

ROBOCALL MITIGATION PLAN

1. INTRODUCTION

This document details ComputerTel Inc.'s (dba Directo) Robocall Mitigation Plan in accordance with current Federal Communications Commission (FCC) requirements, including but not limited to 47 CFR §§ 64.6305 and 64.1200(n).

This plan is designed to satisfy the FCC requirement that providers describe with particularity the specific “reasonable steps” taken to prevent the origination, carrying, and processing of illegal robocall traffic.

Affiliates: ComputerTel Inc. has one operating affiliate relevant to this filing — Directo S.A. de C.V., a Mexico-based foreign voice service provider that services enterprise clients with U.S. NANP DID and toll-free numbers for calls terminating in the United States. Directo S.A. de C.V. maintains its own filing in the FCC Robocall Mitigation Database as a foreign voice service provider in accordance with 47 CFR § 64.6305(d). ComputerTel Inc. acts as the U.S. gateway for this traffic and verifies the affiliate's RMD filing status before accepting calls, consistent with 47 CFR § 64.6305(g)(2).

Prior Enforcement Actions: Within the prior two years, neither ComputerTel Inc. nor any entity sharing common ownership, management, directors, or control with ComputerTel Inc. (including Directo S.A. de C.V.) has been the subject of any formal Commission, law enforcement, or regulatory agency action or investigation with findings of actual or suspected wrongdoing related to transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or related to a deficient Robocall Mitigation Database certification or mitigation program description. (Required disclosure under 47 CFR § 64.6305(d)(2)(iv), (e)(2)(iv), and (f)(2)(iv).)

Directo operates as:

- **Gateway Provider** — receiving calls directly from foreign voice service providers (including its affiliate, Directo S.A. de C.V.) at U.S.-based facilities, where those calls use NANP resources pertaining to the United States, before transmitting downstream to U.S.-based providers.
- **Non-Gateway Intermediate Provider** — carrying or processing transit voice traffic between U.S.-based providers.
- **Voice Service Provider (Originating Provider)** — in circumstances where Directo signs calls with A attestation based on a direct authenticated relationship with enterprise end users and has verified the customer's right to use the calling number.

Accordingly, this plan differentiates mitigation practices by role where applicable. The obligations of 47 CFR §§ 64.6302, 64.6305(b), (c), (d), (e), and (f), and 47 CFR § 64.1200(n), apply to ComputerTel Inc. (dba Directo) depending on its role in the call path.

2. STIR/SHAKEN IMPLEMENTATION

Directo has fully implemented STIR/SHAKEN in the IP portions of its network as of June 30, 2023, in accordance with 47 CFR §§ 64.6301 and 64.6302. Directo authenticates calls in-house using the

TransNexus NexOSS solution; no third-party authentication arrangement is in place to sign ComputerTel-signed calls. Directo holds a valid Service Provider Code (SPC) token and digital certificate issued through the STI Governance Authority and STI Policy Administrator framework, in compliance with the FCC's Eighth Report and Order on Call Authentication (FCC 24-120), which became effective September 18, 2025, and which requires providers certifying STIR/SHAKEN implementation in the Robocall Mitigation Database to obtain their own SPC token and digital certificate and to authenticate all calls using that certificate.

Gateway Role: Directo authenticates all unauthenticated foreign-originated SIP calls with U.S. NANP numbers.

Intermediate Role: Directo authenticates unauthenticated calls where it is the first intermediate provider and passes authentication information unaltered.

Voice Service Provider Role: Directo authenticates all calls it originates or signs. Directo assigns A attestation only where it has a direct contractual relationship with the enterprise customer and has verified the customer's right to use the calling telephone number in accordance with ATIS-1000074 and related STIR/SHAKEN standards.

Such verification includes, as applicable:

- Direct number assignment by Directo, or
- Documented validation of the customer's right to use the telephone number, including letters of authorization or equivalent documentation
- Directo assigns B or C attestation where the criteria for A attestation are not fully satisfied

Directo validates all SHAKEN Identity headers and blocks calls with invalid or malformed authentication.

Non-IP Portions: Directo's network is fully IP-based; Directo does not operate any TDM or other non-IP infrastructure that would qualify for an extension under 47 CFR § 64.6304(b). Accordingly, Directo claims no STIR/SHAKEN implementation extension or exemption.

