

Robocall Mitigation Plan for TrueSIP USA LLC

Effective Date: June 7, 2025

1. Introduction and Purpose

TrueSIP USA LLC ("TrueSIP" or "the Company") is fully committed to combating the proliferation of illegal robocalls and protecting American consumers from fraudulent, unsolicited, and illegal communications. This Robocall Mitigation Plan outlines the specific policies, procedures, and technical frameworks TrueSIP has implemented to prevent the origination, carriage, and termination of illegal robocalls on its network, in accordance with the rules and regulations set forth by the Federal Communications Commission (FCC).

This plan is publicly available and has been filed with the FCC's Robocall Mitigation Database.

2. STIR/SHAKEN Implementation

TrueSIP has implemented the STIR/SHAKEN (Secure Telephone Identity Revisited / Signature-based Handling of Asserted information using toKENs) framework to its IP-based network infrastructure.

- **Authentication Service:** All originating calls from our network are authenticated using STIR/SHAKEN protocols. We sign outbound calls with the highest level of attestation ("A" - Full Attestation) for which we can verify the caller's identity and right to use the associated telephone number.
- **Verification Service:** All inbound IP-based calls are subject to verification. The STIR/SHAKEN information is used to inform our call routing and analytics programs.
- **Attestation Levels:** We have implemented strict policies to assign the appropriate attestation level based on our relationship with the caller and our confidence in the authenticity of the caller ID. We will assign "B" (Partial) or "C" (Gateway) attestations when the conditions for "A" are not met.

3. Robocall Mitigation Program

TrueSIP employs a robust mitigation program based on reasonable analytics to detect and prevent illegal robocalls. This program is dynamic and is continuously updated to adapt to evolving threats.

A. Analytics and Monitoring:

- We utilize a combination of internal and third-party analytics tools to monitor traffic patterns in real-time.
- The system analyzes call metadata to identify suspicious activities, including, but not limited to:
 - Unusually high call volumes or short-duration calls from a single source.
 - Calls originating from invalid, unallocated, or DNO (Do-Not-Originate) numbers.

- Sequential dialing patterns.
 - Repetitive calling to the same numbers.
- We subscribe to industry-generated lists of known and suspected illegal robocalling numbers.

B. Blocking of Illegal Traffic:

- Upon detection of traffic that is highly likely to be illegal, TrueSIP will immediately block the calls from traversing our network.
- Blocking is based on reasonable analytics and is applied in a non-discriminatory manner.
- A process is in place for legitimate callers to report and resolve any erroneous blocks.

4. "Know Your Customer" (KYC) Policies

To prevent the origination of illegal robocalls from our platform, TrueSIP has instituted a stringent KYC policy for all new and existing customers.

- **Customer Vetting:** All new customers are required to provide verifiable business information, including legal business name, physical address, and contact details.
- **Use Case Verification:** We require customers to declare their intended use of our services. High-risk use cases, such as telemarketing, require additional scrutiny and validation of compliance with the Telephone Consumer Protection Act (TCPA).
- **Ongoing Monitoring:** We reserve the right to periodically review customer accounts and traffic to ensure continued compliance with our acceptable use policies and this mitigation plan.

5. Traceback Cooperation

TrueSIP is committed to full and timely cooperation with industry traceback efforts and law enforcement investigations.

- **Designated Contact:** We have a designated point of contact for all traceback requests from the FCC, law enforcement, and the official industry traceback consortium.
- **Response Protocol:** We will respond to all traceback requests within 24 hours of receipt.
- **Investigation and Mitigation:** Upon receiving a traceback request, we will promptly investigate the identified traffic. If the traffic is determined to be illegal, we will take immediate action, which may include suspending or terminating the responsible customer's service, in addition to cooperating with the requesting entity.

6. Contact for Robocall Mitigation Inquiries

For any questions, concerns, or official requests related to this Robocall Mitigation Plan, please contact:

Robocall Mitigation Compliance Office

- **Email:** noc@truesip.net
- **Phone:** (505) 376-1293

7. Certification

I, Jahvoy Gordon, hereby certify that I am an officer of TrueSIP USA LLC, authorized to make this certification. I certify that the company has implemented and is committed to upholding the robocall mitigation plan described herein. I further certify that all statements in this plan are true, complete, and correct to the best of my knowledge.