

TruewayIT, LLC

PO Box 1312 | Willis, TX 77378
936.256.1100 | www.trueway.com

ROBOCALL MITIGATION PLAN

Submitted to the FCC Robocall Mitigation Database pursuant to 47 CFR § 64.6305

Effective Date: June 05, 2026

Section 1 — Company Overview

TruewayIT, LLC ("Trueway" or "the Company") is a managed IT services and VoIP provider headquartered in Willis, Texas. Trueway provides business telephone services exclusively to vetted small and mid-sized businesses in the United States. The Company directly manages endpoint installation, configuration, and ongoing monitoring of all VoIP equipment deployed to its customers.

Trueway's upstream voice provider for call origination and transit is [CARRIER REDACTED] (a [CARRIER REDACTED] company), a registered U.S. voice service provider subject to FCC regulations.

Section 2 — STIR/SHAKEN Implementation Status

TruewayIT, LLC operates with fewer than 100,000 subscriber lines and therefore qualifies for the small voice service provider exemption from the STIR/SHAKEN call authentication framework under 47 CFR § 64.6302(b). As a result, the Company is not currently required to implement STIR/SHAKEN in its own network.

Notwithstanding this exemption, TruewayIT relies on its upstream provider, [CARRIER REDACTED], to apply STIR/SHAKEN attestation to outbound calls originating from the Company's network to the extent technically feasible within [CARRIER REDACTED]'s infrastructure. Trueway commits to evaluating STIR/SHAKEN implementation in its own right as it grows and as technology evolves, and will adopt it no later than required by applicable FCC rules.

Section 3 — Know Your Customer (KYC) Procedures

Trueway conducts thorough due diligence on all prospective customers prior to enabling call origination services. The following information is collected and verified for every new customer account:

- **Business Identity:** Legal business name, physical address, mailing address, and primary contact information.
- **Government Identifiers:** Federal Employer Identification Number (EIN) or, for sole proprietors, a government-issued photo ID of the business owner.
- **Business Purpose:** Description of the nature of the business and the intended use of telephone services, including expected call volume and types of calls to be made.
- **Authorized Agent Verification:** The business owner or a duly authorized agent must be present in-person or via verified video conference to review and execute the Trueway Service Agreement.
- **Service Agreement Execution:** All customers must sign the Trueway Terms of Service and Acceptable Use Policy, which explicitly prohibit: (a) use of automated dialing systems or robocalling software, (b) spoofing caller ID information, (c) making calls that violate the TCPA, TSR, or any

applicable federal or state law, and (d) transmitting unlawful, fraudulent, or deceptive call traffic.

- **High-Risk Screening:** Trueway will not accept customers identified as high-risk, including but not limited to: call centers, lead generation companies, debt collection agencies, political dialing operations, or businesses routing international traffic through domestic numbers.

Endpoint Control: As an additional technical safeguard, all VoIP endpoints are installed and configured exclusively by Trueway technicians. Customers are never provided with SIP account credentials or administrative access to systems that would allow them to independently originate calls outside of the configured hardware endpoints. This eliminates the ability for customers to connect unauthorized auto-dialers or softphones to Trueway's network.

3.2 — Third-Party KYC Analytics Vendors

TruewayIT, LLC does **not** use any third-party vendor for KYC analytics, customer identity verification, or call traffic fraud screening. All customer due diligence is performed in-house by Trueway personnel through the following manual process:

- **Business Verification:** Trueway manually verifies the legitimacy of each prospective customer's business through review of publicly available business records, state registration databases, and web presence prior to onboarding. Businesses that cannot be independently verified as legitimate operating entities are not accepted.
- **In-Person or Verified Identity Confirmation:** The business owner or authorized agent must be present — either in person or via verified video conference — to review, sign, and acknowledge Trueway's Terms of Service and Acceptable Use Policy before service is activated. No service is provisioned based solely on electronic agreement without identity confirmation.
- **Signed Service Agreement:** Every customer executes a written service agreement that explicitly identifies the customer's business purpose, expected call usage, and acknowledgment of prohibited uses. This document is retained on file and serves as the primary KYC record for that account.
- **Manual Risk Assessment:** Prior to activation, Trueway staff assess the customer's stated business type, call volume expectations, and intended geographic calling patterns against known high-risk profiles. Accounts that raise concern — regardless of whether a formal analytics tool flags them — are declined.
- **Ongoing Account Familiarity:** Because Trueway serves a small, direct customer base with in-person equipment installation, Trueway personnel maintain direct familiarity with each customer's business. Unusual requests, changes in business activity, or customer behavior inconsistent with their stated purpose are identified through this direct relationship, without reliance on automated analytics tools.

