



Jaime "Jay" Alvarez
head geek and IT superhero
575-448-1204
headgeek@alvarezsupport.com
alvarezsupport.com

ALVAREZ SUPPORT SERVICES ROBOCALL MITIGATION PLAN

OVERVIEW

Alvarez Support Services is committed to providing reliable service while preventing illegal robocalling. If you suspect robocalls are originating from any of our endpoints please contact us at 575.448.1204 or email us at voipabuse@alvarezsupport.com.

Endpoints

- We do not allow ANY form of robotic calling from our deployed PBX systems, or any device/endpoint connected to our PBX. If you suspect illegal robocalling originating from our network, contact us immediately. Our abuse phone number is 575.448.1204 or you can email us at voipabuse@alvarezsupport.com. We follow the best practices described by the NANC Call Authentication Trust Anchor Working Group. (<https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>)

Traceback

- 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 could attempt to take over our device registrations.

Robocall Mitigation Program

- Alvarez Support Services, LLC uses bandwidth.com for SIP Trunks. This service is fully STIR/SHAKEN compliant and monitors all outbound voice traffic in real time to prevent the origination of illegal robocalls.



Jaime "Jay" Alvarez
head geek and IT superhero
575-448-1204
headgeek@alvarezsupport.com
alvarezsupport.com

Call Abuse Policy

- Any call originated on Alvarez Support Services, LLC PBX or managed PBX equipment is subject to review and investigation if the call is suspected of being fraudulent, abusive, or illegal. Any calls meeting this criterion would be blocked and device accounts deactivated. If conditions are repeated, or this becomes excessive from one specific IP address/location, the locations connectivity could be completely severed. Such activity may be subject to further investigation by the FCC for enforcement of the TRACED Act (2019). Persons found tampering with SIP devices, SIP accounts or the PBX in an attempt to facilitate such calls could be subject to fines and penalties imposed by the FCC or the jurisdictional court.