

Robocall Mitigation Plan

Business Information

SouthLight Services, LLC
3300 South Parker Road
Suite 325
Aurora, CO 80014

Contact Information

Tina Telson
CEO
720-783-9909
tina@southlightservices.com

Overview

In the Commission's recent release, *Call Authentication Trust Anchor*, Sixth Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd. 2573 (2023) ("R&O"), it is stated that all voice service providers ("VSPs") must file robocall mitigation plans ("RMPs") that, among other things, outline "reasonable steps" taken to avoid originating illegal robocalls.

In addition to the "reasonable steps," the FCC requires that a RMP include:

- "know your customer" procedures;
- "know your upstream provider";
- ownership information;
- a description of any call analytics system used to identify and block illegal traffic; and
- whether a third-party vendor is used and if so, the name of the vendor.

The FCC previously stated that an RMP is sufficient if the detailed practices in the plan can reasonably be expected to significantly reduce the origination of illegal robocalls and the VSP complies with the practices it describes in its filing.

Know Your Customer ("KYC")

SouthLight Services, LLC ("SouthLight") maintains a comprehensive KYC framework designed to verify client identity, ensure regulatory compliance, and protect the integrity of our network and services.

Client Onboarding & Identity Verification

Prior to service activation, all prospective clients are required to provide the following:

- Legal business name, principal business address, and proof of entity (e.g., Articles of Incorporation, business license, or equivalent state registration)
- Federal Tax Identification Number (EIN) or equivalent government-issued identifier
- Authorized signatory identification, including government-issued photo ID
- Primary contact information including verified business email and phone number
- Service use case documentation, including intended call volumes and geographic scope

- Billing and payment authorization credentials from an authorized financial representative

Residential customers are required to provide government-issued photo identification, verified billing address, and consent acknowledgment prior to account activation.

Payment Restrictions & Monitoring

SouthLight enforces controls on payment frequency and thresholds to mitigate fraud risk. Accounts flagged for unusual payment patterns — including excessive frequency, mismatched billing information, or high-volume prepayment requests — are subject to manual review prior to processing. Payment methods are validated against account ownership records, and anomalies are escalated to our compliance team.

Caller ID Limitations & Controls

Customers are prohibited from spoofing, misrepresenting, or programmatically cycling Caller IDs in violation of the Truth in Caller ID Act. Caller ID usage is contractually restricted to numbers that have been verified, registered, and authorized under the customer's account. Unauthorized Caller ID manipulation is grounds for immediate service suspension.

Ongoing Customer Verification

Beyond initial onboarding, SouthLight conducts periodic account reviews to confirm continued compliance with our acceptable use policies. This includes re-verification of business credentials for high-volume accounts, review of traffic patterns for behavioral anomalies, and proactive outreach when usage deviates materially from established baselines. Customers found to be in violation of KYC requirements or acceptable use standards are subject to service suspension pending investigation.

Know Your Upstream Providers

In accordance with the Commission's directive in *Advanced Methods to Target and Eliminate Unlawful Robocalls, and Call Authentication Trust Anchor*, Seventh Report and Order in CG Docket 17-59 and WC Docket 17-97, Eighth Further Notice of Proposed Rulemaking in CG Docket 17-59, and Third Notice of Inquiry in CG Docket 17-59, 38 FCC Rcd 5404 (2023), SouthLight provides the following information concerning its upstream voice service carrier.

SouthLight has one upstream provider from which it receives voice traffic:

Vail Systems, Inc.
570 Lake Cook Road, Suite 400
Deerfield IL 60015
Todd Whitley
todd@vailsys.com

SouthLight has a master service agreement with its upstream provider and has received assurances in writing from its officials that it has, and will continue to, sign calls transmitted to SouthLight and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to SouthLight. SouthLight and its upstream provider have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Acceptable Use Policy ("AUP")

SouthLight maintains an AUP that subscribers must sign before being permitted to use SouthLight's network. Among other things, the AUP prohibits:

- providing altered, deceptive, or false information about the identity of the sender or the origin of a message or phone call;
- violating any applicable local, state, or federal law;
- violating applicable industry accepted guidelines; and
- using SouthLight's service to engage in or in connection with fraudulent activities.

SouthLight's contractual terms with subscribers specify that SouthLight may take action up to suspension or termination of service for violation of the AUP.

Continuous Traffic Monitoring & Threat Mitigation

When traffic analysis indicates the presence of likely illegal robocalling, SouthLight works with its upstream provider to follow defined procedures on investigating such subscribers.

SouthLight's upstream provider's fraud mitigation platform analyzes call patterns, dialing cadence, Caller ID usage, and traffic volume against known robocall signatures and behavioral thresholds. When anomalous activity is detected, an automated alert is generated and immediately routed to SouthLight's Network Operations and Compliance teams for review.

Because SouthLight does not have the infrastructure to implement STIR/SHAKEN, no third-party vendors are involved in its analytics.

Immediate Containment

Upon receipt of a suspicious activity alert, SouthLight initiates containment protocols without delay. The identified bad actor is disabled within 15 minutes of alert, halting the propagation of potentially illegal traffic and limiting downstream harm to called parties and the broader network. Service suspension remains in effect for the duration of the investigation.

