



STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN (RMP)

Pursuant to 47 CFR § 64.6304, TOSKR Inc. d/b/a GetThru ("GETTHRU") submits this report on its plan to prevent and mitigate illegal robocalls. This report describes the status of its implementation of STIR/SHAKEN and the practices and procedures GETTHRU has in place to mitigate illegal robocalls as of September 19th, 2024.

Who We are and What We do

GETTHRU operates peer to peer communication tools designed for political candidate organizations and non-profit entities so that those entities may perform SMS or MMS texting and voice calling as clients of GETTHRU at a modern scale with modern connectivity tools. Most GETTHRU clients are vetted as political candidate organizations or non-profit entities who are exempt from the Telemarketing Sales Rule as established by the Federal Trade Commission. Any for-profit clients are prohibited from using our services for the purposes of Telemarketing.

Our voice calling tool, THRUTALK, requires a human being connected to GETTHRU as a registered user of GETTHRU. These human beings perform the work of voice connection via a non-automated modern dialer system that is compliant with the 19-511 *Facebook, Inc. v. Duguid* Supreme Court Ruling of 04/01/2021 because that non-automated modern dialer system does not have the capacity "to store or produce telephone numbers to be called, using a random or sequential number generator," and to dial those numbers.

GETTHRU builds, maintains, and operates its software as systems of interactions via Application Programming Interface ("API") with major voice service providers, currently Twilio and Bandwidth as of September 19, 2024.

How GETTHRU prevents illegal calls

GETTHRU vets all our clients for legitimate uses and accepts only qualified legitimate applicants. We ensure their proper use of our systems through direct training, informational materials, and contractual requirements.

How GETTHRU manages "Know-Your-Upstream Providers"

GETTHRU has no upstream providers. All calls beginning with us are initiated via our vetted clients.

How GETTHRU uses call analytics systems to identify and block illegal traffic

GETTHRU monitors our call termination distribution for deviances from historical patterns of legitimate

usage. If we identify calling patterns that suggest illegitimate uses, we further analyze client data and, when necessary, suspend clients by canceling their account and preventing them from creating new accounts.

How GETTHRU manages contractual obligations for end-users

GETTHRU requires all clients to sign contracts stating that they will adhere to all applicable laws.

The language in our contracts is as follows:

“Customer represents, covenants, and warrants that Customer will not use the Services in any way that (i) is illegal; (ii) disrupts or damages any of Toskr’s computer systems or network or other Parties’ computer systems and networks, or (iii) violates any person’s rights (including without limitation intellectual property, privacy, publicity, and/or statutory rights). Prohibited uses of Toskr Services include communications that are obscene, libelous, defamatory, fraudulent, discriminatory, or abusive; communications that are unsuitable for minors; communications that promote, incite, or instruct on criminal behavior; communications that are false, misleading, or deceptive; communications that infringe on the intellectual property or privacy rights of third parties; and otherwise unlawful communications.”

Status of Implementation

GETTHRU does not own, operate, or manage the equipment required for STIR/SHAKEN implementation.

GETTHRU connects with the telephone network via major voice service providers who are fully STIR/SHAKEN compliant to originate, maintain, and terminate voice call traffic. As GETTHRU cannot implement full STIR/SHAKEN attestation required by 47 CFR § 64.6301 without owning and operating SIP trunks, GETTHRU elects to instead file a ROBOCALL MITIGATION PLAN certification of Option 3: No STIR/SHAKEN implementation.

Robocall Mitigation Plan

This Robocall Mitigation Plan covers the specific methods that GETTHRU has implemented to detect and prevent illegal robocalls on its network as of September 19th, 2024. GETTHRU will mitigate illegal robocalls via Application Design, Application Performance Monitoring (“APM”), and Client Vetting.

Specific Methods for Identifying and Preventing Illegal Robocalls

Application Design:

GETTHRU performs mitigation via Application Design by:

- Initiating, maintaining, and terminating all outbound traffic via major voice service providers with full STIR/SHAKEN implementation; as of September 19th, 2024 those major voice service providers are Twilio and Bandwidth
- Requiring all Client users and End users to be registered users of GETTHRU via email validation
- Requiring all Client users and End users to be registered with unique phone numbers belonging to said user
- Requiring all End users to be invited to create accounts with GETTHRU via Clients of GETTHRU
- Requiring all Client users to provide their own lists of Contacts to be called
- Requiring all End users who connect to the application for purposes of being connected to Contacts to be called do so by logging into the GETTHRU system and selecting the End user's choice of webRTC or PSTN connection for those connected calls
- Enforcing a 15-minute idle user period for End users in GETTHRU's application where the End user is removed from active connections to Contacts if the End user is idle for greater than 15 minutes
- Enforcing that each interaction with a Contact requires human selection of answers to questions to complete each connected call to a Contact
- Enforcing that each interaction with a Contact requires human confirmation of readiness to initiate further calls to more contacts after each connected call to a Contact
- Enforcing that the number of attempts to Contacts made per End user present to receive connections will be maintained and monitored by Staff members
- Offering no method for clients or end users to provide recorded audio to be played repeatedly during connected calls or left as voicemails

Application Performance Monitoring:

GETTHRU performs mitigation via APM by:

- Programmatic collection of key metrics in number of dials attempted, number of calls connected, number of end users connected, duration of connected calls, and average wait time for end users between connected calls
- Storage of key metrics for number of dials attempted, number of calls connected, number of end users connected, duration of connected calls, and average wait time for end users between connected calls
- System alerts for anomalous performance of key metrics

- Staff monitored alerts for real-time performance

Client Vetting:

GETTHRU performs Client Vetting by:

- Human verification of the desired purpose for each client's activity with GETTHRU
- Human verification of the nature of the organization requesting GETTHRU's services to confirm each Client represents a political candidate organization, non-profit entity, or qualifies as a for-profit entity with a use case that excludes all telemarketing activity

Responding to Traceback Requests:

GETTHRU responds to Traceback Requests by:

- GETTHRU has multiple people designated for and proficient in addressing traceback requests, including but not limited to a Support Team that monitors multiple inboxes, and a Success Team that maintains proactive relationships with our clients. We maintain up to date contact information for all our clients. We will facilitate all traceback requests from the Industry Traceback Group (ITG) and will coordinate communication with any client connected to activity for which the ITG initiates a traceback.
- GETTHRU will respond promptly to inquiries from the ITG, and if a pattern of questionable activity is detected, GETTHRU will require our client to cease such activity. If such activity is not immediately ceased, GETTHRU will ensure that the client's service with GETTHRU is suspended and/or terminated.

Cooperation with State and Federal Regulators:

GETTHRU will cooperate with state and federal regulators to prevent illegal robocalls by:

- Responding to law enforcement requests
- Providing relevant data and information in response to requests about illegal robocalls or other suspicious activities