

Section 1: Introduction and Company Background

Introduction. This document outlines the Robocall Mitigation Program (RMP) of Maxus33, developed in compliance with 47 C.F.R. § 64.6305. This program reflects our commitment to implementing effective measures against illegal robocalls, ensuring the integrity and reliability of our telecommunications services.

Company Background. Maxus33 is a provider of personal safety solutions through our mobile application, which connects users to emergency contacts via audio streams. Utilizing Bandwidth's voice services, Maxus33 ensures that each call is authenticated and verified, aligning with the STIR/SHAKEN framework to safeguard our users from fraud and abuse.

Section 2: STIR/SHAKEN Implementation

STIR/SHAKEN Implementation. Maxus33 leverages Bandwidth's robust STIR/SHAKEN implementation to ensure that all calls made through our app are fully authenticated. Bandwidth provides "A" level attestation for all calls using U.S. phone numbers, confirming the legitimacy of the caller's identity. This critical integration with our service provider helps us maintain the highest standards of call integrity and trust.

Section 3: Robocall Mitigation Plan

Robocall Mitigation Plan. Maxus33's robocall mitigation strategies are deeply integrated with Bandwidth's comprehensive analytics and monitoring systems, which screen and analyze call patterns for potential abuse. Our mitigation measures include real-time analytics to detect unusual calling activities, stringent customer verification processes, and immediate responsive actions to any alerts of potential robocall traffic.

Section 4: Customer Due Diligence

Customer Due Diligence. Maxus33 utilizes a unique approach to customer verification that prioritizes the safety and authenticity of emergency communications:

- **Emergency Contact Verification:** Before any calls can be made through the Maxus33 app, users must have their emergency contacts verify their identities and authorization to be contacted in emergencies. This ensures that all parties involved in communications are aware and have consented to participate.
- **App-Only Call Placement:** All calls facilitated by Maxus33 are strictly confined to the app environment, limiting the risk of misuse or unauthorized call origination. This app-centric approach helps ensure adherence to robocall mitigation policies.
- **No Direct User Vetting:** Given the emergency nature of the services, Maxus33 does not directly vet the identities of users but instead focuses on the verification process between users and their designated emergency contacts.

Section 5: Measures to Prevent or Avoid Exchanging Illegal Robocalls

Measures to Prevent or Avoid Exchanging Illegal Robocalls. Maxus33, in partnership with Bandwidth, implements a rigorous set of technologies and procedures designed to ensure the authenticity and legality of all calls made through our app:

- **STIR/SHAKEN Compliance:** Leveraging Bandwidth's capabilities, all calls initiated via the Maxus33 app are signed with full attestation under the STIR/SHAKEN protocol, validating the authenticity of the caller's identity.
- **Real-Time Analytics:** Bandwidth employs advanced analytics to monitor call patterns and behaviors. Any deviation from normal activity is flagged, enabling immediate investigation into potential robocall activities.
- **Single Call Restriction:** To prevent misuse and ensure the effectiveness of emergency communication, the Maxus33 app allows only one outbound call to emergency contacts at a time, preventing duplicate alarms and potential spam.
- **Proactive Blocking and Filtering:** Calls identified as suspicious through analytics are immediately blocked or filtered, preventing potentially harmful or illegal robocalls from reaching users.
- **User Activity Monitoring and Suspension:** Maxus33 actively monitors for excessive use of its calling feature. If unusual activity is detected, the user's account is suspended pending further investigation and resolution via a support ticket. This measure helps mitigate potential abuse and manage the per-user costs effectively.

Section 6: Responding to Traceback Requests

Responding to Traceback Requests. Maxus33, in collaboration with Bandwidth, ensures rigorous compliance with regulatory requirements regarding the tracing and mitigation of illegal robocalls:

- **Dedicated Response Team:** Maxus33, supported by Bandwidth's established infrastructure, has a dedicated team responsible for managing and responding to traceback requests. This team is trained to act swiftly, ensuring all requests are addressed within the mandated 24-hour period.
- **Prompt Investigation and Response:** Upon receipt of a traceback request, our team promptly initiates an investigation to trace the source and nature of the call, providing detailed feedback to the requesting entities as swiftly as possible.
- **Collaboration and Information Sharing:** We actively collaborate with Bandwidth and are part of a broader telecommunications network that exchanges necessary information and cooperates on traceback investigations, ensuring a thorough approach to addressing and mitigating illegal calls.
- **Record Keeping:** Maxus33 maintains comprehensive records of all traceback requests and the subsequent actions taken. These records are kept to ensure transparency and accountability in our efforts to combat robocall abuse.