



Robocall Mitigation Program Description

Filer: Otimi (Brazil)

Provider Type: Foreign Voice Service Provider (Originating)

Date: 2026-03-04

Primary Contact for Robocall Mitigation & Traceback (24/7 or on-call):

- **Name/Title:** Mr. Marcelo Stolai, **CEO**
- **Email:** marcelo@otimi.com.br
- **Phone:** +55 (11) 3192-8908
- **Alternate Contact:** Vanessa Stolai / vanessa@otimi.com.br / +55 (11) 3192-8909
- **Website:** <https://otimi.com.br>

1. Overview and Scope

Otimi is a **foreign voice service provider** headquartered in **Brazil**. Otimi provides voice services to business customers located in Brazil who originate outbound calls, including calls destined to the United States. Calls originate from customer PBXs or endpoints, traverse Otimi's network and **Session Border Controller (SBC)**, and U.S.-bound traffic is delivered via a single upstream provider (**DID Logic**) for U.S. termination.

Otimi does not operate as a U.S. gateway provider. Otimi's role is that of an **originating provider** for its Brazilian customers' traffic.

2. STIR/SHAKEN Status and Reason for Non-Implementation

At this time, Otimi does not implement STIR/SHAKEN authentication on its originating network for U.S.-bound calls due to the filer's current inability to obtain the credentials required to sign calls within the U.S. STIR/SHAKEN ecosystem.

Otimi therefore relies on the controls described in this Robocall Mitigation Program to mitigate the risk of originating illegal robocalls, spoofing, and abusive calling patterns.

3. Customer Onboarding (KYC/KYB) and Use Policy Controls

Otimi uses a "know-your-customer / know-your-business (KYC/KYB)" approach designed to reduce the risk of illegal robocalling and caller ID spoofing.

3.1 Business Verification

Prior to activation, Otimi verifies customer identity and legitimacy using reasonable measures, which may include:

- corporate registration/tax identifier verification (e.g., CNPJ or equivalent);
- verification of authorized signatory and business contact details;

- review of intended use case (e.g., customer support, sales, appointment reminders);
- confirmation of geographic location and billing information;
- validation of domain/email ownership when applicable.

3.2 Prohibited Uses and Contractual Controls

Otimi requires acceptance of an acceptable use policy and contractual terms that prohibit:

- illegal robocalls, scam campaigns, and fraudulent traffic;
- caller ID spoofing without verified right-to-use;
- traffic designed to mislead recipients, evade blocking, or generate complaints;
- unlawful telemarketing or automated calling in violation of applicable laws.

Otimi reserves the right to suspend or terminate service promptly upon detection or reasonable suspicion of prohibited activity.

4. Caller ID Governance (Anti-Spoofing) and Number Authorization

Otimi enforces caller ID controls to prevent spoofing and unauthorized presentation of calling numbers.

4.1 Brazilian Caller ID (+55)

In most cases, customers present **Brazilian caller ID numbers (+55 E.164)** associated with the customer and verified during onboarding and/or provisioning. Otimi requires that caller ID values be valid and in the expected format.

4.2 U.S. DID Caller ID (+1) — Optional/Exceptional Use Case

In limited cases, a customer may request use of a **U.S. DID (+1 NANP)** for legitimate business purposes (e.g., a U.S.-facing support line). Such DIDs may be obtained via Otimi's upstream provider (**DID Logic**) or another authorized provider.

Before enabling any U.S. DID as caller ID, Otimi requires documented proof of the customer's **right to use** the number, which may include:

- service order / invoice / portal evidence from the DID provider;
- Letter of Authorization (LOA) or equivalent documentation;
- contractual documentation demonstrating assignment or authorized use.

Otimi maintains a record of authorized caller IDs per customer and blocks unauthorized caller IDs when detected.

4.3 Validation and Blocking Rules

Otimi applies reasonable caller ID validation, which may include:

- enforcing E.164 format for caller ID;

- blocking invalid or malformed numbering (including invalid NANP patterns for +1 caller IDs);
- blocking caller IDs that are not authorized for the customer account;
- suspending service where spoofing or repeated violations are detected.

5. Traffic Monitoring, Anomaly Detection, and Abuse Response

Otimi monitors traffic for indicators of illegal robocalling, spoofing, and abusive activity. Monitoring may be automated and/or manual and can include review of call detail records (CDRs) and network signals.

5.1 Examples of Risk Indicators

Otimi looks for patterns including, but not limited to:

- unusual spikes in calls per second (CPS) or sudden volume increases;
- repeated short-duration calls (e.g., very low average call duration);
- high call failure rates or abnormal answer-seizure ratio (ASR);
- excessive concentration to specific destinations, area codes, or number ranges;
- repeated attempts using unauthorized caller IDs;
- complaint indicators received from partners, customers, or downstream providers.

5.2 Enforcement Actions

When suspicious or abusive activity is detected, Otimi may take one or more of the following actions:

- temporary rate limiting or traffic shaping;
- immediate blocking of specific caller IDs or destinations;
- suspension of the customer's service pending investigation;
- termination of service for confirmed violations;
- preservation of relevant records to support investigation and traceback.

6. Traceback Cooperation and Response Commitment (24 Hours)

Otimi commits to cooperate with traceback requests and to respond **as soon as practicable**, and in any case **within 24 hours** of receiving a traceback request from an authorized traceback entity, industry partner, or appropriate authority, consistent with applicable requirements.

Otimi will use available data sources to support traceback, which may include:

- CDRs and associated routing information;
- customer account records and authorized caller ID lists;
- SBC logs and signaling information, where available.

7. Vendor/Partner Management (Upstream Provider)

Otimi routes U.S.-bound calls through a single upstream provider (**DID Logic**) for U.S. termination. Otimi maintains a commercial relationship with this provider and expects compliance with applicable U.S. requirements by relevant parties in the call path.

Otimi coordinates with upstream providers as necessary to:

- investigate abuse reports;
- support traceback activities;
- implement call blocking where required;
- address repeated violations and prevent recurrence.

8. Record Retention and Auditability

Otimi retains call records and customer account information sufficient to support operational needs, abuse investigations, and traceback responses. Retention periods and access controls are managed to protect customer information while enabling timely compliance actions.

Otimi restricts access to sensitive records to authorized personnel and maintains operational procedures for handling abuse investigations and lawfully requested information.

9. Program Maintenance and Updates

Otimi reviews and updates this Robocall Mitigation Program periodically and when material changes occur in network architecture, upstream partnerships, or regulatory requirements. Staff are trained to escalate suspected abuse and to follow the enforcement and traceback procedures described herein.

Certification Statement:

Otimi certifies that it has implemented the practices and procedures described above and will maintain and enforce this Robocall Mitigation Program to reduce the risk of originating illegal robocalls and to support traceback efforts.

Authorized Signatory:

Name: Mr. Marcelo Stalai

Title: **CEO**

Company: Otimi Tecnologia

Signature:



Date: 2026-03-04