



Robocall Mitigation Plan for GoLiveSMS

TECHNICAL AND OPERATIONAL FOUNDATIONS OF GOLIVESMS'S PLAN

GoLiveSMS's Robocall Mitigation Plan is premised upon a three-pronged set of technical and operational procedures, the details of which can be summarized as follows:

1. **Prevention:** As a Managed Service Provider, GoLiveSMS only offers VoIP and Hosted VoIP services to existing managed services customers. GoLiveSMS has a stringent on-boarding screening process designed to prevent those that may engage in any illegal operations, including robocalling, from becoming GoLiveSMS customers from the beginning. Once on-boarded, GoLiveSMS works to stay closely aligned with its customers regarding the industry's anti-robocalling objectives by providing regular customer communications to remind, educate and clarify what behaviors may signal or constitute unlawful robocalling and encourage them to take all necessary steps to prevent illegal robocalling behaviors on their networks. GoLiveSMS has also adopted contractual requirements to ensure that its customers agree to cooperate with the ITG and agree to follow all applicable laws against illegal robocalling fraud and abuse.
2. **Detection:** GoLiveSMS analyzes calling patterns and overall usage of VoIP services we offer to help determine when illegal and inappropriate robocalling activity may be occurring. When unlawful robocall campaigns are detected, GoLiveSMS works to stop the unlawful activity as quickly as possible. As we only provide hosted services, we are able to completely disable outbound calling until any issues are resolved.
3. **Mitigation:** In order to prevent the delivery of unwanted and illegal traffic to the greatest degree possible, GoLiveSMS works with third party vendors to manage its STIR/SHAKEN features as well as call blocking tools that are designed to block calls from invalid and illegal telephone numbers in keeping with industry best practices and the FCC's recommendations. As an industry leader, our third-party vendors also continue to work to enhance its mitigation capabilities through wide-spread adoption of STIR/SHAKEN together with critical IP traffic exchange capabilities across the industry. Our third-party vendors also work closely with Law Enforcement Agencies (LEA) at all levels of government and with its interconnected carrier

partners. Relatedly, our third-party vendors fraud and security experts are constantly working to respond to complaints and events, like the ITG, AG and LEA subpoenas that include analyzing our network traffic and initiating trouble tickets with customers that may be associated with the unlawful behaviors that may be at the source of such consumer complaints. In addition to these notifications, we then aim to work diligently together with our customers and other industry members to stop the unlawful robocall campaigns being detected. Finally, together with its active involvement in the ITG, our third-party vendors implement validly requested Do Not Originate (DNO) blocking pursuant to the industry best practices and procedures.