

Robocall Mitigation Plan – Galveston Computer Solutions LLC

Company: Galveston Computer Solutions LLC

FRN: 0031437429

Business Address: 523 24th Street, Suite 5, Galveston, TX 77550

Contact: Steve Burdick, President (steveb@galvcs.com, 409-762-4326)

1. STIR/SHAKEN Implementation Status

Galveston Computer Solutions LLC provides voice services through wholesale carrier partners

that are fully STIR/SHAKEN compliant. All outbound calls placed through our platform are

signed at origination by our upstream provider(s).

- We do not directly originate unauthenticated calls onto the PSTN.**
- We rely on our carrier partners (e.g., Bandwidth) for full STIR/SHAKEN authentication and attestation.**

2. Robocall Mitigation Practices

For any traffic not signed under our own attestation, we implement the following controls:

• Customer Vetting:

All new business customers are manually screened prior to enabling outbound calling.

We verify identity, business legitimacy, and service use-case.

• Traffic Monitoring:

We actively monitor outbound call patterns for high-volume, short-duration, sequential, or otherwise suspicious robocall-like traffic. Calls that exceed normal thresholds or show unusual patterns are flagged and subject to review.

• Call Blocking / Restrictions:

If abnormal or suspicious activity is detected, we immediately suspend outbound traffic pending investigation. Repeat offenders are permanently disconnected.

• Ongoing Review:

Our compliance team conducts periodic audits of call logs and proactively communicates with upstream carriers to address potential issues.

3. Human Principals

• Steve Burdick – President

• Billie Burdick – Vice President

4. Point of Contact for Mitigation Issues

• Name: Steve Burdick

• Title: President

• Department: Voice Services

• Phone: 409-762-4326

• Email: steveb@galvcs.com

This contact information is to be used by the FCC, law enforcement, or other carriers for robocall

mitigation inquiries.

5. Prior FCC Actions / Investigations

Yes — Galveston Computer Solutions LLC was removed from the Robocall Mitigation Database

under DA 25-737 (August 25, 2025) due to an incomplete filing. The company has now corrected its submission to include human principals and complete responses as required, and

certifies ongoing compliance with FCC rules.

6. Certification

Galveston Computer Solutions LLC certifies that it has implemented the above robocall mitigation practices in compliance with the FCC's rules and will maintain these practices on an ongoing basis.

Know Your Customer (KYC)

1. Company profile and traffic type

Galveston Computer Solutions LLC is a small VoIP service provider / IT services firm that primarily serves small and medium-sized business customers. Our customers use our voice services for standard person-to-person and informational calling (e.g., customer support, appointment reminders, business communications). We do **not** target or market to outbound call centers engaged in high-volume lead generation, debt collection, or telemarketing campaigns.

We do not knowingly originate illegal robocall traffic, and we have implemented a KYC and traffic monitoring program designed to prevent our network from being used for unlawful robocalls in violation of the TCPA, TSR, or applicable state laws.

2. New customer onboarding and identity verification

Before enabling outbound calling for any customer, we perform KYC checks to verify identity, business legitimacy, and the intended use of our voice services. At a minimum, for each new customer we:

- Collect full legal **business name, DBA (if any), physical address, phone number, and email address**
- Collect **EIN** and state of incorporation or business registration (for businesses), or government-issued ID (for individuals/sole proprietors)
- Verify business information against **public business records** (e.g., Secretary of State or similar databases)
- Verify domain ownership or control for business email addresses where possible

- Require the customer to sign our **Service Agreement** and **Acceptable Use Policy (AUP)**, which:
 - Prohibits illegal robocalls, spoofing, and other abusive practices
 - Requires compliance with the TCPA, TSR, state telemarketing laws, and do-not-call rules
 - Prohibits the use of our service for autodialed or prerecorded telemarketing calls without proper consent and legal compliance

If the customer's answers are incomplete, inconsistent, or indicate high-risk use (e.g., "lead generation," "cold calling," "mass marketing"), the application is escalated for manual review by management. We may request additional documentation (e.g., sample call scripts, proof of consent process, copies of compliance policies) and we reserve the right to **deny service** if risk cannot be mitigated.

