

Voice Mail Depot, Inc. Robocall Mitigation Plan

This Robocall Mitigation Plan is submitted by Voice Mail Depot, Inc. pursuant to the provisions of 47 C.F.R. § 64.6305, adopted by the Federal Communications Commission (FCC), which requires all “voice service providers” to establish a “robocall mitigation plan”. This document sets forth the Provider’s current policies and procedures designed to reduce or eliminate outbound illegal robocalls originating on its network. The Provider views these policies and procedures as constituting “reasonable steps” to avoid the origination of illegal robocalls on its network and in addition to following these steps the Provider commits to responding to all traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG), and to cooperate with such entities in investigating and stopping any illegal robocallers that may use its service to originate calls.

I. STIR/SHAKEN IMPLEMENTATION STATUS

As indicated in the FCC’s Robocall Mitigation Database, the Provider’s status with respect to STIR/SHAKEN implementation is as follows:

- The Provider has not implemented the STIR/SHAKEN authentication framework on any portion of its network and all calls originating on its network are subject to the policies and procedures set forth in this Robocall Mitigation Plan which are intended to stop anyone from using the Provider’s service to originate illegal robocalls.
- The Provider currently relies on the “Complete STIR/SHAKEN Implementation” of its sole Upstream Provider, listed in **Appendix A**.
- All calls originating on the Provider’s network are sent using an upstream carrier that has attested to full and complete STIR/SHAKEN implementation in the Robocall Mitigation Database.

II. TRACEBACK REQUESTS

As noted above, the Provider will cooperate with the FCC, law enforcement, and the ITG on all traceback requests and investigations. To allow for timely and comprehensive law enforcement response efforts against illegal robocallers, the Provider will dedicate sufficient resources to promptly complete and provide timely responses to all traceback requests received from the FCC, law enforcement and/or the

ITG, and commits to fully responding to any traceback request received within 24 hours. Within **Appendix A** to this Plan, the Provider identifies a single point of contact for all traceback requests.

As part of its efforts to assist in the successful traceback of illegal robocalls, the Provider will include within its carrier interconnection and/or service agreements, language requiring traceback cooperation on any voice service calls. In part, these contract provisions will specify the need for parties to promptly identify the upstream provider from which a suspected illegal robocall originated and/or the customer details of the service from which the call originated.

III. CUSTOMER VETTING PRACTICES

As a means of preventing or minimizing the origination of illegal robocalls through its voice services, the Provider will use best practices in vetting the identity of all its voice service subscribers, whether residential or business/commercial, including any subscribers that are purchasing voice services for resale. The subscriber vetting process is intended to help determine the legitimacy of a customer for the purpose of establishing a service relationship. Generally, the Provider looks to confirm the identity of customers through collecting information such as physical customer location, contact person(s), state or country of incorporation, and the nature of customer's business.

Efforts to vet subscribers can occur during the process of provisioning requested services, executing the Provider's service agreements, and/or granting customers the right to use telephone number resources. Commercial users, which are usually comprised of larger businesses with more complex service configurations, are generally recognized as presenting a higher risk of perpetrating illegal robocalls, and thus, at the Provider's sole discretion, may be subject to additional review, including but not limited to a more stringent background check.

Further, with respect to meeting existing obligations to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls, the Provider:

- Utilizes service agreements and acceptable use policies as a means of preventing its new and existing subscribers from using their voice services in ways that are in violation of local, state, or federal laws, or to engage in any deceptive or fraudulent activity. These documents governing the use of voice services include Terms and Conditions, which specifically indicate to all customers that Provider's voice services are not permitted to be

used for any unlawful purpose, including making illegal robocalls, and the Provider reserves authority within its service agreements to suspend or terminate services for violating applicable terms or conditions.

