



Robocall Mitigation Program and Voice Service Provider Policy

Filing profile	Detail
Company	Gaston Software, Inc.
Business address	133 Gaston Dr., Bastrop, TX 78602
Product	Notive Health
Provider role	United States non-facilities-based interconnected VoIP reseller
Underlying Provider	SignalWire, Inc. — voice origination and carrier-network provider, engaged August 5, 2026. FRN 0028100428; RMD RMD0003809, "Complete STIR/SHAKEN Implementation," verified active against the Commission's public RMD dataset on August 5, 2026. A change of provider triggers an amendment — see § 15.
RMD certification position	Option 3 — No STIR/SHAKEN Implementation
Policy version	1.4
Effective date	August 5, 2026
Policy owner	Chief Executive Officer and designated Robocall Mitigation Database contact
Review cadence	At least annually, before each March 1 RMD recertification, and after every material voice-service change
Next scheduled review	February 1, 2027
Publication status	Public filing copy; no confidential technical thresholds, credentials, customer information, or call records are included

Gaston Software, Inc. implements this program for every call that it originates or enables through its voice service. The company prohibits its services from being used to originate illegal robocalls or unlawfully spoof caller identification information and commits to respond fully within 24 hours to traceback requests from the Federal Communications Commission, law enforcement, and the industry traceback consortium.

1. Purpose and governing requirements

This policy establishes Gaston Software, Inc.'s program for preventing, detecting, investigating, and stopping illegal robocalls and spoofing. It is intended to satisfy the voice service provider obligations in 47 CFR §§ 64.6305(a) and 64.6305(d), the traceback and customer-due-diligence obligations in 47 CFR § 64.1200(n), and the filing requirements applicable to the Robocall Mitigation Database (RMD).

The program separates two duties that must not be conflated:

1. **STIR/SHAKEN implementation:** whether Gaston controls the network infrastructure necessary to authenticate calls using its own Service Provider Code (SPC) token and certificate.
2. **Robocall mitigation:** the customer diligence, caller-ID controls, monitoring, traceback cooperation, investigation, and enforcement Gaston performs even though it does not implement STIR/SHAKEN on its own network.

Reliance on an upstream carrier does not transfer or eliminate Gaston's independent robocall mitigation, traceback, RMD filing, or filing-update duties.

2. Scope

This program applies to:

- every employee, contractor, customer, end user, account, number, credential, application, and endpoint that can originate a voice call through a service offered by Gaston;
- every United States North American Numbering Plan number used as caller identification through that service;
- any Underlying Provider — the voice origination and carrier-network provider identified in the filing profile above — together with any replacement or additional upstream provider engaged in the future; and
- customer onboarding, number assignment, outbound calling, call-detail records, complaints, traceback requests, investigations, suspension, termination, and regulatory filings.

Gaston does not permit a customer to resell, wholesale, or provide Gaston's voice service to another voice service provider without prior written approval, enhanced diligence, proof of an active and accurate RMD filing where required, and an update to this program when the arrangement changes Gaston's role.

3. Option 3 implementation position and applicable exemption

3.1 Applicable Commission authority

47 CFR § 64.6301(a) requires a voice service provider to implement STIR/SHAKEN in its Internet Protocol networks, subject to applicable exceptions. In the First Caller ID Authentication Report and Order, FCC 20-42, paragraph 40, the Commission clarified that its implementation rules do not apply to providers that lack control of the network infrastructure necessary to implement STIR/SHAKEN. The Commission continues to recognize this lack-of-network-control implementation exemption separately from the extensions codified in 47 CFR § 64.6304.

Under 47 CFR § 64.6305(d)(2)(i), a provider that is unable to implement STIR/SHAKEN because it lacks the necessary network control must explain that condition in its RMD certification. Gaston relies on the Commission's lack-of-network-control clarification in FCC 20-42, paragraph 40; it does not rely on the expired small-provider extensions. The absence of an SPC token or certificate is evidence consistent with Gaston's network position, but it is not, by itself, the legal basis for this exemption.

