



Siplink Communications PVT LTD

Robocall Mitigation Plan

Updated February 23, 2026

Company Name: Siplink Communications PVT LTD
Company Address: 30 N Gould St Ste R
Sheridan, WY 82801
Company Phone: 916-236-1262

Purpose and Scope:

Siplink Communications PVT LTD ("Siplink") is a voice service provider that originates traffic to the public switched telephone network (PSTN) and maintains a robocall mitigation program consistent with 47 CFR § 64.6305, including STIR/SHAKEN caller ID authentication in accordance with 47 CFR § 64.6301(a), and may update its filing and associated plan information within 10 business days when filing information changes.

Provider Role

Siplink is a U.S.-based voice service provider that furnishes Hosted PBX, SIP trunking, and DID provisioning services directly to end-user customers. Calls originate on our network using NANP (U.S.) telephone numbers, including for certain end users operating offshore call-center functions, and are delivered to the PSTN via Siplink's downstream interconnection partners. We do not operate as a gateway or other intermediate provider for foreign-originated traffic; it provides service to end users and originates calls on its own network.

STIR/SHAKEN Implementation Details:

Siplink certifies that it has implemented STIR/SHAKEN caller ID authentication across the IP portions of its network for the SIP calls it originates, consistent with 47 CFR § 64.6301(a). We have registered with the STI-PA using OCN **865K**. We have our own STIR/SHAKEN certificate issued by Telonium Certification Authority (STI-CA) that we use when authenticating calls we originate. We have implemented a STIR/SHAKEN solution supplied by TransNexus.

Siplink assigns attestation levels (A/B/C) based on its verification of the calling party and confirmation of the calling party's authority to originate calls using the associated telephone number(s), consistent with applicable FCC rules, orders, and guidance.

Know Your Customer:

Siplink has enforceable Terms of Use and/or an Acceptable Use Policy incorporated into its customer contracts. These policies define the circumstances under which Siplink may deny, suspend, or terminate service.

Before providing service to new customers, Siplink conducts customer due diligence designed to reduce the risk of illegal robocall traffic. Siplink confirms, as applicable:

A handwritten signature in blue ink is written over a circular purple stamp. The stamp contains the text "SIPLINK COMMUNICATIONS PVT LTD" around the perimeter and a small star in the center.

- Customer identity
- Incorporation/formation documents
- Customer's authority to use the telephone number(s) presented on calls
- Service address
- Payment method and/or creditworthiness

Enhanced review is triggered by high-risk verticals, unusually high projected volume, discrepancies in identity, repeated changes to caller ID, short-lived accounts, or any indicators of lead-generation or robocall behavior inconsistent with the stated use case.

Traffic monitoring, analytics and internal enforcement:

Siplink uses real-time call analytics, including TransNexus and in-house monitoring tools, to review all outbound voice traffic and help prevent the origination or transit of illegal robocalls. These tools provide reporting and alerts to identify suspicious patterns such as high-volume, short-burst calling and abnormal spikes. The system also flags outbound calls associated with poor-reputation or invalid calling numbers, including numbers that are unallocated, invalid, or listed on Do Not Originate lists.

We apply the same mitigation process to all outbound calls. When suspicious traffic is identified, we promptly investigate to determine whether the caller is attempting to originate or carry unlawful robocalls. If the traffic appears unlawful, we issue a warning and require immediate remediation. Continued suspicious or unlawful traffic results in escalation up to and including suspension or termination of service.

Siplink has established methods and procedures to monitor its network and detect / prevent fraudulent activity. The company uses call authentication, call labeling, and call blocking services to protect its networks and consumers from harmful calls. It also uses software to monitor its network's daily usage and has established methods and procedures in place to address issues as soon as they are identified.

If a pattern of questionable activity is detected Siplink will require its customer to remedy the problem and, if effective action is not taken, service to the customer may be suspended and/or terminated.

Know Your Upstream Provider

Siplink does not accept traffic from upstream providers, resellers or partners. We only carry traffic associated with our own end-user customers.

Traceback Commitment

Siplink remains committed to responding fully and within 24 hours to call traceback requests from the Commission, law enforcement, and the traceback consortium, and to cooperating with such entities in investigating and stopping illegal robocallers initiating calls.

