



Robocall Mitigation Plan

Believe Wireless, LLC (Believe Wireless) is a provider of Internet and Voice Over Internet Protocol (“VoIP”) services in Maryland and is dedicated to stopping illegal calls from originating on our network.

Believe Wireless has adopted this Robocall Mitigation Plan to describe the measures Believe Wireless has established to prevent the origination, carrying, or processing of unlawful robocalls from its voice services.

Believe Wireless is working to complete full STIR/SHAKEN implementation. Believe Wireless has obtained an OCN and submitted registration information with the Policy Administrator in order to be able to receive Service Provider Code tokens. Believe Wireless has been informed that the Policy Administrator has a temporary freeze in place for new registrations and is awaiting lifting of the freeze. Once lifted, Believe Wireless will move forward with completion of STIR/SHAKEN implementation.

I. KNOW YOUR CUSTOMER

Believe Wireless follows the best practices for vetting caller identity recommended by the North American Numbering Council (NANC) [Call Authentication Trust Anchor Working Group](#). This process includes confirming the identity of Believe Wireless customers – (i) contact person(s); (ii) business location; (iii) state or country of incorporation; (iv) federal tax identification; and (v) the nature of our customers’ businesses.

II. CONTRACTUAL TERMS

Believe Wireless maintains prohibitions against robocalling in its Terms of Service that customers must accept before being permitted to use Believe Wireless’ voice services. Customers using Believe Wireless services agree to abide by the requirements set forth in our Terms of Service Agreement. Customers are informed that Believe Wireless will block services to a customer suspected or found to be using the services for illegal activities, including Robocalling. Customer’s subscription to Believe Wireless’ services will be terminated if it is determined the violations occurred.

III. KNOW YOUR UPSTREAM PROVIDER

Believe Wireless will not accept traffic from any carrier that is not registered or has been removed from the Robocall Mitigation Database.



IV. TRACEBACK REQUESTS

Believe Wireless commits to respond fully, within 24 hours, to all traceback requests from the Federal Communications Commission, law enforcement, state attorneys general, and the Registered Traceback Consortium. Believe Wireless will cooperate with such entities to investigate and stop any illegal robocallers that use Believe Wireless' service to originate calls.

V. ROBOCALL MITIGATION PROGRAM

Believe Wireless has taken the following actions to comply with the Robocall Mitigation Caller ID requirement:

Believe Wireless has the capability to mitigate robocalls using the mitigation methods listed below.

- Blacklists
 - Block calls by calling numbers or call prefixes
 - Block calls by SPIDs that are not customers of Believe Wireless
 - Block calls originating outside Believe Wireless's network or its customers' networks
 - Block IP addresses identified as SPAM or robocalls
 - Identify User agents that our customers do not use
- Call CAPTCHA
 - Call Detail Record (CDR) Analysis
 - Generate reports that identify high call volume, short call durations, and excessive calls to and from the same number
- Customer Controls
 - Call volume limits
 - Ability to block calls
 - Limit caller id to assigned telephone number

VI. PLAN UPDATES

Believe Wireless will continue to monitor industry best practices and improve our internal processes to ensure our systems adapt to address the ongoing challenges affecting this industry.