3.2 Why the exemption applies to Gaston

Gaston is a non-facilities-based VoIP reseller. For calls within the scope of this program, Gaston may configure its application, customer accounts, endpoints, authorized telephone numbers, and routing to the upstream provider, but it does not own, lease, operate, or control the carrier-network infrastructure necessary to implement the STIR/SHAKEN framework. In particular, Gaston does not control the carrier switching and interconnection facilities, the Secure Telephone Identity Authentication Service, the insertion of STIR/SHAKEN Identity headers at the carrier edge, an SPC token, or a Secure Telephone Identity certificate.

Gaston's Underlying Provider is SignalWire, Inc., which supplies the voice origination and carrier-network service and controls the network elements and credentials used to authenticate eligible outbound calls at its network edge. SignalWire certifies Complete STIR/SHAKEN Implementation in its own RMD filing, RMD0003809. Gaston does not characterize a call signed with the Underlying Provider's certificate as a call authenticated with Gaston's own certificate, and does not certify that such signing constitutes partial or complete STIR/SHAKEN implementation by Gaston.

Gaston therefore selects **Option 3 – No STIR/SHAKEN Implementation**. This position depends on the facts above. Before Gaston acquires or controls a carrier softswitch, session border controller used for carrier interconnection, authentication service, SPC token, certificate, attestation-level decision process, or comparable network function, the Policy Owner must obtain a documented compliance review and update the RMD filing within the required period. Merely hiring a third party to perform the technological act of signing calls would not preserve this exemption if Gaston otherwise has an implementation obligation.

3.3 Supplemental explanation for the RMD form

Gaston Software, Inc. relies on the implementation exemption recognized in the First Caller ID Authentication Report and Order, FCC 20-42, paragraph 40, for providers that lack control of the network infrastructure necessary to implement STIR/SHAKEN. Gaston is a non-facilities-based VoIP reseller. Gaston does not own, lease, operate, or control carrier switching or interconnection facilities, a Secure Telephone Identity Authentication Service, or the network elements that insert STIR/SHAKEN Identity headers at a carrier edge; it does not possess a Service Provider Code token or a Secure Telephone Identity certificate; and it has not implemented STIR/SHAKEN on any portion of a carrier network.

Gaston's Underlying Provider is SignalWire, Inc., which supplies voice origination and carrier-network service. SignalWire owns and controls the authentication infrastructure and signs eligible outbound calls using its own credentials; it certifies Complete STIR/SHAKEN Implementation in its own RMD filing, RMD0003809. Gaston does not claim those signatures as its own implementation, and will amend this filing within the period required by 47 CFR § 64.6305(d)(5) if the Underlying Provider changes.

Gaston remains fully subject to its robocall mitigation, customer-due-diligence, traceback, and RMD obligations, and performs the program described in this document.

4. Know-your-customer program

Gaston takes affirmative, effective measures to know every direct voice-service customer and to prevent new or renewing customers from using its service to originate illegal calls.

4.1 Before activation

Voice service must not be activated anonymously or immediately through an unreviewed self-service signup. Before activation, Gaston collects and verifies, using records appropriate to the customer's risk:

- legal business name, any doing-business-as name, physical service address, formation jurisdiction, and business registration or tax identifier;
- the identity, role, business email address, and direct contact information of at least one authorized representative;
- the customer's website or other evidence of its bona fide operations;

- the nature of the customer's business, intended calling use cases, expected destinations, anticipated call volume and call-initiation rate, and whether automated or prerecorded calling is proposed;
- the telephone numbers the customer is authorized to use and the basis for that authorization; and
- whether the customer will provide voice service to third parties or is otherwise required to maintain its own RMD filing.

Gaston compares submitted information for material inconsistencies and may request formation records, government-issued identification, an IRS document, proof of address, proof of number ownership or right to use, contracts, regulatory registrations, or other corroborating records. Service is denied or held when the customer cannot be identified, the proposed use is unclear, material information is inconsistent, or the risk of unlawful traffic is not adequately resolved.

4.2 Continuing diligence

Customer information is reviewed at renewal, at least annually while voice service is active, and whenever ownership, control, address, calling use, number inventory, expected traffic, or an authorized contact materially changes. Gaston also performs an immediate review after a traceback request, government inquiry, material complaint, carrier warning, suspicious traffic alert, unusual account activity, or credential compromise.

