

ROBOCALL MITIGATION PLAN - Updated July 2026

BUSINESS INFORMATION

ISUNET LLC
618 Douglas Avenue
Ames, IA 50010

CONTACT INFORMATION

Timothy Payton 515.233.4777
admin@opencom.net

OVERVIEW:

The FCC requires that all voice service providers (“VSPs”) certify in the Robocall Mitigation Database that they have implemented a Robocall Mitigation Plan (“RMP”) to ensure that they are not originating illegal robocalls.

The FCC requires that VSPs develop an RMP that:

- details the reasonable steps taken to avoid originating illegal robocalls;
- demonstrates a commitment to respond to traceback requests to cooperate with investigators and stopping illegal robocalls; and
- is filed in the Robocall Mitigation Database.

The FCC states that a 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.

PURPOSE:

ISUNET LLC (“ISUNET”) is dedicated to stopping illegal calls that may originate in our network and monitoring the calls coming into our network. This document delineates ISUNET’s RMP.

STIR/SHAKEN STATUS:

ISUNET certifies that it has implemented Complete STIR/SHAKEN caller ID authentication for calls it originates on its IP network, consistent with 47 CFR § 64.6301(a).

ISUNET uses third-party providers to support its STIR/SHAKEN implementation. ISUNET utilizes Telonium for hosted STIR/SHAKEN signing services. Attestation levels are assigned based on the ISUNET’s verification of the caller and calling rights, consistent with applicable FCC STIR/SHAKEN guidance.

KNOW YOUR CUSTOMER (“KYC”):

GENERAL POLICY: ISUNET provides VoIP services only to customers located in the continental United States. We do not provide services to any marketing companies, outbound marketing calls, or customers whose business model involves high-volume outbound marketing calls. We also do not allow the resale of our services. We have a direct relationship with all of our customers, whether business or residential, and require customer identity

and service use-case information before provisioning voice services.

INFORMATION WE COLLECT AND VERIFY:

Before any voice service is provisioned or an active telephone number is assigned, we collect and verify core customer information, which may include:

1. Legal Name of the individual or entity.
2. Physical Service Address (P.O. Boxes are strictly prohibited as primary addresses).
3. Government-Issued Tax or Identification Number.
4. Alternate Telephone Number and verified secondary contact method such as email address.

For residential customers, we verify identity and service location before shipping equipment or activating services. This may include customer's full legal name, physical billing/service address, Date of Birth, or SSN. Additionally, we have a phone conversation with every customer prior to shipping hardware to the verified physical address associated with the customers' account.

For business customers, we collect additional information, including the legal business name, EIN, state of formation, physical business address, prior telephone billing records when available, expected service use, authorized contact information, and the IP address or addresses from which SIP traffic will originate. We may also review state business records or other documentation to confirm that the business is active and in good standing.

USE-CASE REVIEW AND RISK ASSESSMENTS:

We review each customer's stated use-case (e.g., personal residential use, customer support, telemarketing, education, political campaigns) prior to service activation. We do not provision service for customers intending to use the service for unlawful robocalling, spoofing, lead-generation scams, or unauthorized outbound marketing. We also verify the customer's right to use telephone numbers assigned to or ported by the customer to support appropriate STIR/SHAKEN attestation.

DATA RETENTION:

We retain KYC records, verification materials, and related account information for four (4) years after the customer relationship ends. We may review or update customer information if account activity, traffic patterns, traceback activity, or other risk indicators suggest that additional verification is needed.

ONGOING MONITORING OF CURRENT ACTIVE CUSTOMERS:

All current customers are subject to channel limitations that restrict the number of active phone calls they may maintain at any one time. ISUNET actively monitors customer traffic for patterns or changes that may indicate fraud, abuse, unauthorized use, or other violations of applicable service requirements.

ISUNET utilizes Sangoma's fraud-prevention systems to analyze network traffic, identify abnormal activity, issue urgent SMS and email alerts, and automatically block or stop suspicious traffic when appropriate. Monitored indicators include, but are not limited to, sudden volume spikes, asymmetric call volume, inconsistent IP address geography, PBX hacking indicators, and potential international toll-fraud activity.