Trueway believes this manual, relationship-based approach is appropriate and sufficient given the Company's small, vetted customer base and the structural controls described in Section 4 that prevent unauthorized call origination regardless of customer intent.

Section 4 — Traffic Monitoring and Anomaly Detection

4.1 — Third-Party Analytics Vendors

TruewayIT, LLC does **not** use any third-party vendor for call traffic analytics, robocall detection, or traffic monitoring. The Company does not subscribe to services such as call analytics platforms, fraud detection data feeds, or third-party robocall screening tools. All traffic monitoring and anomaly identification is performed through the combination of in-house practices, upstream carrier-level controls, and reactive investigation described in Sections 4.2 through 4.4 below.

4.2 — Primary Control: Structural Prevention

TruewayIT, LLC's primary mitigation strategy against illegal robocall traffic is structural in nature. Because of how Trueway's network is designed and operated, the ability for illegal robocall traffic to originate from the Company's systems is substantially eliminated before any monitoring is required. Specifically:

- **Physical Endpoint Control:** All VoIP endpoints are installed and configured exclusively by Trueway technicians. No customer installation or self-provisioning is permitted.
- **No Customer Credential Access:** Customers are never provided with SIP account credentials, administrative portal access, or any other means to independently originate calls outside of the physical hardware endpoints Trueway has installed and configured. This technically prevents the connection of auto-dialers, softphones, or robocalling software to Trueway's network.
- **Hardware-Only Origination:** Call origination is restricted to fixed, registered hardware endpoints. Calls cannot be originated from software clients or third-party systems without Trueway's direct involvement.
- **Vetted, Small Customer Base:** Trueway serves a small number of known, vetted business customers. Each customer has been screened through the KYC process described in Section 3, and high-risk customer categories are categorically rejected. The Company does not provision service to call centers, lead generation operations, or any entity with a high potential for abusive calling.

As a result of these structural controls, Trueway's network does not provide a viable pathway for illegal robocall traffic origination. A bad actor cannot connect to the network programmatically, cannot obtain credentials to do so, and cannot scale call volume beyond the physical hardware in place.

4.3 — Upstream Carrier-Level Controls

As a secondary layer of mitigation, Trueway relies on the network-level controls and traffic monitoring capabilities of its upstream voice carrier, [CARRIER REDACTED], Inc. ([CARRIER REDACTED]). As a major registered U.S. voice service provider, [CARRIER REDACTED] maintains robust anti-robocall infrastructure, including:

- **STIR/SHAKEN Call Authentication:** [CARRIER REDACTED] applies STIR/SHAKEN attestation to calls originating from Trueway's network to the extent technically supported, providing downstream carriers and terminating providers with call authentication signals.
- **Traffic Anomaly Detection:** [CARRIER REDACTED] employs automated systems to detect and flag anomalous traffic patterns — including sudden volume spikes, invalid caller ID, and short-duration call clusters — at the carrier level.
- **Robocall Blocking and Filtering:** [CARRIER REDACTED] participates in industry robocall mitigation programs and applies network-level blocking of known illegal traffic patterns.

Trueway monitors its relationship with [CARRIER REDACTED] and will act promptly on any traffic concerns, flags, or notifications communicated by [CARRIER REDACTED] regarding traffic originating from Trueway's accounts.

4.4 — Reactive Investigation and Escalation

In addition to the structural and carrier-level controls above, Trueway conducts reactive investigations whenever a concern is identified. Triggers for investigation include:

- A complaint received from any party regarding calls originating from Trueway's network or a customer's assigned numbers.
- A traceback request received from the FCC, the USTelecom Industry Traceback Group (ITG), or any other authorized entity.
- A notification or flag raised by [CARRIER REDACTED] regarding anomalous traffic from Trueway's accounts.

- Any internal observation of unusual customer behavior, service usage patterns, or customer communications that suggest potential misuse.

