

Telasip robocall mitigation plan

Overall robocall mitigation is achieved using a very simple three step plan. This plan is implemented and enforced as part of our onboarding process, and Acceptable Use Policy. Because of the challenges with enforcing telemarketing do-not-call lists and illegal robocall blocking, we instead choose not to offer services to either group.

Illegal robocalling can easily be identified using traffic analysis. The traffic pattern is easily identifiable by very low average call durations, 12 seconds or less, and very low answer ratios. This pattern is also observed with telemarketing activities. Because it is nearly impossible to distinguish between the two without recording and listening to calls, we choose to deny services to both parties.

Our processes involve the following steps:

STEP 1 - Know Your Customer

We only do business with customers based in the United States. We verify the business identity as part of the onboarding process. We ensure the business understands that we do not accept telemarketing/call center activities. As part of the onboarding process, we explain the expectations for traffic patterns, and it is against our acceptable use policy to engage in these activities. We make it very clear that we reserve the right to block outbound traffic if the policy is abused.

We follow the best practices for vetting caller identity described by the NANC Call Authentication Trust Anchor Working Group. (<https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>)

Step 2: Traffic Analysis

Our traffic analysis is looking for very low call durations, and the low volume of answered calls. These are clear signs of unwanted calls and robocall telemarketing.

We use software provided by our underlying vendor to monitor our outbound voice traffic in real time to prevent the origination of illegal robocalls. Combining behavioral analytics, caller authentication and verification, our solution features:

Fraud Detection: Detection of high volume robocalling, spoofing and spam call activity.

Subscriber Notification: Caller ID Name override to warn subscribers of suspicious calls.

Call Blocking Support: Accurate identification enabling you to block fraudulent phone calls as per the TRACED Act (2019)

Business Number Verification: Register legitimate business numbers to prevent unintentional call blocking.

Caller ID Name Service: Easy integration of Caller ID name lookup service, including robocall mitigation with override to include original caller ID even when call is determined fraudulent.

Step 3: Enforcement

We take our Acceptable Use Policy very seriously and have zero tolerance. We quickly identify the offending subscriber and notify them of the violation. We then block the outgoing traffic. We then work with the customer to determine if the issue was a result of a hack, or if they were in fact violating our policy. If they are in violation, then we block them from placing outbound traffic.

We have implemented a Call Abuse Policy and have published the following policy to our web site, terms of use, and have notified our customers of the policy as copied below:

“Any call originated on the Telasip 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, becoming excessive, the subscriber may be disconnected from the Telasip network, may be subject to further investigation by the FCC for enforcement of the TRACED Act and the subscriber may be subject to fines and penalties imposed by the FCC or the jurisdictional court.”

By not waiting for complaints or enforcement actions, we have been able to effectively manage our network and manage customer expectations. If by chance we have received a complaint respond very quickly, and proactively to maintain the integrity of the network.

Having said that above, 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.

STIR/SHAKEN Extensions

We are eligible for and are taking STIR/SHAKEN implementation extension received under 47 CFR § 64.6304 because we have fewer than 100,000 voice subscriber lines. All the voice traffic that originates on our network is subject to the robocall mitigation program described below.