

CALLCLOUD

Robocall Mitigation Program Description

Voice Service Provider - Originating Traffic

This description applies to the entity filing under the CallCloud business name. CallCloud uses SignalWire, Inc. as its underlying voice-services provider and maintains customer verification, caller-ID controls, traffic monitoring, investigation, blocking, and traceback-cooperation procedures intended to prevent illegal robocall traffic from originating through its service.

1. Purpose and Scope

CallCloud provides cloud-based outbound calling functionality to business customers. This program applies to all calls originated through CallCloud and is designed to take reasonable steps to avoid the origination of illegal robocall traffic. The program combines pre-activation customer due diligence, caller-ID authorization controls, ongoing review of call-detail and account activity, complaint and traceback handling, and the ability to restrict, suspend, or terminate service.

CallCloud does not permit customers to use the platform for unlawful spoofing, fraud, impersonation, deceptive calling, or calls that violate applicable consent, Do Not Call, prerecorded or artificial-voice, abandonment, opt-out, or other consumer-protection requirements.

2. Know-Your-Customer Procedures

Before enabling outbound calling, CallCloud conducts a risk-based review of each customer. The review is intended to establish the customer's identity, legitimate business purpose, expected use of the service, and authority to place the proposed calls.

CallCloud collects and reviews, at minimum:

- Legal business name, any doing-business-as name, business address, website, and jurisdiction of organization.
- Name, title, business email address, and telephone number of an authorized representative.
- Description of the customer's products or services, intended calling purpose, target audience, expected call volume, and expected concurrency.
- Source of called-party information and the customer's basis for consent or other legal authority where required.
- Whether the customer intends to use prerecorded messages, artificial or AI-generated voice, voicemail drops, predictive or parallel dialing, debt collection, lead generation, or other higher-risk calling methods.
- Billing information and other account information sufficient to evaluate whether the applicant's identity and proposed use are consistent.

CallCloud verifies business existence using reasonably available public business-registration records and reviews consistency among the applicant's website, email domain, representative information, billing information, and stated use case. Accounts are manually approved before outbound calling is enabled.

Enhanced review may include formation documents, W-9 or EIN confirmation, government-issued identification for the authorized representative, proof of business address, sample call scripts, consent records, list-source documentation, or proof of telephone-number ownership. CallCloud may reject or delay activation when information is false, incomplete, inconsistent, unverifiable, or associated with a materially elevated risk of illegal calling.

3. Customer Contractual Requirements and Caller-ID Controls

Customers must contractually agree to comply with applicable federal and state calling laws and regulations; maintain required consent and suppression records; honor opt-out requests; use accurate caller identification; and cooperate promptly with CallCloud, SignalWire, carriers, regulators, law enforcement, and traceback investigators.

CallCloud limits outbound caller identification to telephone numbers obtained through SignalWire or externally owned numbers that have completed SignalWire's caller-ID verification process. Customers may not present a number they do not own or have authority to use. Requests to impersonate another person or entity, transmit misleading caller ID, or evade spam labeling or carrier controls are prohibited.

4. Know-Your-Upstream-Provider Procedures

CallCloud uses SignalWire, Inc. as its underlying voice-services provider. Before relying on an upstream provider, CallCloud reviews the provider's identity, service capabilities, compliance posture, operational contact information, and status in the FCC Robocall Mitigation Database. CallCloud periodically rechecks the upstream provider's status and maintains a process to act on notices from the provider regarding suspicious or prohibited traffic.

CallCloud does not knowingly route originating traffic through an upstream provider that is not eligible to accept and exchange traffic under applicable FCC rules. Any addition or replacement of an upstream provider is subject to compliance review before production use.

5. Traffic Analytics and Monitoring

CallCloud uses internal operational analytics and manual review of call-detail records and account activity to identify traffic that may be inconsistent with a customer's verified business purpose or may indicate illegal robocalling. CallCloud does not use a separate third-party analytics vendor. SignalWire is CallCloud's underlying provider, and CallCloud also considers network or carrier notices received through SignalWire.