- Has established a routine process for monitoring the usage and quality of its networks, and conducts recurring and timely reviews of its call detail records (CDRs) to facilitate early identification of unusual or suspicious calling activity or patterns that may indicate use of its network for originating illegal robocalls. In those instances where Provider identifies activities or patterns consistent with illegal robocalls, the customer will be contacted in regard to further investigation and possible termination of their services.

IV. TELEPHONE NUMBER VALIDATION PRACTICES

Telephone Number Validation refers to the process of confirming the customer or end-user's right to use a telephone number in connection with their subscribed voice service(s). In accordance with industry best practices, the Provider has procedures in place to confirm the calling customer's right to use a telephone number. Specifically, a subscriber of Provider's voice services is permitted to use a telephone number as their caller identity if a number is managed directly by the Provider and/or obtained by the Provider via an underlying partner. Further, for: (1) single line voice service subscribers, the switching equipment has been set up to only accept calls from the number assigned to that subscriber; and (2) multi-line voice service subscribers, the Provider screens all originating calls and only allows calls to be connected if the originating number matches one of the numbers assigned to the subscriber. These screening capabilities ensure an automated and secure method of validating originating telephone numbers.

V. INTERNATIONAL CALL ORIGINATORS

The Provider is not currently an international voice services provider. If at any time in the future it decides to sell its services to international call originators using North American Numbering Plan resources, it will familiarize itself with, and develop best practices for, fully vetting such customers and performing telephone number validation on all international originating calls.

VI. KNOW YOUR UPSTREAM PROVIDER PROCEDURES

As a small provider of voice services, the number of upstream providers used by the Provider to receive and deliver its originated voice calls for termination are limited. The Provider has longstanding relationships with its upstream providers and maintains its awareness of the nature of their businesses and the legitimacy of their call transmission services.

The Provider, in the interest of providing the highest quality voice services to all its customers, is committed to taking the steps necessary to ensure that any upstream providers providing connectivity are equally committed to monitoring their networks and preventing their use for the transmission of illegal robocalls. Included as part of **Appendix A** to this Robocall Mitigation Plan is a list of the Provider's current "Upstream Provider(s)" along with contact information for each.

VII. ONGOING ROBOCALL MITIGATION PRACTICES

The Provider monitors the usage of its networks and examines call detail records (CDRs) on a recurring basis for the purpose of detecting suspicious call activity and/or calling patterns. When network usage patterns consistent with illegal robocalls are detected, or the Provider otherwise suspects illegal robocalling or spoofing is taking place on its network, it immediately seeks to identify the party that is originating, terminating, or routing these calls so that it may take appropriate action. These actions may include, but are not limited to: initiating a traceback investigation; verifying that the originating customer owns or is authorized to use the Caller ID number; determining whether the Caller ID name sent to a receiving party matches the subscriber name, trademark, or d/b/a name; terminating the offending party's ability to originate, terminate, or route calls over the Provider's network; and providing notice to law enforcement authorities.

As part of its Plan to mitigate and prevent any originating robocalls on its network, the Provider is committed to early identification and investigation of possible robocalling situations. In monitoring usage of its network, particular attention is given to: (1) higher than normal subscriber traffic volume including large bursts of traffic in small timeframes or inconsistent volumes of traffic (spikes in usage); (2) originating calls of short duration and low call completion percentages; (3) originating calls with sequential called to number dialing patterns; (4) repeated calls made to do-not-call registry or invalid numbers; and (5) calls to NPA-NXXs not assigned by the North American Numbering Plan Administrator.

Appendix A

Traceback Request Single Point of Contact:

Name: Will Conry

Title: CTO

Phone Number: 949-223-3935

Email Address: wconry@voicemaildepot.com

Upstream Provider Information:

Name of Upstream Provider: Bandwidth Inc.

Nature of Business: Wholesale Telecom Provider

Network Location of Upstream Provider: Raleigh, NC

Name of Contact: Steven Thayer

Title: Director, Fraud Operations

Phone Number: 919-704-3069, ext. 1