When suspicious traffic is detected, ISUNET may immediately suspend or restrict service while the activity is

reviewed. Access is not restored until the customer completes a re-verification process and ISUNET determines that continued service does not present an unacceptable risk.

When traffic analysis indicates likely illegal robocalling activity, ISUNET follows established investigation procedures. These procedures include, but are not limited to:

- reviewing recent and historical call detail records and comparing them against expected traffic patterns;
- reviewing recent and historical account activity, purchases, and service changes;
- determining whether any system issue may have generated or contributed to the unusual traffic;
- verifying that the call-originating path is valid and authorized; and
- contacting the subscriber to understand the subscriber's use case and confirm that the activity is authorized and consistent with the subscriber's stated business purpose.

ISUNET may maintain service restrictions, suspend service, or take other appropriate mitigation measures until the investigation is complete and the subscriber's traffic has been validated.

KNOW YOUR UPSTREAM PROVIDER ("KYUP"):

ISUNET does not accept third-party traffic for transit. Outbound calls originate only from ISUNET's end users, and inbound calls are received from its upstream carrier(s) for delivery to those end users.

We coordinate with our upstream carrier(s) on suspected illegal traffic, blocking or enforcement issues, and applicable traceback requests.

PRIOR INVESTIGATIONS:

ISUNET discloses that, within the prior two years, we were subject to a formal FCC action relating to deficiencies in our Robocall Mitigation Database certification and robocall mitigation plan.

AGENCIES INVOLVED: This matter involved the FCC's Wireline Competition Bureau and Enforcement Bureau.

DATE COMMENCED: The matter began with the March 29, 2024 notice from the FCC's Robocall Mitigation Database Team, which stated that our RMD certification and robocall mitigation plan needed to be updated. The notice gave us until April 29, 2024 to correct the issue.

The matter proceeded under FCC File No. EB-TCD-24-00036891. On December 10, 2024, the Enforcement Bureau issued a Show Cause Order, DA 24-1235, directing us to either cure the deficiencies or explain why our certification should not be removed from the RMD. The matter was later assigned File No. EB-TCD-25-00038590.

SUMMARY OF FINDINGS: The FCC found that our RMD certification and robocall mitigation plan were incomplete because they had not been updated with the information required by the February 26, 2024 deadline. The FCC also found that we did not timely correct the issue or provide a sufficient explanation after the Show Cause Order.

The findings were limited to our RMD filing and mitigation-plan compliance. The FCC orders did not find that we originated illegal robocalls, engaged in spoofing, or transmitted unlawful traffic.

FINAL DETERMINATION: The FCC's final determination was issued in DA 25-737 on August 25, 2025. The Enforcement Bureau removed our certification from the RMD and stated that we could not refile unless both the Wireline Competition Bureau and Enforcement Bureau consented.

CURRENT STATUS: The Enforcement Bureau provisionally reinstated our RMD filing on September 5, 2025. The provisional reinstatement noted that FCC staff could request additional changes and that provisional reinstatement was not a final determination of compliance.

After we updated our filing and robocall mitigation plan to address the identified deficiencies, Commission staff reviewed the updates and notified us by email on July 13, 2026 that our status had been converted from provisional reinstatement to full reinstatement. Our current filing reflects our present robocall mitigation practices and STIR/SHAKEN implementation status.

TRACEBACK NOTIFICATIONS:

We respond to all traceback requests from the Commission, law enforcement, and the registered traceback consortium and cooperate with such entities in investigating and stopping any illegal robocallers that use our service to originate calls. To allow for timely and comprehensive responses, ISUNET will devote sufficient resources to provide prompt and complete resources within 24 hours to any traceback requests. Receiving a Traceback Request from the ITG (Industry Traceback Group) will trigger an immediate audit of the customer's traffic.

PLAN UPDATES:

This plan and industry best practices must evolve to respond to the dynamic nature of mitigating illegal robocalling. ISUNET will monitor industry best practices and continuously improve our internal processes to ensure this plan and our system adapt to this ever-changing issue.

In the event of any material change to this plan, ISUNET 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.