

Robocall Mitigation Program Description

This Robocall Mitigation Program (“Program”) describes the reasonable steps that **Reach IT Solutions LLC** has taken to avoid originating illegal robocall traffic, in compliance with **47 C.F.R. § 64.6305(d)(ii)-(iii)**, and the updated FCC requirements under DA-24-73. It also describes our use of Viirtue as a part of our STIR/SHAKEN and carrier service infrastructure.

1. STIR/SHAKEN Implementation Status

- **Extent of Implementation:** **Reach IT Solutions** has implemented the STIR/SHAKEN authentication framework across the IP portions of its network. All traffic originated that passes through our IP voice network is signed and authenticated in accordance with § 64.6301(a)(1)-(2).
 - **Extensions or Exemptions:** In non-IP portions of our network where we lack the infrastructure to sign calls (e.g., certain legacy TDM or circuit-switched segments), we have requested an extension under § 64.6304. The basis for this extension is the present inability to control certain network elements required for generating signed tokens.
 - **Use of Viirtue:** We engage Viirtue (or similar carrier/STIR/SHAKEN service provider) to provide secure certificate management, token issuance, and call signing capability. Viirtue acts as our certificate authority and/or helps with the signing of calls where we do not directly hold a certificate. We ensure that any third-party (including Viirtue) arrangement meets the guardrails specified in the relevant FCC orders for third-party authentication.
-

2. “Know Your Customer / Know Your Upstream Provider” Measures

- **Customer Vetting Procedures:** Before onboarding, customers (end users and resellers) must provide verifiable business or individual identification, contact information, physical address, and a description of the anticipated use of voice service, including expected volume of calls and traffic patterns.
 - We require customers to agree contractually not to originate illegal robocalls or spoofed traffic. We monitor for compliance.
 - **Upstream Providers:** We maintain records of all upstream carriers/carrier partners through whom traffic flows (wholesale or transit). We require written assurances from upstream providers regarding their own compliance with robocall mitigation obligations, including that they are listed (or will list) in the Robocall Mitigation Database, that they respond to traceback requests, and that they enforce STIR/SHAKEN or equivalent authentication.
-

3. Traffic Analytics, Monitoring, and Blocking

- **Systems Used:** We use an internal analytics platform augmented by third-party analytics, currently including Viirtue's analytics, to monitor outgoing call traffic. The analytics system is designed to detect anomalous patterns, e.g., sudden surges in call volume, high rates of failures or rejections, unusual calling destinations, or atypical traffic signatures that suggest spoofing or illegal robocalls.
 - **Blocking & Mitigation:** Whenever suspicious or clearly illegal traffic is detected, we have a process to block or rate-limit such traffic, including declining to carry calls from customers who repeatedly violate policy.
 - **Periodic Review & Updating:** We review the thresholds, detection rules, and system efficacy at least quarterly. We adjust rules as needed to respond to new threats.
-

4. Traceback Commitment

- We commit to responding **within 24 hours** to all traceback requests from the Commission, law enforcement, and the industry traceback consortium.
 - We maintain internal procedures and staff responsible for handling traceback requests, preserving call records, metadata, and signaling information necessary to assist with investigations.
-

5. Certifications & Declarations

- We affirm that all of the calls we originate on our network are subject to this Program, consistent with § 64.6305(a).
 - We confirm that any prior certification in the Robocall Mitigation Database has not been removed by Commission action, nor have we been prohibited from filing.
 - We declare whether we have fully implemented STIR/SHAKEN, or partially (on a portion), or not at all (with explanation, in the case of lack of control or an approved extension).
-

6. History of Legal, Regulatory or Enforcement Actions

- We state that in the past two years, neither **Reach IT Solutions LLC**, nor any entity over which it has common ownership, management, directors, or control, has been the subject of formal Commission, law enforcement, or regulatory investigation or action with findings of actual or suspected wrongdoing for facilitating illegal robocalls or spoofing, nor for a deficient RMD certification or mitigation program description. *(Or, if there has been such action, provide summary of what entity, when, findings, current status, etc.)*

7. Contact and Business Information

- Business Name: **Reach IT Solutions LLC**
- Primary Address: **7901 Prescot Glen Pkwy, Waxhaw, NC 28173**
- Other Names in Use / Previously Used: **Reach IT Solutions**
- Whether Foreign Provider: **No**
- Officer Responsible: **Alex Alcantara, Company Officer, support@reachitsolutions.com**
- Role in the Call Chain: **Reseller.**

8. Cooperating with FCC Rules & Updating Filings

- We will keep our indications of STIR/SHAKEN implementation status (full / partial / none) current, including submitting amendments in the Robocall Mitigation Database within **10 business days** of any change to the required information. (As per the updated rules under DA-24-73.)
- We will maintain our Program, updating as required based on our risk assessments, new service offerings, regulatory changes, or changes in vendor relationships (including with Viirtue).

9. Use of Carrier / Vendor Services – Specifics

To illustrate how Viirtue is incorporated:

- **Certificate Management:** Viirtue holds or assists with obtaining certificates required for STIR/SHAKEN attestation, including handling the SPC token (if we do not maintain our own).
- **Signing Process:** Calls that traverse parts of our network that connect to VoIP or SIP trunks are signed in accordance with levels A/B attestation appropriate under FCC rules.
- **Vendor Analytics:** Viirtue provides analytics dashboards and reporting which we use to monitor signed vs. unsigned traffic, failures in signature verification, and suspected abuse.
- **Vendor Relations & SLAs:** We have service level agreements with Viirtue requiring cooperation in traceback, timely issuance of certificates, audits of signing practices, and transparency about signing errors.