

Robocall Mitigation Plan for UnitedCloud Inc

UnitedCloud'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, UnitedCloud only offers VoIP and Hosted VoIP services to existing managed services customers. UnitedCloud has a stringent on-boarding screening process designed to prevent those that may engage in any illegal operations, including robocalling, from becoming UnitedCloud customers from the beginning. Once on-boarded, UnitedCloud 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. UnitedCloud 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: UnitedCloud 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, UnitedCloud 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, UnitedCloud works with Bandwidth Inc 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, Bandwidth Inc also continues to work to enhance its mitigation capabilities through wide-spread adoption of STIR/SHAKEN together with critical IP traffic exchange capabilities across the industry. Bandwidth Inc also works closely with Law Enforcement Agencies (LEA) at all levels of government and with its interconnected carrier partners. Relatedly, Bandwidth Inc's 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, Bandwidth Inc implements validly requested Do Not Originate (DNO) blocking pursuant to the industry best practices and procedures