



2537 Greenwood Ln #C2
Cameron Park, CA 95682
(916) 365-4800

2024 Robocall Mitigation Program Description

Astoundant Communications directs 100% of calls that originate from its network through wholesale voice service providers. Every wholesale provider has full STIR/SHAKEN implementation, and has certified that their implementations meet the requirements in 47 CFR § 64.6305(d)(ii)-(iii). Those wholesale providers have mechanisms to block illegal robocall traffic on their networks. By extension, if any calls originating on Astoundant's network contained illegal robocall signatures, Astoundant's wholesale providers would block those calls.

Additionally, Astoundant has the following in place to mitigate illegal robocalls.

- Astoundant Communications vets every customer to ensure that we do not provide services to outgoing call centers, telemarketing companies, political organizations, or any entities that would place large numbers of outgoing calls.
- Astoundant's terms of service indicate that outgoing calls using any type of automated calling devices such as ACD systems are prohibited, and all customers are required to agree to those terms before accepting service. Astoundant reserves the right to immediately terminate a subscriber's service and report any suspected illegal activity to law enforcement upon violation of the terms of service.
- All outgoing calls originating from Astoundant have caller ID that match the end user's assigned phone number. End users are not allowed to spoof or disable caller ID at any time.
- Astoundant's cloud PBX servers only allow connected devices to dial one number at a time. No device is allowed to dial more than one number simultaneously.
- Once a number is dialed and the call is active, Astoundant's PBX servers activate a 60 second countdown for the connected device that blocks dialing of 10 digit numbers. Internal extension dialing is allowed.
- Astoundant's PBX servers allow each connected device a maximum of two active concurrent outgoing calls to allow for 3-way calling.
- Astoundant blocks calls that match the signature of illegal robocalls, such as short duration calls. Call logs are live monitored to immediately detect any patterns that indicate illegal robocall activity that are not blocked and are not typical of end user calls. Any detected unusual patterns trigger an email of the call log entries to a system admin

for manual review. If there are indications of robocall behavior, the subscriber is immediately notified. A first incident results in a warning, and subsequent incidents within a 24 month period may result in immediate suspension or termination of services depending on severity of each incident.

- Astoundant assigns each end user a password protected account to connect an end device to a server for incoming and outgoing calls. Authentication is encrypted.
- All of Astoundant's cloud PBX servers operate in data centers in the United States. All of these instances whitelist US IP addresses and block all other foreign IP addresses of any external devices connecting to the server.