

LineShield Robocall Mitigation Plan

Filed pursuant to 47 CFR § 64.6305 and the FCC Robocall Mitigation Database requirements

I. Introduction and Purpose

This document sets forth the current policies and procedures of **the iDudes, LLC**, d/b/a LineShield ("the Provider"), a voice service provider offering caller reputation, call authentication support, and number-monitoring services to independent and captive property & casualty (P&C) insurance agencies operating in the United States. These policies are designed to reduce or eliminate the origination of illegal robocall traffic on the Provider's network. The Provider views the practices described below as constituting the "reasonable steps" required under 47 CFR § 64.6305(a)(2) to avoid originating illegal robocalls, and commits to the traceback cooperation obligations described in Section VI below.

II. STIR/SHAKEN Implementation Status

The Provider does not have a STIR/SHAKEN implementation obligation. The Provider is a non-facilities-based reseller of voice service and does not own, control, or operate the network infrastructure necessary to authenticate calls under the STIR/SHAKEN framework, consistent with the exemption described in 47 CFR § 64.6305(d)(2)(i). All calls placed through the Provider's platform originate on the network of the Provider's underlying voice services provider, Twilio Inc. ("Twilio"), which independently holds its own STIR/SHAKEN authentication obligations and signs calls originated on its network with its own certificate as the originating provider of record.

III. Know-Your-Customer (KYC) Procedures

The Provider extends outbound calling capability only to business customers that have completed the Provider's onboarding process, which includes:

- Verification of the customer's legal business name, business address, and, where applicable, insurance producer license number or agency identifier;
- Collection of a named point of contact at the customer organization responsible for that customer's outbound calling activity;
- Review of the intended use case for outbound calling to confirm it is consistent with legitimate insurance sales, service, and retention activity, and specifically inconsistent with illegal robocalling, unlawful prerecorded-voice calling, or caller ID spoofing;
- Execution of a customer agreement that prohibits the origination of unlawful robocalls, prerecorded-voice calls placed without required consent, spoofed or falsified caller identification, and any calling activity that would violate the Telephone Consumer Protection Act (TCPA) or the Commission's rules, and that sets out suspension and termination as consequences for violation;
- Maintenance of number authorization records identifying which telephone numbers are authorized for use by which customer, so that any number's calling activity can be traced back to a specific, vetted customer; and
- Periodic review of each customer's standing at renewal, including re-confirmation of business identity and continued consistency between represented use case and observed calling activity.

IV. Know-Your-Upstream-Provider Procedures

The Provider's sole upstream voice services provider is Twilio. Before routing customer traffic through Twilio, and on an ongoing basis, the Provider confirms that Twilio:

- Is listed as an active filer in the Commission's Robocall Mitigation Database;

- Holds its own STIR/SHAKEN implementation and signs outbound calls under its own certificate as the originating network provider;
- Maintains its own know-your-customer and robocall mitigation obligations as a Commission-regulated voice service provider; and
- Provides caller-reputation monitoring and remediation tooling and per-call STIR/SHAKEN attestation-level visibility that the Provider uses directly as part of its own monitoring practices described in Section V.

The Provider reviews Twilio’s Robocall Mitigation Database filing status periodically and will suspend traffic or transition to an alternative upstream provider in the event Twilio’s filing lapses or is removed from the Database.

V. Affirmative, Effective Measures to Prevent Illegal Robocalls

Consistent with its obligation under 47 CFR § 64.6305(a) to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls, the Provider uses the following call analytics system: Twilio Voice Integrity (carrier reputation monitoring and remediation) together with Twilio Lookup (per-number and per-call risk signals), both provided by the Provider’s upstream provider, Twilio Inc. Using this system, the Provider:

- Monitors outbound call volume, pacing, and duration patterns on a per-number and per-customer basis to detect calling behavior inconsistent with legitimate agency outreach, including abnormally high call volume per line, minimal call duration, or rapid sequential dialing;
- Monitors carrier-reported reputation status across major U.S. carrier analytics platforms via Twilio Voice Integrity and investigates any number that receives a “Spam Likely” or comparable label;
- Reviews inbound complaint and opt-out requests received on behalf of customers and escalates repeat or substantiated complaints for customer-level review;
- Reserves the right to suspend or terminate service to any customer found to be originating illegal robocall traffic, spoofed caller identification, or calling activity inconsistent with the customer’s represented use case; and
- Maintains records of customer onboarding, monitoring activity, and any suspension or termination actions for not less than 2 years from the date of the relevant event, available to the Commission upon request.

VI. Traceback Cooperation Commitment

The Provider commits to responding within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium (currently the USTelecom Industry Traceback Group), and to cooperate with such entities in investigating and stopping any illegal robocallers that use the Provider’s service to originate calls.

VII. Enforcement Against Violating Customers

Where the Provider identifies, or is notified of, a customer originating illegal robocall traffic, the Provider will:

- Promptly investigate the reported activity;
- Suspend the customer’s outbound calling capability pending investigation where the activity presents an ongoing risk; and
- Terminate service to any customer confirmed to have originated illegal robocall traffic in violation of its customer agreement.

VIII. Point of Contact

Questions regarding this robocall mitigation plan, or reports of suspected illegal robocall traffic originating from the Provider's service, may be directed to:

Lannie Sullivan
Director of Operations
LineShield

lannie@theidudes.com
5102 E Pima St Ste 100
Tucson, AZ 85712

IX. Certification

This robocall mitigation plan is submitted in connection with the Provider's certification in the Commission's Robocall Mitigation Database pursuant to 47 CFR § 64.6305. The Provider certifies that the information contained in this document is accurate as of the date of filing and commits to updating this filing within 10 business days of any material change.

Date: **08/09/2026**