

Robocall Mitigation Program Description

S Tier Communications LLC

47 C.F.R. §§ 64.6305(a), 64.6305(d)(2) | Effective September 14, 2026

1. Provider Overview and Scope

S Tier Communications LLC ("S Tier" or the "Provider") is a U.S. non-facilities-based voice service provider that resells business voice/SIP services using wholesale network services supplied by a third-party carrier. S Tier does not operate the underlying public switched telephone network (PSTN) facilities used to originate or terminate calls.

Wholesale network provider: **Skye Telecom LLC d/b/a Skyetel ("Skyetel")**. S Tier purchases wholesale SIP trunking/network services from this provider for delivery of customer voice traffic to and from the PSTN.

This program applies to calls originated through S Tier services and is intended to satisfy S Tier's obligations under 47 C.F.R. § 64.6305(a) to take reasonable steps to avoid originating illegal robocall traffic, respond to traceback requests within 24 hours, and cooperate with the FCC, law enforcement, and the industry traceback consortium in investigating and stopping illegal robocallers.

2. STIR/SHAKEN Implementation

S Tier has not implemented the STIR/SHAKEN authentication framework on its own network. S Tier does not own or control the underlying network infrastructure necessary to perform STIR/SHAKEN authentication. Skyetel, S Tier's wholesale SIP provider, originates S Tier customer traffic onto the public network and performs caller-ID authentication, as applicable, using Skyetel's own STIR/SHAKEN credentials and certificate.

Accordingly, S Tier will certify "No STIR/SHAKEN Implementation" in its Robocall Mitigation Database filing and will explain that it lacks control over the network infrastructure necessary to implement STIR/SHAKEN. S Tier does not represent that calls authenticated by its wholesale provider are authenticated using an S Tier certificate.

3. Know-Your-Customer and Customer Onboarding Controls

Before activating service for a new customer, and when materially renewing or expanding service, S Tier uses risk-based customer due diligence designed to establish that the customer is a legitimate user of voice service and to reduce the risk that S Tier services will be used to originate illegal traffic. The onboarding process includes, as appropriate to the customer and risk presented:

- Collecting the customer's legal name, any DBA name, service/billing address, website or other business presence, responsible contact information, and billing/payment information.
- Obtaining a description of the customer's business and intended use of the voice service, including expected call types and approximate calling volume when relevant.
- Reviewing available business-registration, website, contact, payment, or other information for consistency with the customer's stated identity and intended use.
- Requiring customers to provide accurate information and declining or delaying activation where identity, business purpose, or authority to obtain service cannot be reasonably verified.
- Applying enhanced review to customers presenting risk indicators such as inconsistent identity information, unusually high-volume outbound calling, short-duration traffic inconsistent with the stated use, requests to present unverified caller-ID numbers, repeated abuse complaints, or an unclear business purpose.

S Tier does not knowingly provide anonymous voice service to customers whose identity or legitimate service purpose cannot be reasonably established. If information obtained after activation materially undermines the customer's legitimacy or permitted use, S Tier may restrict, suspend, or terminate service while the matter is investigated.

4. Acceptable Use and Prevention of Illegal Calling

S Tier prohibits customers from using its services to originate illegal robocalls, unlawful telemarketing, caller-ID spoofing intended to defraud or cause harm, or other calls that violate applicable federal or state law. S Tier's customer terms and enforcement practices are intended to make clear that customers must comply with applicable calling-consent, do-not-call, caller-identification, and telemarketing requirements.

Customers are required to use caller-ID information that they are authorized to use. Requests to use externally assigned caller-ID numbers may be subject to verification. S Tier may reject or restrict traffic where the presented identity, customer history, complaint information, or calling pattern indicates a material risk of illegal or abusive traffic.

5. Traffic Monitoring, Analytics, and Complaint Review

Third-party/network analytics. S Tier does not currently operate a separate proprietary robocall analytics engine. S Tier relies on network-level controls made available through Skytel, including STIR/SHAKEN authentication and any fraud-screening, call-analytics, or automated blocking features applied by Skytel to the wholesale service. S Tier does not currently use another third-party call analytics vendor for originating traffic unless separately disclosed in an updated RMD filing or mitigation plan.

S Tier supplements wholesale network controls by reviewing information reasonably available to it, including call-detail records, customer account history, carrier notifications, traceback requests, complaints, and unusual changes in calling behavior. Indicators that may trigger review include sudden or unexplained traffic spikes, high concentrations of short-duration outbound calls, repeated consumer or carrier complaints, use of caller-ID information inconsistent with the customer account, and other patterns inconsistent with the customer's stated business use.