3. Caller ID / number assignment and verification

We only assign or port telephone numbers through reputable carriers and require that:

- The customer may use only caller IDs that they **own or are authorized to use**
- Caller ID names and numbers must accurately represent the calling party and may not be used to mislead or impersonate others
- We do not permit "neighbor spoofing," rotating caller IDs to evade blocking, or use of invalid/unallocated numbers

For any customer requesting large quantities of numbers or frequent changes to caller ID, we conduct additional review to confirm the legitimacy of the use case.

4. Use of analytics and monitoring

We **do not currently use a separate third-party analytics vendor** for call scoring; instead, we rely on:

- Analytics and signaling feedback provided by our upstream carrier(s)
- Our own monitoring of call detail records (CDRs) and traffic patterns

We periodically review traffic for each customer to identify patterns indicative of possible illegal robocalls, including:

- High volumes of very short-duration calls
- Unusual spikes in call attempts, especially to known high-risk NPAs or destinations
- High answer-to-attempt ratios with very short calls, or extremely low answer ratios
- Multiple calls in short succession to the same destination number(s)

If our upstream carrier or another provider notifies us of suspicious or abusive traffic originating from our network, or if we receive traceback requests or end-user complaints, we immediately investigate the associated customer and call records.

5. Application of KYC to existing customers

Our KYC plan applies not only to new customers but also to **existing customers**:

- We are in the process of performing a **KYC refresh** of our entire existing customer base, verifying business identity, contact details, and the nature of their calling use cases
- For existing customers, we review:
 - Current address and contact information
 - Business registration / EIN (where applicable)
 - Types of calls they place (e.g., internal business calls, customer support, appointment reminders, etc.)
- Any existing customer whose traffic profile appears high-risk (e.g., high-volume outbound campaigns, short call durations, high complaint rates) is subject to enhanced due diligence, including:
 - Requesting additional documentation (e.g., TCPA compliance procedures, consent process, recordings or scripts)
 - Reviewing tracebacks and any known complaints

Existing customers who cannot satisfy our KYC requirements or who refuse to cooperate with reviews may have their outbound calling **restricted or terminated**.

We will complete the initial review of existing customers and then perform **periodic reviews at least annually**, and more frequently for any high-risk or high-volume customer.

6. Handling of complaints, tracebacks, and high-risk traffic

We maintain a point of contact for robocall or abuse complaints. When we receive:

- A traceback request from the USTelecom Industry Traceback Group or another provider
- A complaint from a recipient of a call claiming it was illegal or unwanted
- A notice from an upstream carrier about potentially illegal or abusive traffic

We will:

1. Acknowledge the request and respond within a reasonable timeframe (typically within one business day)
2. Identify the responsible customer and examine relevant CDRs and call recordings (if available)
3. Evaluate whether the calls appear to be:
 - Misdialed / operational errors
 - Potentially abusive but correctable behavior
 - Clearly illegal robocalls or spoofing

Depending on the findings, we may:

- Warn the customer and require changes to their practices
- Require written confirmation of their compliance measures (including consent procedures)
- Block or rate-limit specific destinations or traffic types
- Suspend or terminate the customer's service where we determine that illegal robocalls have occurred or will likely continue

We fully cooperate with traceback efforts and other law enforcement inquiries relating to suspected illegal robocalls.

7. Call authentication and cooperation with upstream carriers

We work with our upstream carrier(s) to ensure that outbound calls are **authenticated under STIR/SHAKEN** where applicable and that caller ID is not manipulated in a way that would undermine call authentication. We comply with any reasonable requests from our carrier(s) to adjust calling patterns, enforce restrictions, or terminate problem accounts when there is evidence of illegal robocall activity.

8. Prohibited use and enforcement

Our service agreements and AUP explicitly prohibit:

- Placing calls in violation of the TCPA, TSR, or applicable state laws
- Spoofing caller ID to defraud, cause harm, or wrongfully obtain anything of value
- Originating high-volume prerecorded or autodialed telemarketing calls without proper prior express consent
- Use of our services to facilitate scams, fraud, or other unlawful activity

Violation of these terms may result in immediate **suspension or termination** of service, in addition to any other remedies available under law.

This KYC and robocall mitigation plan is implemented across our customer base and is subject to ongoing review and improvement as regulations, enforcement guidance, and industry best practices evolve.