

Robocall Mitigation Plan

Voximplant, Inc.

Voximplant, Inc. (“**Voximplant**”) submits the following Robocall Mitigation Plan in compliance with 47 CFR § 64.6305(d)(ii)-(iii).

Reasonable Steps to Prevent New and Existing Customers from Originating Illegal Calls:

Voximplant has implemented meaningful protections to mitigate illegal robocalls. As described herein, they include traffic analytics, Know-Your-Customer and Know-Your-Upstream-Provider procedures, cooperation with its upstream provider and other parties in tracebacks, and contractual protections, such as the acceptable use policy.

Acceptable Use Policy:

Before services commence, Voximplant’s customers must agree to comply with Voximplant’s terms of service, including the acceptable use policy, which contains provisions designed to combat unlawful robocalling activity. Customers agree that they will not misuse Voximplant’s services, including by engaging in spamming or unsolicited advertising, marketing, or other activities (including, without limitation, any activities that violate anti-spamming laws including the CAN-SPAM Act, TCPA, and Do-Not-Call Implementation Act). Voximplant’s terms of service similarly prohibit the use of the platform for sending unsolicited marketing messages or broadcasts; placing prohibited calls to emergency services such as hospitals, fire and police; utility-related telephone numbers; using strings of numbers (or engaging two or more lines of a multi-line business); misleading others as to caller identity; and any type of fraudulent activity.

Description of Analytics to Block Illegal Traffic:

Voximplant works to detect a calling pattern consistent with illegal robocalls. Voximplant deploys an internal analytics system to monitor call volumes and detect anomalies such as high-volume patterns or suspicious source behavior. It monitors for abnormal call patterns, such as:

- Excessive short-duration calls.
- High-volume call bursts.
- Traffic suggestive of autodialed or spoofed activity.

If any anomalies are detected and a call source exhibits suspicious behavior, Voximplant immediately coordinates with its upstream providers for further investigation and possible mitigation or blocking. Voximplant works to identify the party who is using its network to originate potentially illegal robocalls and takes appropriate action, which may include initiating a traceback investigation, verifying that the originating subscriber owns or is authorized to use the Caller ID number, and suspending or terminating the party’s ability to originate calls on Voximplant’s network. No third-party vendors are involved in deploying Voximplant’s analytics.

Voximplant follows Industry Traceback Group (“ITG”)-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive

Robocall Mitigation Plan

Voximplant, Inc.

responses, Voximplant will devote sufficient resources to provide prompt and complete resources to traceback requests.

Know Your Customer Practices:

Voximplant complies with applicable FCC know-your-customer requirements and implements procedures to verify the identity and legitimacy of both business and individual customers before allowing them to originate traffic. For business customers, Voximplant verifies corporate formation, good standing, tax or registration information, business address, phone number, commercial presence, authorized representatives, and a certification that the customer has not been subject to adverse robocall-related determinations. For natural-person customers, Voximplant verifies the person's identity, address, phone number, commercial presence, and the same robocall-related certification.

Voximplant also renews proof of good standing for business customers every six months, monitors customer traffic for suspicious robocalling patterns, conducts enhanced review or reverification when warranted, and safeguards all sensitive or confidential customer information through appropriate administrative, technical, and physical protections.

Voximplant also conducts special screening to ensure customers are not identified in any international sanctions lists.

Know Your Upstream Provider Practices:

Voximplant complies with applicable FCC due-diligence requirements for gateway and intermediary providers immediately upstream from Voximplant by obtaining and verifying corporate information (such as corporate formation, good standing, tax or registration information, business address, phone number, commercial presence, authorized representatives, and a certification that the entity has not been subject to adverse robocall-related determinations), confirmation of the upstream provider's active Robocall Mitigation Database certification, and contractual certifications that the upstream provider prohibits unlawful traffic and maintains mechanisms to ensure compliance with federal and state robocalling restrictions.

Voximplant verifies each upstream provider's RMD status before accepting traffic and at least quarterly thereafter, documents the verification results, and stops accepting traffic if the provider is not listed in the RMD or has been delisted. Voximplant includes robocall-compliance certifications, unlawful-traffic prohibitions, and notice obligations in upstream-provider agreements. Voximplant also monitors upstream traffic on an ongoing basis, responds to tracebacks under its established procedures, monitors FCC EB Docket No. 22-174 for relevant Final Determination Orders, blocks traffic from affected upstream providers within the required

Robocall Mitigation Plan

Voximplant, Inc.

timeframe, and safeguards sensitive and confidential upstream-provider information through administrative, technical, and physical protections.

Voximplant's upstream providers are NUSO LLC, Bandwidth Inc., Multitel LLC.

Voximplant maintains written agreements with its upstream providers, requiring them to:

- Certify they implement STIR/SHAKEN or acceptable robocall mitigation measures.
- Ensure traceability and prompt cooperation in traceback investigations.

Voximplant and its upstream providers have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Commitment to Respond to Traceback Requests:

Voximplant is willing and able to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the Industry Traceback Group, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

Blocking:

Voximplant will promptly respond to Do Not Originate requests it receives from ITG. Voximplant has mechanisms to automatically block suspicious calls using internal analytics.

Plan Updates:

This plan, along with industry best practices, will evolve to response to the dynamic nature of mitigating illegal robocalling. Voximplant will monitor industry best practices and continuously improve our internal processes to ensure this plan, and our system adapts to this ever-changing issue.

In the event of any material change to this plan, Voximplant will file such an update to the FCC Robocall Mitigation Database within ten (10) days of such update.