

United World Telecom L.C Robocall Mitigation Plan

Company Name: United World Telecom L.C. (UWT)

Operating Company Number (OCN): 164L

STIR/SHAKEN Implementation Status: Fully implemented

Reasonable Steps to Prevent Illegal Robocalls

UWT has implemented multiple reasonable and proactive measures as part of its Robocall Mitigation Program to prevent the origination, carriage, or processing of illegal robocall traffic. These measures include:

- STIR/SHAKEN Deployment: Full implementation of the STIR/SHAKEN framework across our IP-based network, ensuring the authentication and verification of caller identity in accordance with FCC requirements.
- Ongoing Traffic Monitoring: Continuous monitoring and analytics are used to identify suspicious calling patterns, including high volumes of short-duration calls, elevated call failure rates, and sudden spikes in call traffic.
The following parameter anomalies trigger alerts, which are manually reviewed by company staff:
 - > *Balance Limit:* Similar to credit card limits, we impose default balance limits to detect abnormal usage or risk.
 - > *Short Call Durations:* Consistently brief calls may indicate robocall activity or technical issues.
 - > *Answer-Seizure Ratio (ASR) Issues:* Low ASR can be symptomatic of robocall behavior or call quality problems.
 - > *Overall Traffic Increase:* Sudden traffic spikes may signal the activity of a bad actor.
 - > *Sequential Dialing Patterns:* Our systems monitor for sequences of incrementally dialed numbers, which may indicate robocall campaigns.
- Immediate Mitigation Measures: Prompt application of mitigation actions such as call blocking, rate limiting, or other necessary technical measures to prevent the propagation of suspect traffic.
- Account Enforcement: Swift suspension or termination of customer accounts determined to be generating or facilitating illegal robocall activity.

Know Your Customer / Upstream Provider Policies

UWT employs a Know Your Customer (KYC) process to verify the identity and legitimacy of all customers and, where applicable, upstream providers. This process includes:

- Manual Verification: Every new customer is manually reviewed and either approved or declined. The verification process includes checking the customer's business profile and purpose, phone number, email address, website authenticity, and IP address. In some

cases, we request additional documentation, such as a certificate of incorporation, a government-issued ID or passport of a representative (including a selfie holding the ID/passport), recent utility bills or invoices as proof of address, etc. We also use various security tools to authenticate the documents and images of IDs we receive from customers during the verification process.

- Outbound Calling Policy: We do not support or accept customers engaged in outbound calling campaigns, and we do not provide any tools or services designed for such calling patterns.
- Ongoing Monitoring: We continuously monitor customer behavior, including but not limited to call volumes, credit usage, destination changes, call completion ratios, and changes in average call durations. We also conduct periodic reviews and revalidation of customer information, including verification of active websites and up-to-date contact details.
- Payment Policy: We do not accept cryptocurrency payments. Accepted payment methods include verified credit cards, PayPal, and wire transfers only.

Analytics Systems for Robocall Detection

UWT leverages a combination of proprietary traffic analysis tools and behavior-based algorithms to detect and mitigate potential robocall traffic. Our systems are designed to:

- Detect anomalous call behavior, including patterns indicative of robocall activity.
- Flag calls to unallocated, invalid, or known problematic numbers.
- Generate alerts in response to high-volume bursts or sudden shifts in traffic patterns.
- Correlate STIR/SHAKEN attestation levels with real-time traffic behavior to identify inconsistencies or suspicious activity.
- Automatically suspend traffic when a line reaches its monthly credit limit, which is dynamically set based on the customer's average usage over the previous three months.

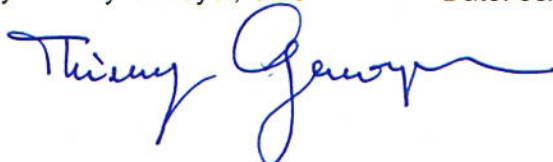
Use of Third-Party Analytics Vendors

Following the implementation of UWT's in-house STIR/SHAKEN solution, we do not rely on third-party analytics vendors for robocall detection or mitigation. All monitoring and mitigation efforts are conducted internally using proprietary tools and supported by human oversight. However, we remain open to integrating third-party analytics solutions in the future, should operational needs or regulatory requirements warrant it.

UWT certifies that all of the calls that it carries or processes on its network are subject to a robocall mitigation program consistent with 47 CFR § 64.6305(c), which shall include reasonable steps to avoid carrying or processing illegal robocall traffic and shall include a commitment 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 that use its service to carry or process calls.

Signed By: Thierry Genoyer, CEO

Date: 05/08/2025

A handwritten signature in blue ink, appearing to read 'Thierry Genoyer', with a stylized flourish at the end.