Accounts use named users, role-appropriate access, strong authentication, and multi-factor authentication where the service supports it. Shared administrative credentials are prohibited. Access is removed promptly when a user's authority ends.

5. Know-your-upstream-provider program

The Underlying Provider is SignalWire, Inc. Before enabling traffic with any upstream provider, and at least annually thereafter, Gaston:

- verifies the contracting carrier's legal identity, business contact, and escalation contact;
- verifies that the applicable provider's RMD filing appears active and has not been removed by Commission action;
- documents which party provides numbering, origination, switching, interconnection, caller-ID authentication, traceback support, analytics, blocking, and call-detail records;
- completes the provider's required KYC and STIR/SHAKEN account-validation processes;
- confirms that Gaston can retrieve or timely obtain the records needed to answer a traceback request;
- reviews material changes to the provider's terms, signing practices, RMD status, ownership, or network role; and
- prohibits routing through an unapproved provider or through a provider whose RMD status makes acceptance of its traffic unlawful.

The Underlying Provider's RMD filing was verified against the Commission's public Robocall Mitigation Database dataset on August 5, 2026: RMD0003809, FRN 0028100428, SignalWire, Inc., "Complete STIR/SHAKEN Implementation," voice service provider, active and not removed by Commission action.

5.1 Contractual provisions with the Underlying Provider

Gaston's service agreement with the Underlying Provider incorporates that provider's acceptable-use and traffic terms. Described in general terms, those provisions prohibit unlawful calling, illegal robocalls, and unlawful manipulation of caller identification information; require Gaston to comply with applicable calling law and with the provider's number-authorization and traffic requirements; obligate Gaston to cooperate in traceback and fraud investigations; and permit the provider to apply traffic-level controls, to suspend or restrict service, and to terminate for violation. Provisions of this kind are typically included in Gaston's upstream agreements. Gaston does not route traffic through an upstream provider whose terms fail to prohibit unlawful calling, and reviews those terms for material change under Section 5.

The applicable carrier legal entity, RMD identifier, contract, account validation, review date, and escalation contacts are maintained in Gaston's non-public compliance records. A change in upstream provider requires approval by the Policy Owner before traffic is moved.

6. Caller-ID, number, and access controls

Gaston uses the following controls to reduce spoofing and unauthorized origination:

- Outbound caller identification is restricted to a number provisioned to the relevant account or a number for which the customer has supplied proof of a current right to use and the Underlying Provider has approved the number for the account.
- Arbitrary caller-ID substitution, caller-ID rotation intended to evade blocking, and presentation of invalid, unallocated, unused, or unauthorized numbers are prohibited.
- Numbers designated as inbound-only must not be used for outbound calling. Gaston communicates applicable number status to the upstream provider and maintains a reasonable do-not-originate control through its authorized-number allowlist.
- Calling credentials and network access are limited to approved systems and users. Suspected credential compromise triggers immediate containment, credential rotation, record preservation, and traffic review.
- Administrative changes to number assignments, caller-ID authorization, routing, or calling privileges are restricted to authorized personnel and recorded.
- International, high-cost, high-rate, or other elevated-risk calling capabilities are disabled unless the customer's verified use requires them and the risk is approved.

7. Acceptable use and prohibited traffic

Customers and users may place only lawful calls for legitimate business, healthcare, administrative, or customer-service purposes. They must comply with the Telephone Consumer Protection Act, Truth in Caller ID Act, federal and state do-not-call requirements, consent and revocation requirements, and other applicable calling laws.

The service must not be used for:

- illegal robocalls, unlawful spoofing, scams, impersonation, harassment, threats, phishing, or fraudulent solicitation;
- calls using a caller-ID number the caller is not authorized to use;
- traffic intended to evade carrier analytics, blocking, traceback, law enforcement, or consumer opt-out requests;
- lead-generation, traffic-pumping, short-duration mass calling, or high-volume dialing inconsistent with the customer's approved use;
- transmitting prerecorded or artificial-voice messages, operating a predictive dialer, or conducting a bulk outbound campaign unless Gaston has separately approved the specific use in writing after the customer documents the lawful basis, consent controls, do-not-call controls, identification disclosures, opt-out handling, and supervision; or
- resale or wholesale use that Gaston has not expressly approved under Section 2.

