



ROBOCALL MITIGATION PLAN

In accordance with the new laws created to mitigate the spread of illegal robocalls, we at ITVoxCom Tech LLC have taken the following steps:

- 1) All clients must submit a KYC (Know Your Customer) form that verifies their real name, company name, and other essential information, such as the type of business, physical address, website, and/or verified social media accounts, main contact cell phone number, and the intended use of our phone systems before they can receive service from us. We do not accept anonymous organizations that are not properly registered as a business in the Sunbiz.org database, nor individuals who refuse to provide proper identification.
- 2) We strictly require all clients to read and sign a service agreement form that clearly defines the scope and limits of legal service usage. We also tell all our clients in that document that our services cannot be used for fraudulent purposes, including robocalls, and that we will fully cooperate with authorities if such activities occur. Additionally, we reserve the right to cancel the accounts of clients who violate our policies for proper service use.
- 3) We do not allow our clients to use Fake Caller IDs for their outbound calls. Clients are required to use the same Caller ID as their provided DIDs.
- 4) We have agreements and "Know Your Customer" (KYC) documents submitted to our carriers, which already have a robocall mitigation plan and STIR/SHAKEN implementations, as these carriers have requested these documents from us to continue doing business.
- 5) Our infrastructure and PBX Systems are protected with firewalls, and their access is restricted to the IPs of our clients only. If a security issue arises on our PBX systems or if a client believes someone has taken over or stolen their system admin credentials, or if passwords for current extensions have been changed, we proceed to trace and identify the intruder's IPs, block them with our firewalls, and change all passwords to ensure safety and peace of mind. Our firewalls capture and block most malicious traffic coming to us, but "human errors" such as exposing passwords to third parties may still occur. We have measures in place to help customers minimize the risk of unauthorized access for malicious purposes.

Finally, as a small VoIP traffic reseller, we understand that we have chosen to implement option #2 of the Form (Partial STIR/SHAKEN) as specified under 47 CFR § 64.6304.