Upon any such trigger, Trueway initiates the following escalation process:

- **Step 1 - Internal Review (same business day as trigger):** Trueway pulls and reviews available call records for the relevant customer account, examining call volume, duration, caller ID usage, and call destinations to assess whether the traffic is consistent with the customer's stated business purpose.
- **Step 2 - Customer Contact (within one business day of trigger):** If the call data cannot be explained by normal business activity, the customer is contacted directly and required to provide a written explanation.
- **Step 3 - Suspension (within two business days of trigger):** If the customer cannot provide a satisfactory explanation, or if the data strongly indicates illegal activity, outbound call origination is suspended for that account pending further investigation.
- **Step 4 - Termination:** If investigation confirms a Terms of Service violation or violation of applicable law, service is permanently terminated and the matter is documented for potential referral to the FCC, FTC, or applicable state authorities.

Section 5 — Traceback and Complaint Response

TruewayIT, LLC is committed to full cooperation with traceback investigations conducted by the FCC, the USTelecom Industry Traceback Group (ITG), and other authorized entities. The Company maintains a dedicated point of contact for all robocall mitigation and traceback matters:

Traceback Point of Contact	
Name:	[REDACTED], President/CEO
Email:	[REDACTED]
Phone:	[REDACTED]
Availability:	Monday – Friday, 8:00 AM – 5:00 PM CT

Upon receipt of a traceback request from the FCC, the ITG, or any other authorized government or industry body, Trueway commits to:

- Acknowledge the traceback request within **24 hours** of receipt.
- Provide all requested call records and relevant traffic data within **72 hours** of the request, or sooner where technically feasible.
- Cooperate fully with any investigation, including identifying the customer account responsible for the traffic in question.
- Take immediate remediation action (up to and including service suspension) against any customer identified as a source of illegal robocall traffic.
- Document all traceback requests, responses, and resulting actions in the Company's internal compliance records.

Section 6 — Contractual Prohibitions and Enforcement

All Trueway customers are bound by the Company's Terms of Service and Acceptable Use Policy, which contain explicit prohibitions on illegal call traffic. Specifically, the agreement prohibits customers from:

- Using Trueway's network to originate automated, pre-recorded, or artificial voice calls to any person without proper consent as required by the Telephone Consumer Protection Act (TCPA) and Telemarketing Sales Rule (TSR).
- Transmitting calls with false, misleading, or spoofed caller ID information in violation of the Truth in Caller ID Act.
- Using auto-dialers, predictive dialers, or any robocalling software in connection with Trueway's services.
- Reselling or sharing Trueway's VoIP services to third parties without express written authorization.
- Routing traffic that originates from, or is destined for, foreign call centers or overseas origination points.

Violations of these provisions constitute grounds for immediate service suspension and/or termination without refund, as well as potential referral to the FCC, FTC, or applicable state authorities. Trueway reserves the right to seek damages for violations that expose the Company to regulatory liability.

Section 7 — Upstream Provider Disclosure

TruewayIT, LLC transmits its outbound call traffic through the following upstream voice service provider:

Upstream Provider	Role	RMD Filing Status
[CARRIER REDACTED]	Primary Voice Origination & Transit Provider	Registered in FCC RMD

Trueway's service agreement with [CARRIER REDACTED] requires that [CARRIER REDACTED] apply applicable STIR/SHAKEN attestation to calls originating from Trueway's network. Trueway does not knowingly accept call traffic from any provider not registered in the FCC Robocall Mitigation Database.

Section 8 — Certification

I, [REDACTED], as President/CEO and an authorized representative of TruewayIT, LLC, hereby certify under penalty of perjury that: (1) I have read and understand the FCC's rules regarding robocall mitigation set forth in 47 CFR Part 64, Subpart Z; (2) the information contained in this Robocall Mitigation Plan is true, accurate, and complete to the best of my knowledge; (3) TruewayIT, LLC has implemented and will maintain the robocall mitigation measures described herein; and (4) TruewayIT, LLC will update this plan in the Robocall Mitigation Database within 10 business days of any material change to these practices.

Signature: _____

Printed Name: [REDACTED]

Title: President / CEO

Company: TruewayIT, LLC

Date: June 05, 2026