



Simple Phone Company - Robocall Mitigation Program (RMP)

Updated March 2026

Purpose and Scope

Pursuant to 47 C.F.R. § 64.6305, Simple Phone Company (“smpl”) submits this Robocall Mitigation Plan describing its current STIR/SHAKEN status and the policies, practices, and procedures it uses to prevent and mitigate illegal robocalls originating on its service. This Robocall Mitigation Plan applies to all outbound voice traffic that originates on smpl’s network.

Provider Role / Call Flow

smpl serves primarily end-user business customers, with limited white-label reseller arrangements. smpl does not accept third-party provider traffic for transit and does not operate as a gateway provider for foreign-originated traffic.

smpl does not directly operate or control the underlying switching, SBC, or softswitch infrastructure used to originate outbound calls to the PSTN. smpl’s hosted platform provider operates and maintains the switching environment on which smpl’s services run. smpl manages customer devices, service configuration, and customer-level call flow settings, but does not exercise control over the underlying network infrastructure necessary to implement STIR/SHAKEN.

STIR/SHAKEN Implementation Status

smpl has not represented that it has fully implemented STIR/SHAKEN using its own SPC token and STI certificate. Based on its current service architecture, smpl does not have direct control over the network infrastructure necessary to implement STIR/SHAKEN itself and therefore relies on underlying platform and carrier arrangements for the routing and network functions associated with outbound traffic.

Accordingly, to the extent STIR/SHAKEN has not been fully implemented by smpl directly, the basis is that smpl lacks control over the network infrastructure necessary to implement STIR/SHAKEN under 47 C.F.R. § 64.6305(d)(2)(i).

ROBOCALL MITIGATION PROGRAM

Know Your Customer

Before activating new customers, smpl collects and reviews identifying and business-related information reasonably necessary to understand who is using the service and for what purpose. Depending on the customer and service type, this may include business identity information, contact information, service details, payment details, and other information sufficient to evaluate whether the requested use is consistent with legitimate communications activity.

For its limited reseller white-label customers, smpl performs additional diligence appropriate to the nature of the relationship and expected use of the service.

If suspicious call patterns, upstream notifications, traceback requests, or complaints indicate potential misuse, smpl escalates the matter for review, may request clarification or supporting documentation,

and may restrict, suspend, or terminate service pursuant to its acceptable use policy and contractual terms, which prohibit unlawful robocalling, spoofing, fraud, and other illegal telecommunications activity.

Traffic Monitoring, Analytics and Enforcement

smpl monitors customer traffic and service usage for suspicious patterns that may indicate illegal robocalling, spoofing, fraud, or other abusive activity. Monitoring may include review of calling behaviors such as unusual call volumes, burst activity, short-duration patterns, invalid or suspicious caller ID usage, and other irregular traffic indicators. smpl also relies, in part, on analytics, notifications, and traffic-related alerts provided by its hosted platform provider, 2600Hz, and carrier partners, including Telnyx and Bandwidth.

If suspicious activity is identified, smpl investigates and may take action including temporary suspension, blocking, limitation of service, requests for clarification or supporting information, or termination of the customer relationship where warranted.

Traceback Commitment and Plan Governance

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

smpl has not been prohibited from filing a certification in the Robocall Mitigation Database.

smpl reviews and maintains its robocall mitigation program and updates it within 10 business days when filing information, services, traffic patterns, or risk controls change.

Know Your Upstream Provider

smpl does not accept third-party traffic for transit. Outbound calls originate only from smpl's customer bases; inbound calls are received from carrier partner(s) only for delivery to those customers.

smpl coordinates with its upstream carrier partner(s) on suspected illegal traffic and traceback requests.

Point of Contact:

Name: Christopher Meadows

Title: CEO

Email: chris@smpl.co

Phone: 844-404-7675

Mitigation Commitment

Simple Phone Company remains committed to taking reasonable steps to prevent and mitigate illegal robocalls and to ensuring that its services are not used to facilitate unlawful traffic. smpl will continue to review its service arrangements, customer activity, and upstream relationships and will revise its Robocall Mitigation Database filing if its STIR/SHAKEN status or operational structure materially changes.