

April 26, 2024

Pursuant to the applicable orders and regulations of the Federal Communications Commission ("FCC" or "Commission"), the following is [REDACTED], LLC's ("[REDACTED]") Robocall Mitigation Program ("RMP") that it established to prevent unlawful robocalls from originating, terminating, or being carried or processed on [REDACTED] call distribution platform where it is operating as a small voice service provider.

[REDACTED] hereby certifies to the implementation of the following practices:

1. Traceback requests: [REDACTED] will respond fully and in a timely manner within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.
2. Upstream providers and monitoring: [REDACTED] is a VOIP reseller and does not control any of the underlying network infrastructure. [REDACTED] carriers are [REDACTED], all of which are authorized providers from the STIR/SHAKEN policy administrator and which [REDACTED] has confirmed are listed in the Robocall Mitigation Database. Because [REDACTED] does not have access to the necessary infrastructure, it relies on its upstream providers to assist in robocall mitigation. [REDACTED] has master service agreements with its upstream providers, and has reviewed all upstream provider filings and their plans via RPM on how they plan to monitor their originating traffic for robocall mitigation. [REDACTED] does not use any third-party analytics vendor.
3. [REDACTED] customers:
 - a. [REDACTED] maintains and validates customer information and identity using customers' address (physical and emailing), and Federal Tax ID.
 - b. [REDACTED] logs all calls originated from its platform and maintains those logs for at least 7 years.
 - c. [REDACTED] service will not allow a customer to utilize a particular phone number as Caller ID unless:
 - i. The number was obtained directly from CallShaper and is currently assigned to that customer.
 - ii. Or the customer has provided sufficient proof that they are authorized to use a particular number themselves or on behalf of their client.
 - d. [REDACTED] service does not allow automated dialing to wireless numbers unless the customer specifies that they have properly obtained express written consent.
 - e. [REDACTED] will block services to any customer if it determines the customer is using the service for illegal robo-calling.

4. This plan and industry best practices must evolve to response to the dynamic nature of mitigating illegal robocalling. [REDACTED] will monitor industry best practices and continuously improve our internal processes to ensure this plan and our system adapt to this ever-changing issue.

[REDACTED] further certifies:

1. All of the calls by any of its customers and that [REDACTED] originates are subject to this RMP, any prior certification has not been removed by the Commission, and [REDACTED] has not been prohibited from filing in the Robocall Mitigation Database by the Commissions.
2. [REDACTED] commits to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.
3. In the prior two years, [REDACTED] has not been, to the best of its knowledge, the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.