3. ROBOCALL MITIGATION PROGRAM – REASONABLE STEPS

Directo implements a robocall mitigation program including the following reasonable and effective measures:

3.1 Know Your Customer (KYC) / Know Your Traffic (KYT)

Directo performs due diligence prior to onboarding all customers, including:

- Corporate identity verification
- FCC/USAC registration checks
- Proof of number ownership / right-to-use
- Business reference and credit checks

New and Renewing Customer Controls:

- Periodic re-verification of existing customers
- Enhanced monitoring of customers during initial traffic ramp-up

- Periodic re-screening of customers upon contract renewal, or if traffic patterns change
- Immediate escalation and suspension for customers linked to illegal robocall campaigns

In its role as a Voice Service Provider, Directo applies these KYC/KYT procedures specifically to prevent customers from originating illegal robocall traffic, consistent with 47 CFR § 64.1200(n)(3). Directo does not originate traffic on behalf of any customer that cannot be verified or that presents an unacceptable risk of illegal robocalling.

These measures satisfy the FCC requirement to take affirmative, effective steps to prevent new and renewing customers from originating illegal robocalls.

3.2 Know Your Upstream Provider (KYUP)

In accordance with its gateway-provider obligations under 47 CFR § 64.1200(n)(5) and the know-your-upstream-provider requirements applicable to non-gateway intermediate providers under the Sixth Caller ID Authentication Report and Order, Directo implements procedures to evaluate and monitor upstream providers, including:

- Verification that upstream providers are listed in the FCC Robocall Mitigation Database
- Review of upstream provider mitigation plans where available
- Monitoring upstream traffic patterns for anomalies or high-risk behavior
- Immediate mitigation or blocking of upstream providers associated with repeated, high-volume, or confirmed illegal traffic

3.3 Traffic Monitoring and Analytics

Directo conducts 24/7 continuous monitoring of all traffic traversing its network, supplemented by dedicated fraud analyst review during extended business hours and on-call coverage outside business hours.

Analytics Tools Used:

- YouMail Score (third-party analytics vendor)
- YouMail Watch
- Internal SIP signaling and CDR analytics tools

Analytics are used to:

- Identify high-risk traffic patterns (e.g., short-duration calls, high ASR anomalies)
- Assign fraud risk scores in real time
- Trigger automated or manual blocking actions
- Generate alerts to the Fraud & Abuse team, with documented escalation to the VP Wholesale for confirmed illegal-traffic incidents

Calls exceeding defined fraud thresholds are:

- Blocked in real time, or

- Flagged for immediate investigation and mitigation
-

3.4 Do-Not-Originate (DNO) Controls

Directo blocks calls using:

- SOMOS Toll-Free DNO database
 - SOMOS Local DNO database
 - Internal dynamic DNO lists
 - Additional calling number screening tools include:
 - Global number GNR filters for international calling numbers (Global Number Range)
 - LERG (Local Exchange Routing Guide)
-

3.5 Contractual Controls

Directo includes contractual provisions prohibiting:

- Caller ID spoofing
- Traffic masking
- Re-origination schemes
- Any unlawful robocalling activity

Violations result in:

- Immediate blocking
 - Contract termination
-

3.6 Active Mitigation and Enforcement

When suspicious traffic is detected:

- Traffic is investigated in real time
- Customer is notified
- Traffic is blocked if necessary

Repeat or severe violations result in permanent termination.

3.7 Voice Service Provider (Originating) Controls

In circumstances where Directo acts as a Voice Service Provider and originates or signs calls with A attestation, Directo implements the following additional controls:

- Ensures a direct contractual relationship with the enterprise customer
- Verifies and documents the customer's right to use all telephone numbers associated with A attestation

- Applies enhanced onboarding and monitoring procedures for originating customers
- Continuously monitors originating traffic for patterns indicative of illegal robocalling
- Immediately blocks and terminates any customer found to be originating illegal robocall traffic

Directo assigns A attestation only where it has a high degree of confidence in the identity of the customer and the customer's right to use the calling number, consistent with industry standards and FCC expectations.