Approval of a use case never authorizes illegal calls. Gaston may impose more restrictive controls than applicable law or the upstream provider.

7.1 Contractual provisions with customers and end users

The prohibitions in this section are contractual, not advisory. Described in general terms, Gaston's voice service terms are incorporated into every customer agreement — Gaston does not offer voice service on terms that omit them — and they: require compliance with the Telephone Consumer Protection Act, the Truth in Caller ID Act, and applicable federal and state do-not-call, consent, and revocation requirements; prohibit use of a caller-identification number the customer is not authorized to use; require Gaston's prior written approval before any prerecorded, artificial-voice, predictive-dialer, bulk-

campaign, or resale use; require the customer to supply and keep current the diligence information described in Section 4; obligate the customer to cooperate with traceback, complaint, and investigation requests; and reserve Gaston's right to rate-limit, block a number, disable a credential, suspend, or terminate without prior notice where immediate action is warranted or where notice is prohibited or would compromise an investigation. Provisions of this kind are typically included in Gaston's customer agreements.

8. Traffic monitoring and analytics

Gaston uses a layered monitoring program. Gaston reviews customer, account, number, complaint, security, and call-detail information under operational rules. For carrier-network analytics and network blocking, Gaston relies on the Underlying Provider. Gaston does not identify a separate third-party robocall analytics vendor other than this reliance on the Underlying Provider as the upstream network provider.

The program reviews or escalates indicators that may include:

- an unexpected increase in outbound volume or call-initiation rate;
- outbound traffic materially exceeding the customer's documented use or inbound activity;
- repeated short-duration calls, low answer rates, abnormal failure patterns, or rapid number changes;
- calls outside expected times, geographies, destinations, or business purpose;
- repeated use of the same content or calling pattern across large destination sets;
- attempts to use an unauthorized or mismatched caller-ID number;
- carrier surcharge, fraud, spam-label, reputation, KYC, or policy alerts;
- complaints, opt-out failures, traceback requests, subpoenas, or government inquiries; and
- account takeover indicators or suspicious portal, credential, or configuration activity.

Thresholds are risk-based and may be adjusted to avoid publishing evasion guidance. An alert is investigated in context; it is not treated as proof of wrongdoing. Gaston may rate-limit, block a caller-ID number, disable a credential, pause outbound calling, require additional customer evidence, or suspend the entire account while an investigation is pending. Confirmed illegal traffic results in termination and any additional cooperation or reporting required by law.

9. Traceback response and cooperation

Gaston commits to respond fully within 24 hours to every traceback request from the Commission, civil or criminal law enforcement, or the industry traceback consortium, and to cooperate with those entities in investigating and stopping illegal robocallers that use its service.

The designated RMD contact is responsible for ensuring that traceback communications are monitored, preserved, acknowledged, investigated, and answered without avoidable internal delay. The response process is:

1. Authenticate the request and record the time received, requester, case identifier, numbers, timestamps, and response deadline.
2. Preserve relevant customer, account, number, credential, configuration, complaint, and call-detail records.
3. Search Gaston's records and promptly escalate to the Underlying Provider when carrier records or network action are required.
4. Identify the direct customer or account, the originating caller-ID number, the upstream provider, the immediate call path known to Gaston, and the requested call details.
5. Fully answer the requester within 24 hours, even when the response must state which information is held by the upstream provider and what action has been taken to obtain it.
6. Investigate related traffic and take proportionate containment action, including suspension or termination when warranted.

7. Cooperate with follow-up questions, lawful process, preservation requests, and efforts to identify and stop the responsible caller.

Gaston does not notify a customer about a traceback or investigation when notice is prohibited, would compromise an investigation, or is otherwise inappropriate under law or the requester's instructions.

10. Complaints, investigations, and remediation

Robocall, spoofing, unwanted-call, and caller-ID complaints are routed to the designated compliance contact. Gaston records the complainant's contact information when supplied, the numbers and call times involved, the allegation, related account and call records, investigative steps, carrier communications, interim controls, conclusion, and corrective action.