Internal Investigation

Following containment, SouthLight conducts a structured internal investigation that includes:

- Traffic log analysis to identify the origin, scope, duration, and volume of the suspicious activity
- Review of the customer's account history, onboarding documentation, and prior compliance record
- Correlation of flagged traffic against known illegal robocall campaigns, STIR/SHAKEN attestation failures, and Do-Not-Call registry violations
- Assessment of whether the activity reflects intentional misuse, compromised credentials, or misconfigured systems
- Regulatory Reporting & Escalation
- Where investigation findings indicate potentially illegal robocall activity, SouthLight follows established escalation protocols that include:
- Reporting to the FCC as required under the Industry Traceback Group (ITG) framework and applicable TRACED Act obligations

- Cooperation with USTelecom's Robocall Traceback Consortium and law enforcement upon request
- Filing Suspicious Activity Reports (SARs) where financial fraud indicators are present
- Notifying downstream carriers and partners who may have been impacted by the traffic

Customer Notification & Remediation

The implicated customer is formally notified of the investigation findings, including a detailed summary of the flagged activity. Customers who demonstrate inadvertent violations are required to implement corrective measures and acknowledge updated acceptable use terms before service is reinstated. Customers found to have engaged in willful illegal robocall activity are permanently terminated and reported to the appropriate regulatory bodies.

Post-Incident Review

SouthLight conducts a post-incident review following every confirmed suspicious activity event to evaluate the effectiveness of detection thresholds, response timelines, and mitigation protocols. Findings are used to continuously improve our monitoring infrastructure and update our KYC and acceptable use frameworks accordingly.

DNO Request Intake & Acknowledgment

SouthLight Services is fully committed to honoring Do Not Originate ("DNO") requests received from the Industry Traceback Group ("ITG") and maintaining compliance with all applicable robocall mitigation obligations under the TRACED Act and FCC regulations.

SouthLight has established a dedicated compliance intake process for receiving and logging DNO requests from the ITG. Upon receipt of a DNO request, our Compliance team acknowledges the request promptly and initiates the blocking protocol without delay. All DNO requests are logged with timestamp, originating source, and action taken to maintain a complete and auditable compliance record.

Blocking & Mitigation Protocols

Once a DNO request is received and validated, SouthLight implements blocking of the identified number(s) at the network level. This action is executed swiftly, consistent with our broader commitment to disabling bad actors within 15 minutes of alert. Blocking is applied across all relevant network entry points to ensure the DNO number cannot be used to originate traffic on our platform.

Ongoing DNO List Management

SouthLight maintains an active and continuously updated DNO list that is integrated into our fraud mitigation partner platform. This ensures that numbers identified as Do Not Originate are systematically blocked from traffic origination in an automated fashion — reducing reliance on manual intervention and eliminating gaps in enforcement. The list is reviewed and reconciled on a regular basis to reflect the most current ITG guidance.

Customer Notification & Enforcement

When a DNO request impacts an active customer account, SouthLight notifies the customer of the restriction and the basis for the block. Customers are informed that DNO compliance is a non-negotiable network obligation and that any attempt to circumvent a DNO block constitutes a

material violation of their service agreement. Repeated or willful violations result in immediate account termination and referral to the appropriate regulatory authorities.

Cooperation with the ITG & Regulatory Bodies

SouthLight maintains an open and cooperative relationship with the Industry Traceback Group and responds to all traceback inquiries within the timeframes prescribed by the ITG's established protocols. Our team participates in traceback investigations as required, providing call detail records and supporting documentation to assist in identifying the upstream source of illegal traffic. SouthLight views ITG cooperation not merely as a compliance obligation, but as an active contribution to the industry-wide effort to eliminate illegal robocall activity.

SouthLight follows ITG-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, SouthLight will devote sufficient resources to provide prompt and complete resources to traceback requests. SouthLight commits to respond within 24 hours to all traceback requests from the FCC, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

Robocall Mitigation Database Filing

SouthLight's robocall mitigation program, inclusive of our DNO response procedures, is documented and filed with the FCC's Robocall Mitigation Database, affirming our commitment to network integrity and consumer protection in accordance with federal requirements.

This plan, along with industry best practices, will evolve to response to the dynamic nature of mitigating illegal robocalling. SouthLight will monitor industry best practices and continuously improve our internal processes to ensure this plan, and our system adapts to this ever-changing issue.

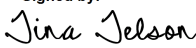
In the event of any material change to this plan, SouthLight will republish it to employees, consultants and contractors and file such an update to the FCC Robocall Mitigation Database within ten (10) days of such update.

Certification of Tina Telson

I, Tina Telson, CEO of SouthLight Services, LLC ("SouthLight"), do hereby certify, under penalty of perjury, the following:

- (1) SouthLight does not have access to the necessary infrastructure to implement STIR/SHAKEN, and therefore has not implemented STIR/SHAKEN in the IP portions of its network.
- (2) SouthLight 's Business name and primary address are as follows:

SouthLight Services, LLC
3300 South Parker Road
Suite 325
Aurora, CO 80014
- (3) SouthLight has no other business names in use
- (4) SouthLight has not previously used any other business name.
- (5) SouthLight has the following owners/principals: Tina Telson and Ash Somo. Neither of them had any licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding.
- (6) SouthLight has no subsidiaries, affiliates, or parent companies.
- (7) The name, title, department, business address, telephone number, and email address of the individual responsible for addressing robocall-related issues are listed in the above robocall mitigation plan.
- (8) SouthLight's role in the call chain is that of a voice service provider without a STIR/SHAKEN obligation.
- (9) SouthLight has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (10) SouthLight is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- (11) SouthLight is not required to have, and does not have an operating company number.

Signed by:

EB146BF3E0384E6...

Tina Telson

April 7, 2026