4. TRACEBACK AND LAW ENFORCEMENT COOPERATION

Directo commits, in accordance with 47 CFR § 64.6305(a)(2), (b)(2), and (c)(2), to:

- Responding fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium (currently USTelecom's Industry Traceback Group)
- Cooperating with the Commission, law enforcement, and the industry traceback consortium in investigating and stopping any illegal robocallers that use Directo's service to originate, carry, or process calls, including, in its role as a Voice Service Provider, identifying and mitigating customers responsible for originating illegal robocall traffic
- Taking action against customers and upstream providers identified through traceback as sources of illegal traffic, up to and including immediate blocking and termination

Directo maintains internal procedures to ensure rapid identification of call paths and long-term preservation of call detail records (>2 years).

5. FCC NOTIFICATION AND MANDATORY BLOCKING

Directo will, in accordance with 47 CFR §§ 64.1200(n) and 64.6305(g):

- Upon receipt of a Notification of Suspected Illegal Traffic from the Commission, effectively mitigate the identified traffic promptly, and within any timeframe specified by the Commission by identifying the source and preventing that source from continuing to originate, carry, or process traffic of the same or similar nature, consistent with 47 CFR § 64.1200(f)(18) and (n)(2)
 - Within 14 days of such Notification, implement effective measures to prevent new and renewing customers from using Directo's network to originate, carry, or process illegal calls, and inform the Commission and the Traceback Consortium of the steps taken
 - Promptly comply with any Initial Determination Order and Final Determination Order issued by the Commission, including blocking traffic from identified providers within the timeframes specified by the Commission
 - Cease accepting traffic from any provider whose RMD certification has been removed by Commission action, within two (2) business days of the removal order, consistent with 47 CFR § 64.6305(g)
-

6. ROBOCALL MITIGATION DATABASE COMPLIANCE

Directo:

- Maintains an accurate and current filing in the FCC Robocall Mitigation Database
 - Updates filings within required timeframes
 - Refuses traffic from providers not listed in the database
-

7. ROLE-BASED MITIGATION SUMMARY

Gateway Provider Obligations:

- Authenticate foreign-originated traffic
- Know upstream providers
- Prevent entry of illegal traffic into U.S. network

Intermediate Provider Obligations:

- Authenticate when first in path
- Validate and pass authenticated traffic unaltered
- Monitor and mitigate transit traffic

Voice Service Provider (Originating) Obligations:

- Verify customer identity and right to use telephone numbers
 - Assign STIR/SHAKEN attestation levels appropriately (A/B/C)
 - Prevent customers from originating illegal robocall traffic
 - Monitor originating traffic and take immediate mitigation action where necessary
-

8. CONTINUOUS IMPROVEMENT

Directo continuously evaluates and enhances its robocall mitigation controls to comply with evolving FCC rules and industry best practices.

Directo will recertify and resubmit its filing in the FCC Robocall Mitigation Database annually on or before March 1, in accordance with 47 CFR § 64.6305(h), and will update its filings within ten (10) business days of any material change to the information required under 47 CFR § 64.6305(d)–(f).

9. CONTACT INFORMATION

Fraud & Abuse Contact:

- Email: fraud@directo.com; support@directo.com
 - Phone: +1-754-347-3286
-

CERTIFICATION

I hereby certify, under penalty of perjury and in conformity with 47 CFR § 1.16, that I am an officer of ComputerTel Inc. (dba Directo) authorized to make this certification on the company's behalf; that all calls that ComputerTel Inc. originates, carries, or processes are subject to the robocall mitigation program described above; that the information contained in this Robocall Mitigation Plan is true and correct to the best of my knowledge, information, and belief; that ComputerTel Inc. has fully implemented STIR/SHAKEN in the Internet Protocol portions of its network and claims no extension or exemption; that ComputerTel Inc. commits to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers; and that ComputerTel Inc.'s prior certification has not been removed by Commission action and ComputerTel Inc. has not been prohibited from filing in the Robocall Mitigation Database.

Signature: René Brun

Name: René Brun

Company: **ComputerTel Inc. (dba Directo)**

Title: VP Wholesale

Date: **07 May 2026**

Physical Address: 6500 River Place Blvd., Building 7, Suite 250-242, Austin, TX 78830 USA

Registered Address: 123 W. Nye Lane, Suite 129, Carson City, NV, 89706 USA



Digitally signed
by René Brun

Date:
2026.05.07
12:59:04 -04'00'