

Robocall Mitigation Program Description

Ligmeec Tecnologia Ltda

Draft for FCC Robocall Mitigation Database filing - review before submission

Legal Name	Ligmeec Tecnologia Ltda
FRN	0038635165
Country of Business Address	Brazil
Foreign Voice Service Provider	Yes
Provider Type	Voice Service Provider Filing
Voice Service Provider Role	Voice Service Provider with a STIR/SHAKEN implementation obligation serving end-users
STIR/SHAKEN Certification Status	No STIR/SHAKEN implementation at the time of this filing; hosted STIR/SHAKEN signing is being pursued through Anveo Direct after issuance of Ligmeec's own valid STIR/SHAKEN certificate.
Responsible Contact	Leandro Moraes de Oliveira - leandro.oliveira@ligmeec.com

1. Overview

Ligmeec Tecnologia Ltda ("Ligmeec") operates a multi-tenant PBX/VoIP platform for business customers. Ligmeec customers may originate outbound SIP/IP calls through Ligmeec infrastructure, including calls to U.S. destinations that are routed through upstream providers such as Anveo Direct.

Ligmeec is a foreign voice service provider. At the time of this filing, Ligmeec has not implemented its own STIR/SHAKEN authentication framework across its network. Ligmeec is pursuing hosted STIR/SHAKEN signing through Anveo Direct and intends to use its own valid STIR/SHAKEN certificate after completing the required registration and certificate issuance process. All calls originated through Ligmeec are subject to the robocall mitigation measures described below.

2. Robocall Mitigation Commitment

Ligmeec maintains and will continue to maintain reasonable practices designed to avoid originating illegal robocall traffic, spoofed caller ID traffic, and other abusive traffic. Ligmeec commits to cooperate with the Federal Communications Commission, law enforcement, the registered industry traceback consortium, upstream providers, and other appropriate entities in investigating and stopping illegal robocallers that use or attempt to use Ligmeec services.

Ligmeec commits to respond fully and within 24 hours to traceback requests from the Commission, law enforcement, and the industry traceback consortium.

3. Customer Onboarding and Know-Your-Customer Procedures

Ligmeec provides services to business customers and applies onboarding and account review procedures intended to identify the customer and the intended use of the service before service activation and during the customer relationship.

- Collection and review of customer business identity information, including legal name, contact information, billing information, and business purpose for the PBX/VoIP service.
- Use of written service terms or agreements that prohibit illegal robocalls, spoofing, fraud, phishing, impersonation, unlawful telemarketing, and other abusive traffic.

- Review of unusual or high-risk use cases before allowing large-scale outbound calling or atypical traffic patterns.
- Maintenance of customer account records sufficient to identify the customer associated with outbound call traffic.

4. Caller ID Authorization and Spoofing Controls

Ligmees seeks to prevent unauthorized caller ID use. Ligmees does not permit customers to intentionally transmit misleading or inaccurate caller ID information for unlawful purposes.

- Outbound caller IDs are associated with customer accounts when configured in the PBX platform.
- Ligmees may require proof of authorization to use a caller ID, such as ownership of a number, number assignment by a provider, porting documentation, customer attestation, or other reasonable evidence.
- Ligmees may block, remove, or restrict caller IDs that appear invalid, unauthorized, misleading, or associated with complaints or suspicious traffic.
- For U.S. outbound calling, Ligmees intends to apply attestation controls and hosted STIR/SHAKEN signing through Anveo Direct after Ligmees obtains its own valid STIR/SHAKEN certificate.

5. Traffic Monitoring and Abuse Detection

Ligmees monitors outbound call traffic and customer behavior for indicators of potentially illegal robocall activity or caller ID spoofing. Monitoring may include manual review, automated alerts, and investigation of upstream provider feedback.

- Unusual call volume spikes, short-duration call patterns, high failure rates, or repeated calls to similar destination ranges.
- Complaints from called parties, upstream providers, traceback requests, or regulatory contacts.
- Use of invalid, suspicious, or frequently changing caller IDs.
- Customer behavior inconsistent with the stated business purpose or normal usage profile.

6. Response to Suspicious or Illegal Traffic

When Ligmees identifies suspicious or potentially illegal traffic, Ligmees may take reasonable corrective measures based on the severity and evidence available.

- Temporary suspension or throttling of outbound calling for the affected account, route, or caller ID.
- Request for additional customer information or caller ID authorization evidence.
- Blocking or removal of unauthorized or suspicious caller IDs.
- Termination of customer service for confirmed or repeated illegal robocall, spoofing, fraud, or abusive activity.
- Cooperation with upstream providers and traceback or law enforcement inquiries.

7. Traceback, Complaint Handling, and Regulatory Cooperation

Ligmees designates a responsible contact for robocall mitigation, traceback, and regulatory inquiries. Ligmees will use commercially reasonable efforts to investigate traceback requests promptly and provide responsive information within 24 hours where required.

- Responsible Contact: Leandro Moraes de Oliveira, leandro.oliveira@ligmees.com.
- Ligmees maintains call records and customer-account information that may assist in identifying the source of a call routed through Ligmees.
- Ligmees will cooperate with the FCC, law enforcement, the industry traceback consortium, and upstream providers to investigate and stop illegal traffic.

8. Call Logging and Record Retention

Ligmees maintains operational records related to outbound calls and customer accounts to support billing, troubleshooting, abuse investigation, and traceback response.

- Customer account identifier and related PBX tenant information.
- Outbound caller ID presented by the customer or platform.
- Destination number, route/trunk, timestamp, call duration, and call result when available.
- Relevant SIP signaling and platform logs where retained for troubleshooting or abuse review.

9. STIR/SHAKEN Implementation Plan

Ligmees does not currently operate its own STIR/SHAKEN signing infrastructure. Ligmees is pursuing hosted STIR/SHAKEN signing through Anveo Direct for U.S. outbound calls routed through Anveo Direct. Under this approach, Ligmees intends to obtain its own valid STIR/SHAKEN certificate through the applicable STI-PA/Certification Authority process and upload the certificate and corresponding private key to Anveo Direct's hosted signing service.

Ligmees intends to control attestation decisions for calls originated by its customers. Ligmees expects to use full attestation only where the customer and caller ID authorization can be verified, partial attestation where the customer is known but caller ID authorization cannot be fully verified, and gateway-level attestation or blocking where the source or caller ID cannot be adequately validated.

10. Ongoing Review and Updates

Ligmees will review and update this robocall mitigation program as its network, customers, upstream providers, STIR/SHAKEN implementation status, and regulatory obligations evolve. Ligmees will update its Robocall Mitigation Database filing when required to reflect material changes.

11. Certification Statement

Ligmees certifies that the calls it originates are subject to this robocall mitigation program, which includes reasonable steps to avoid originating illegal robocall traffic, cooperation with traceback and law enforcement requests, and procedures to identify, investigate, and stop illegal traffic that uses or attempts to use Ligmees services.

References

FCC Robocall Mitigation Database: <https://www.fcc.gov/robocall-mitigation-database>

FCC Robocall Mitigation Database External Filing Instructions: <https://www.fcc.gov/sites/default/files/rmd-instructions.pdf>

47 CFR Section 64.6305: Robocall Mitigation Database filing and certification requirements