Monitoring may include, at minimum:

- Material increases in call volume or concurrency compared with the customer's approved use and recent historical baseline.
- An unusually high proportion of very short answered calls, including calls lasting only a few seconds.
- Repeated calls to the same destination over a short period or other high-frequency dialing patterns.
- Rapid rotation among caller-ID numbers or attempts to use unauthorized or unverified caller IDs.
- Answer, no-answer, voicemail, automated-system, failure, and hang-up patterns that materially differ from normal account activity.
- Customer, consumer, carrier, platform, spam-label, law-enforcement, regulatory, or Industry Traceback Group complaints and notices.
- Traffic that is materially inconsistent with the customer's onboarding disclosures, approved calling purpose, expected geography, or expected volume.

Voicemail or automated-system detection may be used as one data point when evaluating calling patterns, but it is not treated by itself as evidence of unlawful activity. Alerts and anomalies are reviewed in context, including the customer's verified use case and supporting documentation.

6. Investigation, Blocking, and Remediation

When CallCloud identifies a credible indication of suspicious or potentially illegal traffic, it may immediately rate-limit, pause, or disable outbound calling while the matter is reviewed. CallCloud may request call scripts, consent records, list-source information, proof of caller-ID authorization, customer explanations, or other supporting materials.

Depending on the facts and severity, CallCloud may:

- Restrict calling volume, concurrency, destinations, features, or caller-ID numbers.
- Require corrective action, additional documentation, or enhanced monitoring.
- Suspend or terminate the customer account and prevent re-registration.
- Block specific caller-ID numbers, campaigns, destination patterns, or other traffic.
- Preserve and provide relevant account and call-detail information as legally permitted.
- Coordinate with SignalWire, downstream carriers, the FCC, law enforcement, or the Industry Traceback Group.

CallCloud will not restore restricted service unless it reasonably concludes that the risk has been addressed and the customer has demonstrated a lawful use of the platform.

7. Complaints and Traceback Cooperation

CallCloud maintains a process for promptly receiving, escalating, and investigating robocall-related complaints and provider notices. Relevant account, customer, caller-ID, campaign, and call-detail information is reviewed to identify the source and scope of the traffic and determine appropriate remedial action.

CallCloud commits to respond within 24 hours to all traceback requests from the Federal Communications Commission, law enforcement, and the industry traceback consortium, and to cooperate with those entities in investigating and stopping illegal robocallers that use CallCloud's service to originate calls.

8. Records, Training, and Program Review

CallCloud maintains customer onboarding records, account and caller-ID authorization information, complaint and investigation records, and available call-detail records in accordance with its retention policies and applicable law. Access to such information is limited to personnel and service providers with a legitimate operational, security, legal, or compliance need.

Personnel responsible for customer approval, support, operations, and compliance are instructed to escalate suspected unlawful calling, misleading caller-ID use, consumer complaints, carrier notices, and traceback requests. CallCloud periodically reviews this program and its controls in light of operational experience, changes in traffic patterns, provider requirements, and applicable law.

9. STIR/SHAKEN and Regulatory Disclosures

CallCloud originates traffic using SignalWire as its underlying provider and does not alter, strip, or bypass caller-ID authentication information applied at the network layer. CallCloud's RMD submission separately identifies its applicable STIR/SHAKEN implementation status and any required extension or exemption explanation.

Any required disclosure concerning formal FCC, law-enforcement, or regulatory actions or investigations during the prior two years is made in the corresponding RMD submission fields. CallCloud will update its RMD filing within the period required by FCC rules when filing information changes and will complete required annual recertification.

PROGRAM COMMITMENT

CallCloud will take reasonable steps to prevent illegal robocall traffic from originating through its service, will act on credible indications of unlawful use, and will cooperate promptly with traceback and enforcement efforts.