



Landing Point

LP Telecom dba Landing Point Telecom **Robocall Mitigation Plan**

March, 2026

The Federal Communications Commission (“FCC”) requires all voice service providers to implement and maintain effective measures to prevent the origination, transmission, and processing of illegal robocall traffic within U.S. communications networks. These requirements are set forth in 47 C.F.R. § 64.6305 and further detailed in the Sixth Caller ID Authentication Report and Order (WC Docket No. 17-97).

Pursuant to these rules, voice service providers must file a Robocall Mitigation Plan (“RMP”) and certification in the FCC’s Robocall Mitigation Database (“RMD”), indicating whether they have fully implemented the STIR/SHAKEN framework and certifying that any calls they originate, carry, or process are subject to an effective robocall mitigation program.

In accordance with 47 C.F.R. § 64.6305(a)(2), LP Telecom’s RMP describes reasonable and effective measures to prevent illegal robocalls and affirms LP’s commitment to respond within 24 hours to traceback requests from the FCC, law enforcement, and the Industry Traceback Group (“ITG”), and to cooperate fully in investigations of suspected unlawful robocall activity.

This RMP also outlines LP’s Know Your Customer (KYC) procedures, as well as the analytic tools and third-party services used to detect, monitor, and mitigate potentially illegal traffic. LP will update its RMD filing within ten (10) business days of any material change to the information provided.

Finally, LP affirms that any prior certification filed in the RMD has not been removed or revoked by Commission action and that LP is not prohibited from filing or maintaining certification in the RMD.

1. Stir-Shaken Implementation

LP has fully implemented the STIR/SHAKEN authentication framework on its network. All calls that traverse our network must be signed with a minimum of a “C” attestation prior to reaching our network to be routed to our downstream carriers. Any unsigned calls are signed with a C attestation from LP.

2. Traceback Requests

LP will cooperate with the FCC, law enforcement and the ITG on all traceback requests and investigations. All traceback requests will be respond within a 24-hour window. In addition to the automated traceback tickets generated by the ITG, LP will also open internal tickets with any customer/upstream carriers identified in the traceback.

All customers/upstream carriers must respond to traceback requests within the 24-hour window or face immediate account suspension.

If 3 or more traceback requests of different campaign types or dates lead back to the same customer/upstream carrier within 30 days, they will have their account suspended for 90 days.

Traceback Request Single Point of Contact:

Name: Omar Luna

Title: Manager

Email Address: noc@landingpointtele.com

3. Customer Vetting Practices

In an effort to minimize or prevent illegal robocalls from traversing our network, LP will use its best practices to vet the identity of all of its customers/upstream carriers. LP attempts to confirm the identity of its potential customers by collecting KYC information such as physical customer location, billing address, state or province, country, year of incorporation, contact person(s), federal tax ID, 499 ID, and RMD number.

In addition to vetting the identity of potential customers, LP also collects the following information regarding:

- The nature of the customer's business.
- Traffic profile.
- Do they actively participate in the traceback process?
- Have they been determined to be a "Non-Cooperative Voice Service Provider"?
- Have they been determined to be a "bad-actor upstream voice service provider"?
- Have they ever had an adverse judgement against them in a civil lawsuit alleging claims under the TSR, the TCPA, or any other lawsuits regarding Robocalls, automated dialing, calls to the DNC Registry or the do not call registry of any state, spoofed caller ID numbers, or otherwise unlawful telemarketing or solicitations.

As part of its efforts in vetting potential customers LP will require all customers/upstream carriers to provide trade and credit references.

4. Network Monitoring, Call Filtering and Blocking

LP currently uses the SipNav soft switch platform (Third party vendor). SipNav provides its users with a robust selection of robocall mitigation services such as:

- Call filtering to block invalid originating numbers, neighborhood dialing, and numbers on the Somos® DNO list from traversing our network.
- The ability to block all calls that have not been signed via STIR SHAKEN from traversing our network.
- Block lists to input originating or terminating numbers that appear in carrier tickets to prevent continuing abuse.
- Global block lists maintained by the platform provider that include originating or terminating numbers, and media IP addresses that have been identified in ITG tracebacks and FCC enforcement actions.
- We also utilize the Roboguard service by FraudCentral.io which identifies, and blocks known “Bad Actors” in real time.

LP utilizes SIP Code 603+ as the standardized response for analytics-based call blocking, ensuring proper signaling, compliance with applicable FCC requirements, and transparency across the network. Legacy SIP response codes (e.g., 603, 607) are not used for analytics-based blocking determinations.

LP monitors the usage of its network and examines call detail records (CDRs) for the purpose of detecting suspicious call activity and/or calling patterns. When we detect or are notified of suspected illegal robocalling or spoofing, we seek to immediately identify the customer/upstream carrier routing those calls so that we may take the appropriate action. The actions taken can include but are not limited to blocking the originating and terminating numbers pending investigation, immediately notifying the upstream carrier routing the calls of the issue and verifying the amount of traffic being received from our customer’s client(s).

5. Mandatory Blocking Following Commission Notification

In accordance with FCC robocall mitigation rules, LP will promptly investigate and block any illegal traffic upon receiving a Notice of Suspected Illegal Traffic from the FCC’s Enforcement Bureau.

6. Only Accepting Traffic from Providers in the RMD

In accordance with 47 C.F.R § 64.6305(e)(1), LP only accepts calls from Providers listed in the RMD.

7. Contractual Provisions to Mitigate Illegal Robocalls and Acceptable Use Policy (AUP).

LP requires all customers to execute a Master Service Agreement (“MSA”) that obligates compliance with all applicable federal, state, and international telecommunications laws and regulations, including those related to robocalls, caller ID authentication, and consumer protection.

LP prohibits the use of its services for any unlawful, fraudulent, abusive, or deceptive activity, including illegal robocalls, caller ID spoofing, or other non-compliant traffic, as further described in its Acceptable Use Policy (“AUP”).

Pursuant to its MSA and AUP, LP may suspend or terminate services, without prior notice, where necessary to address policy violations, suspected fraud, regulatory compliance obligations, or to protect network integrity.