A credible complaint receives prompt triage. Multiple complaints, a complaint corroborated by call records, a government or carrier notice, or evidence of fraud triggers immediate review and may trigger a temporary traffic hold. Gaston does not wait for a final adjudication before taking a reasonable protective action.

When a violation is substantiated, Gaston may:

- block the number or calling function;
- reset or revoke credentials;
- require a corrective-action plan and additional proof;
- reduce call limits or remove elevated-risk capabilities;
- suspend or terminate the customer or user;
- notify and coordinate with the Underlying Provider;
- preserve and provide records in response to lawful requests; and
- update this program, training, contracts, product controls, or the RMD filing.

Gaston does not restore suspended service until the Policy Owner documents that the risk has been resolved and any required carrier or government direction has been satisfied.

11. Records and evidence

Gaston maintains sufficient non-public records to demonstrate and operate this program, including:

- customer identity and diligence records, risk reviews, approved use cases, and authorized contacts;
- customer agreements, acceptable-use acknowledgments, number authorization, and approval records;
- upstream-provider diligence, RMD verification, contracts, KYC validation, escalation contacts, and material-change reviews;
- number inventory, account and credential linkage, call-detail records available to Gaston, and procedures for obtaining carrier records;
- monitoring alerts, complaints, investigations, traffic holds, suspensions, terminations, and remediation;
- traceback requests, responses, supporting records, deadlines, and follow-up cooperation;
- annual policy reviews, training, RMD certifications, recertifications, and updates; and
- any relevant Commission, law-enforcement, or regulatory action or investigation involving Gaston, an affiliate, or an entity with shared ownership, management, directors, or control.

Records are retained for at least two years after the related service, agreement, investigation, or response ends, or longer when another law, contract, litigation hold, or company retention rule requires it. Access is limited to personnel with a business need. Customer information and call records are not placed in the public RMD attachment.

12. Training and accountability

Personnel who sell, provision, support, administer, monitor, or investigate voice service receive training before receiving access and at least annually thereafter. Training covers:

- prohibited robocalls and spoofing;
- customer and upstream-provider diligence;
- approved caller-ID and number handling;
- recognizing anomalous traffic and account compromise;
- complaints, preservation, escalation, and suspension;
- the 24-hour traceback commitment;
- confidentiality and lawful disclosure of customer and call information; and
- RMD accuracy, change reporting, and annual recertification.

Violations by workforce members may result in access removal and disciplinary action. Contractors with relevant access are subject to equivalent obligations.

13. RMD and CORES governance

The Policy Owner must ensure that:

- RMD and Commission Registration System credentials use multi-factor authentication and remain accessible to an authorized successor;
- the RMD filing, this program description, provider role, implementation selection, contact information, ownership and principal information, upstream-provider description, analytics description, and investigation disclosures remain accurate;
- any changed RMD information is updated within 10 business days as required by 47 CFR § 64.6305(d)(5);
- changed CORES information is updated within 10 business days as required by 47 CFR § 1.8002(b)(2);
- the RMD filing is reviewed, recertified, and resubmitted on or before March 1 each year as required by 47 CFR § 64.6305(h); and
- Option 3 is reconsidered before any technical, contractual, ownership, or operational change that could give Gaston control of the infrastructure or decisions necessary to implement STIR/SHAKEN.

The officer submitting the RMD certification must verify the filing and supporting evidence for truth, accuracy, and completeness. A vendor statement, an upstream signature, or the absence of contrary evidence is not sufficient by itself.

14. Program approval and review

The Chief Executive Officer is accountable for this program and may designate a compliance lead and operational responders. The program is reviewed:

- before each annual RMD recertification;
- after a traceback request, substantiated illegal-traffic event, or material complaint pattern;
- after a change in upstream carrier, calling architecture, number provider, analytics, signing arrangement, customer type, resale model, or automated-calling capability;
- after an applicable FCC rule, order, filing instruction, or enforcement advisory changes; and
- whenever Gaston obtains or becomes eligible to obtain and use network infrastructure, an SPC token, or a certificate in a manner that may change its implementation obligation.

