips may:

- Temporarily restrict outbound calling
- Disable affected SIP credentials
- Block specific destinations
- Require the customer to provide supporting documentation
- Preserve relevant call and account records
- Notify or cooperate with the upstream provider
- Suspend or terminate the customer's service

Tech Grips will not knowingly continue transmitting unlawful robocall traffic.

9. Traceback cooperation

Tech Grips, LLC will authenticate and investigate traceback requests received from the Federal Communications Commission, authorized civil or criminal law-enforcement entities, or the designated Industry Traceback Consortium. Tech Grips will respond fully within the applicable 24-hour response period using records reasonably necessary to identify the source and routing of the call at issue. Tech Grips will cooperate with those entities in investigating and stopping illegal robocallers that may use its service to originate calls.

Tech Grips will limit disclosures to information reasonably necessary to respond to the specific traceback, investigate the identified traffic, and mitigate substantiated unlawful or abusive use. Tech Grips will not disclose unrelated customer information, credentials, communications content, or unrelated call records except when required by applicable law or valid legal process.

Tech Grips may dispute inaccurate traceback information or report that identified traffic was lawfully originated. Where unlawful, abusive, unauthorized, or compromised traffic is substantiated, Tech Grips will take proportionate corrective action appropriate to the circumstances.

10. Review and maintenance

Tech Grips reviews this program periodically and whenever there is a material change in its voice-service architecture, upstream providers, customer-onboarding procedures, or traffic-monitoring systems.