



Robocall Mitigation Plan

Radiant Solution Providers Effective Date: May 20, 2026

Know Your Customer

We have established and follow written Know Your Customer (KYC) procedures prior to activating service for any customer. Our KYC program includes the following steps:

- **Customer Identity Verification:** Prior to activating service, each prospective customer must complete our written Know Your Customer (KYC) questionnaire. The form collects: (A) company legal name, DBA/trade names, holding company, primary contact name/number/email, business type (wholesale, retail, call center, etc.), service type requested (VoIP termination, hosted PBX, SIP trunking, UCaaS, CCaaS, contact center, predictive dialer, etc.), website URL, state of incorporation, and Federal Tax ID; (B) main and toll-free telephone numbers, headquarters physical address, billing address, and registered-agent status; (C) all officers, owners, and principals including name, title, ownership percentage, phone/email, citizenship, and whether more than 20% of the company is controlled by a non-US citizen or entity, plus social media profiles (LinkedIn, Twitter, Facebook); and (D) disclosure of any prior lawsuits or law enforcement actions against the customer or any controlling person, the intended business use case for the interconnection, and anticipated call traffic KPIs (ASR%, ALOC/ACD, CPS, MOU). The questionnaire is signed and dated by an authorized representative before service is provisioned.
- **Telephone Number Authorization:** We confirm that each customer is the authorized subscriber or user of the telephone numbers they intend to use on our network. For numbers ported in, we validate the port authorization. For numbers assigned from our inventory, we document the assignment.
- **Fraud Screening:** We actively monitor customer call activity after activation for indicators of illegal robocalling. This includes ongoing review of call volume trends, answer-seizure ratios, average call duration, and calls-per-second rates against the KPIs disclosed at onboarding. We monitor inbound complaints and industry robocall-complaint databases for reports tied to numbers or customers on our network. Where call volume is elevated or complaint activity is detected, we may require the customer to provide a written explanation of the traffic. In cases where the legitimacy of high call volume cannot be confirmed through records alone — for example, distinguishing lawful predictive-dialer traffic from illegal robocall campaigns — we reserve the right to inspect the customer's PBX or dialing platform configuration to verify that the traffic



profile is consistent with the stated use case. Customers who cannot or will not cooperate with an inspection request may have service suspended pending resolution.

- **Use-Case Review:** We require customers to disclose their intended calling purpose. Customers who intend to conduct any form of outbound calling campaigns must attest in writing to compliance with the TCPA, TSR, and all applicable federal and state telemarketing laws.
- **Ongoing Monitoring:** We periodically review existing customer accounts for changes in call volume, call patterns, or complaint activity that may indicate fraudulent or illegal robocalling, and take appropriate action including suspension or termination of service.
- **Record Retention:** We retain all subscriber onboarding documentation and KYC records for a minimum of 2 years and make them available to the FCC, law enforcement, or the registered traceback consortium upon request.

Traceback

We respond to all traceback requests from the Commission, law enforcement, and the registered traceback consortium within 24 hours of receipt, and cooperate fully with such entities in investigating and stopping any illegal robocallers that use our service to originate calls. We maintain sufficient call detail records to support traceback investigations for a minimum of 18 months.

STIR/SHAKEN Compliance

We have fully implemented STIR/SHAKEN call authentication on our network in compliance with 47 CFR § 64.6300 et seq. and the FCC's rules implementing the TRACED Act (2019). No extension or exemption is claimed. Specifically:

- **Digital Signing:** All IP calls originated on our network are digitally signed using SHAKEN attestation in accordance with ATIS-1000074 and RFC 8224/8225.
- **Attestation Levels:** We apply Full Attestation ('A') for calls where we have authenticated the calling party and confirmed they are authorized to use the number; Partial Attestation ('B') where we have authenticated the customer but cannot confirm number authorization; and Gateway Attestation ('C') for calls received from outside our network where the originating carrier cannot be identified.
- **Service Provider Code (SPC) Token:** We have obtained a valid SPC token from the Policy Administrator (PA) and are registered in the FCC's Robocall Mitigation Database.
- **Certificate Authority:** We use a SHAKEN-approved Certificate Authority (CA) to obtain SHAKEN certificates used for signing.
- **Verification:** We verify STIR/SHAKEN signatures on all calls received over IP interconnections and pass PASSporT information downstream where technically feasible.



Robocall Mitigation Program

In addition to full STIR/SHAKEN implementation, we employ the following real-time and proactive measures to prevent the origination of illegal robocalls on our network:

- **Fraud Detection:** Continuous monitoring for high-volume robocalling, caller ID spoofing, and spam call activity using behavioral analytics.
- **Subscriber Notification:** Caller ID Name override to warn downstream subscribers of suspicious or flagged calls.
- **Call Blocking:** Accurate call identification enabling blocking of fraudulent calls in accordance with the TRACED Act (2019).
- **Business Number Verification:** Registration of legitimate business numbers to prevent unintentional blocking of lawful traffic.
- **Caller ID Name Service:** Integration of CNAM lookup with robocall mitigation, preserving the original Caller ID even when a call is flagged as potentially fraudulent.

Call Abuse Policy

We have implemented a Call Abuse Policy published on our website, incorporated into our terms of use, and communicated to all customers:

"Any call originated on the Radiant Solution Providers network is subject to inspection and investigation if the call is suspected of being fraudulent, abusive, or illegal. Calls meeting any of these criteria will be blocked. If these conditions are repeated or become excessive, the subscriber may be disconnected from the Radiant Solution Providers network, may be subject to further investigation by the FCC for enforcement of the TRACED Act, and may be subject to fines and penalties imposed by the FCC or a jurisdictional court."

FCC Robocall Mitigation Database Registration

This Robocall Mitigation Plan is filed with the FCC's Robocall Mitigation Database as required by 47 CFR § 64.6305. We will update this filing within 10 business days of any material change to our robocall mitigation practices, STIR/SHAKEN implementation status, or contact information, as required by FCC rules.