Material changes are documented, approved, communicated to affected personnel, and reflected in the RMD within the applicable deadline.

15. Revision history

Section 14 requires material changes to be documented, approved, and reflected in the RMD within the applicable deadline. This section is that record.

Version	Effective	Change	Approved by	RMD update
1.0	July 25, 2026	Initial program. Identified a prospective upstream provider.	CEO	Filed
1.1	—	Superseded before filing. Not submitted.	—	—
1.2	August 4, 2026	Carrier-neutral revision. The prospective upstream provider named in version 1.0 declined Gaston's account at its own customer-diligence review on July 27, 2026. No service was activated and no traffic was ever carried under version 1.0. This version states Gaston's actual position — no upstream provider engaged, no voice traffic carried — and rewrites section 3.3 so the lack-of-network-control exemption rests on Gaston's own facts rather than any carrier's identity. Structured RMD field values are unchanged and remain accurate.	CEO	Amended attachment, filed August 5, 2026
1.4	August 5, 2026	Contractual-provision description added. New Sections 5.1 and 7.1 describe, in general terms, the provisions in Gaston's upstream agreement and in its customer agreements that are designed to mitigate illegal robocalls, and state whether such provisions are typically included. This responds to 47 CFR § 64.6305(d)(2)(ii) as explained in Wireline Competition Bureau Public Notice DA 24-73, which requires providers describing their "new and renewing customer" and "know-your-upstream provider" procedures to describe any such contractual provisions. No other substantive change; the Section 3 implementation position and all structured RMD field values are unchanged.	CEO	Amended attachment
1.3	August 5, 2026	Upstream provider engaged. Gaston entered into service with SignalWire, Inc. on August 5, 2026 and began provisioning telephone numbers. Version 1.2's statements that no upstream provider was under contract and no voice traffic was carried were accurate when filed earlier that day and ceased to be accurate upon that engagement; this amendment follows within the period required by 47 CFR § 64.6305(d)(5). This version names SignalWire in the filing profile and in sections 3.2, 3.3, and 5, and records verification of SignalWire's own RMD filing. The section 3 implementation position is unchanged : the lack-of-network-control exemption turns on Gaston's own facts, and Gaston still owns no carrier switching or interconnection facilities, no authentication service, no SPC token, and no certificate. Structured RMD field values are unchanged and remain accurate.	CEO	Amended attachment

A change of upstream provider, or Gaston acquiring control of any network element or credential described in section 3, will change information in this filing and will be reflected in the RMD within the period required by 47 CFR § 64.6305(d)(5), together with an amendment to the filing profile and to sections 3.2, 3.3, and 5.

16. References

- 47 CFR § 64.1200, including paragraphs (n) and (o): <https://www.ecfr.gov/current/title-47/section-64.1200>
- 47 CFR § 64.6301: <https://www.ecfr.gov/current/title-47/section-64.6301>
- 47 CFR § 64.6304: <https://www.ecfr.gov/current/title-47/section-64.6304>
- 47 CFR § 64.6305: <https://www.ecfr.gov/current/title-47/section-64.6305>
- First Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking, FCC 20-42, paragraph 40: <https://docs.fcc.gov/public/attachments/FCC-20-42A1.pdf>
- Wireline Competition Bureau Public Notice, DA 24-73, expanded RMD requirements and filing instructions: <https://docs.fcc.gov/public/attachments/DA-24-73A1.pdf>
- Wireline Competition Bureau Public Notice and RMD Frequently Asked Questions for Filers, DA 26-72: <https://docs.fcc.gov/public/attachments/DA-26-72A1.pdf>
- FCC Robocall Mitigation Database filing instructions: <https://www.fcc.gov/sites/default/files/rmd-instructions.pdf>
- Underlying Provider Robocall Mitigation Database entry: SignalWire, Inc., filing RMD0003809, FRN 0028100428, "Complete STIR/SHAKEN Implementation," verified against the Commission's public RMD dataset on August 5, 2026: https://fccprod.servicenowservices.com/api/x_g_fmc_rmd/rmd/csv_download
- The Underlying Provider's contract, call-signing description, KYC records, and account-validation evidence are maintained in Gaston's non-public compliance records under Section 5.