When suspicious activity is identified, S Tier may contact the customer for additional information, limit calling capabilities, require corrective action, suspend service, or terminate the account depending on the circumstances and urgency of the risk.

6. Response to Tracebacks, Regulatory Requests, and Abuse Reports

S Tier commits to respond fully and within 24 hours to traceback requests from the Federal Communications Commission, law enforcement, and the industry traceback consortium. S Tier also commits to cooperate with those entities in investigating and stopping any person or entity using S Tier services to originate illegal calls.

S Tier maintains a designated compliance function for robocall and traceback matters. Upon receipt of a traceback or credible abuse report, S Tier will promptly review available account and call-detail information, identify the customer associated with the traffic when possible, identify the relevant wholesale route/provider, preserve relevant records, and provide a complete response within the required timeframe.

RMD/traceback contact: Jose Juan Salinas Salto, Regulatory Compliance Officer **Email:** jose.salto@stiercomm.com **General compliance mailbox:** regulatory@stiercomm.com **Telephone:** (307) 400-5960

If a traceback, FCC notice, law-enforcement request, or other credible evidence indicates illegal traffic, S Tier will take prompt remedial action appropriate to the circumstances, which may include restricting specific calling capabilities, suspending service, terminating the customer, coordinating with the wholesale provider, and preserving relevant records for investigation.

7. Wholesale Provider Due Diligence

S Tier uses established wholesale voice providers rather than accepting voice traffic from unknown or anonymous third-party carriers. Before establishing or materially renewing a wholesale voice relationship, S Tier takes reasonable steps to confirm the provider's identity, role, and regulatory status. S Tier reviews the provider's Robocall Mitigation Database status where applicable and considers available FCC enforcement or blocking information relevant to the provider.

S Tier expects its wholesale provider to maintain required robocall mitigation and STIR/SHAKEN practices applicable to the provider's role in the call path. S Tier will reassess a wholesale relationship if it receives credible evidence that the provider is facilitating a high volume of illegal traffic, has been removed from the RMD, is subject to a relevant FCC blocking order, or otherwise presents a material robocall-compliance risk.

S Tier does not presently operate as a gateway provider and does not intentionally accept unrelated third-party transit traffic for carriage onto the U.S. network. If S Tier changes its role in the call path, it will update this program and its RMD filing as required.

8. Customer Enforcement and Remediation

S Tier applies a risk-based escalation process. The nature and speed of the response depends on the evidence available, seriousness of the conduct, and risk of continued illegal traffic. Potential actions include:

- Requesting an explanation or supporting documentation from the customer;
- Requiring the customer to cease or modify the activity at issue;
- Restricting caller-ID presentation or outbound calling features where technically available;
- Temporarily suspending outbound service while an investigation is pending;
- Terminating service when S Tier determines that a customer is using, or is likely to continue using, the service for illegal calling; and
- Coordinating with the wholesale provider, the FCC, law enforcement, or the industry traceback consortium as appropriate.

S Tier will not knowingly continue providing unrestricted originating service to a customer when credible information demonstrates that the customer is using the service to originate illegal robocall traffic and effective mitigation has not occurred.

9. Records and Program Administration

S Tier maintains customer onboarding, account, billing, complaint, and call-detail information to the extent reasonably available and consistent with applicable legal, contractual, and business-record requirements. Relevant records are preserved when S Tier becomes aware of a traceback, enforcement inquiry, or abuse investigation involving the account.

The compliance function periodically reviews this mitigation program and S Tier's actual practices, including customer onboarding controls, abuse handling, wholesale-provider status, and traceback response procedures. S Tier will update its Robocall Mitigation Database filing within the period required by FCC rules when information required in the filing materially changes, and will complete the required annual recertification.

10. Regulatory / Enforcement History

For the prior two-year period applicable to this filing, S Tier Communications LLC has no reportable legal or regulatory actions, investigations, or enforcement proceedings to disclose.

11. Commitment

S Tier Communications LLC is committed to preventing its services from being used to originate illegal robocalls. S Tier will maintain reasonable customer due diligence and abuse-prevention measures; use available network, complaint, and call-detail information to identify suspicious traffic; respond fully within 24 hours to qualifying traceback requests; and cooperate with the FCC, law enforcement, the industry traceback consortium, and its wholesale provider to investigate and stop illegal calling activity.

This program is intended to describe S Tier's actual robocall mitigation practices as of the effective date above. S Tier will revise the program as necessary to reflect material changes in its network role, wholesale arrangements, analytics, customer controls, or applicable FCC requirements.