

Document ID: VRR-2026-002

Version: 2.0

Date: January 12, 2026

Status: Final

1. Introduction

Consultizor LLC (“Company”) is a newly formed Voice over Internet Protocol (VoIP) service provider operating in the United States. We provide services as both a **Gateway Provider** (accepting calls from outside the U.S. destined for U.S. consumers) and a **Non-Gateway Intermediate Provider** with STIR/SHAKEN obligations (transporting authenticated traffic within the U.S.). We are committed to providing reliable and secure communication services while actively working to prevent illegal and fraudulent robocalls. This Robocall Mitigation Policy (“Policy”) outlines the measures we have implemented to comply with the Federal Communications Commission (FCC) rules, the TRACED Act, and industry best practices for mitigating illegal robocalls.

This policy is submitted to the Robocall Mitigation Database maintained by the FCC as required under 47 C.F.R. § 64.6305 and in accordance with FCC gateway provider and intermediate provider obligations (47 C.F.R. §§ 64.6300-6316).

2. Purpose

The purpose of this Policy is to:

- Prevent our network from being used to originate, transmit, or facilitate illegal robocalls, including spoofed calls and fraudulent campaigns.
 - Implement and maintain robocall mitigation measures as required by law for both our Gateway and Non-Gateway Intermediate Provider roles.
 - Provide clear information to the FCC, industry partners, and customers regarding our dual-role robocall mitigation efforts.
-

3. Compliance Framework

Consultizor LLC adheres to the following regulations and industry standards:

- The **Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act**.
 - FCC rules on **Caller ID Authentication (STIR/SHAKEN)** and **Robocall Mitigation** (47 C.F.R. § 64.6300 et seq.).
 - **Gateway Provider Requirements** (47 C.F.R. § 64.6300(g), 64.6311).
 - **Intermediate Provider Obligations** (47 C.F.R. § 64.6300(f), 64.6303).
 - Industry standards and best practices established by the **Industry Traceback Group (ITG)**, **ATIS**, and the **SIP Forum**.
-

4. Robocall Mitigation Program

4.1. STIR/SHAKEN Implementation

- **Consultizor LLC** has fully implemented the STIR/SHAKEN framework across its IP-based network.
- **As a Non-Gateway Intermediate Provider:** We pass through all SIP Identity headers and do not strip authentication information. We maintain the capability to authenticate signed calls and verify the validity of STIR/SHAKEN signatures.
- **As a Gateway Provider:** We authenticate all foreign-originated calls entering the U.S. network. In accordance with our role and FCC requirements, we sign these calls with the appropriate attestation level:
 - **Attestation Level 'C' (Gateway Attestation):** Applied as the default, attesting that the call entered the U.S. network via our gateway.
 - **Attestation Level 'B' (Partial Attestation):** May be applied in limited circumstances where we have a direct, trusted relationship with the foreign service provider and can authenticate the source of the call, but **we cannot verify the end-subscriber's right to use the calling number**.
 - ***We do not use Attestation Level 'A' for gateway traffic, as we are not the originator of the call and cannot verify the caller's right to use the telephone number.***

4.2. Network Monitoring and Analytics

- We employ **24/7 network monitoring** tools to detect anomalous calling patterns from all ingress points, with enhanced scrutiny on our **gateway ingress points**.

- We utilize **analytics platforms** to identify and investigate potential robocall campaigns in real time, with specific algorithms focused on identifying suspicious foreign-originated traffic.
- We apply **traffic profiling** to establish baselines for normal customer behavior and flag deviations for review.

4.3. Know Your Customer (KYC) Procedures

- We implement strict **customer identification and verification** processes prior to service activation.
- **For Gateway Customers (Foreign-originating traffic):** We apply **enhanced due diligence**, which may include verification of foreign business registration, understanding the nature of call traffic, and contractual prohibitions against illegal robocalling.
- **For Domestic Intermediate Customers:** We require attestation of compliance with applicable U.S. robocall rules.
- We reserve the right to terminate service for customers found to be engaging in illegal calling activity.

4.4. Illegal Traffic Prevention and Response

- We maintain and enforce **acceptable use policies (AUP)** that prohibit illegal robocalling and spoofing for all customers.
- We promptly investigate and respond to **traceback requests** from the ITG, law enforcement, and regulatory bodies. We prioritize traceback requests involving our gateway ingress points.
- We take swift action to mitigate illegal traffic, which may include **blocking, filtering, or terminating** service to bad actors.
- **As a Gateway Provider:** We implement mandatory **mitigation on all gateway traffic** upon notification of illegal traffic from the FCC or a downstream provider, as required by 47 C.F.R. § 64.6311.

4.5. Call Blocking and Filtering

- We participate in **industry-wide call-blocking lists** and analytics feeds to identify and block known bad-actor numbers and carriers.
- We implement **network-based call filtering** for suspected illegal spoofed calls and high-risk destinations.

- **Gateway-Specific Measures:** We apply **additional screening** to foreign-originated calls, including checks against known fraudulent numbering patterns and unallocated numbering blocks.
- We offer optional **call-blocking tools** to end-users to empower them to manage unwanted calls.

4.6. Cooperation and Traceback

- We fully cooperate with the **Industry Traceback Group (ITG)**, USTelecom, and other authorized entities in identifying the source of illegal robocalls.
- We respond to traceback requests within **24 hours** and provide all necessary routing and customer information in accordance with legal requirements.
- We maintain specific **records of gateway traffic** to facilitate rapid traceback, including source IP, customer identity, and call detail records (CDRs).

4.7. Employee Training

- We provide **annual training** to relevant employees on robocall mitigation regulations, with specialized modules for **gateway-specific obligations** and **intermediate provider requirements**.

5. Recordkeeping and Reporting

- We maintain detailed records of robocall mitigation efforts, including:
 - STIR/SHAKEN implementation and performance metrics, segregated by gateway and intermediate traffic.
 - Enhanced KYC documentation for gateway customers.
 - Traceback requests and responses, with identifiers for gateway-related investigations.
 - Actions taken against illegal traffic, including gateway-specific mitigation actions.
- We will file required **certifications and updates** in the FCC Robocall Mitigation Database as needed, clearly indicating our dual roles.

6. Policy Review and Updates

This Policy will be reviewed **annually** and updated as necessary to reflect changes in regulations, industry standards, or operational practices, with particular attention to evolving FCC requirements for gateway and intermediate providers.

7. Contact Information for Robocall Mitigation

Provider Legal Name: Consultizor LLC

FCC Registration Number (FRN): 0037697455

Provider Type(s) Filed Under: Gateway Provider & Non-Gateway Intermediate Provider with STIR/SHAKEN Obligation

Robocall Mitigation Point of Contact:

- Name: Muhammad Nazim
- Title: CEO
- Email: nazim@consultizor.net
- Phone: 206-317-1316

Address:

312 W 2nd ST Unit A2924
Casper, WY 82601
