



Robocall Mitigation Plan

Business Information:

Primevox Communications, LLC
1321 Upland Dr #8245
Houston, TX 77043

Contact Information:

Luke Escude
Chief Executive Officer
(972) 600-1150 x4
compliance@Primevox.net

Overview:

Per FCC STIR/SHAKEN requirements, all voice service providers (“VSPs”) must certify that they have taken reasonable and necessary steps to prevent and mitigate illegal, originating robocalls by submitting a Robocall Mitigation Plan (“RMP”) in the FCC’s Robocall Mitigation Database. This plan is expected to significantly reduce the origination of illegal robocalls and must contain the following information:

- Details on the steps taken to avoid illegal, originating robocalls
- A commitment to respond to traceback requests and cooperate with investigators to stop illegal, originating robocalls

Purpose:

Primevox Communications, LLC (“Primevox”) is dedicated to stopping and preventing illegal robocalls from originating or terminating on its network. This document describes the steps taken by Primevox to accomplish this.

STIR/SHAKEN:

Primevox’s traffic is fully STIR/SHAKEN compliant and authorized directly by the STI-PA.

Know Your Customer:

New customers are required to provide the following information to assure they are a legitimate organization:

- Company Name
- Physical Service Address
- Federal EIN
- Authorized User Information (Name, Phone Number, Email Address)
- FCC 499 Filer ID (If customer is a reseller)

If a new customer is porting existing numbers from another VSP, the following information is required to verify DID ownership:

- Signed Porting Letter of Authorization by an authorized user
- A VSP invoice dated within 30 days

A Customer Service Record (CSR) is used to establish additional validity if available or accessible.

Acceptable Use Policy (AUP):

Before being allowed to use Primevox's network and services, customers must sign a service agreement which contains its AUP.

Prohibited conduct includes, but is not limited to, the distribution, transmission, receiving, use or store any type or kind of material that:

- in violation of any local, state, or federal laws and regulations; or
- that may adversely affect Primevox Services or other Primevox Customers.

The fair and reasonable use of Primevox's network and services does not include:

- spamming or blasting (e.g., sending one hundred (100) or more bulk and/or junk voicemail or faxes simultaneously); or
- auto-dialing or "predictive" dialing (i.e., non-manual dialing or using a software program or other means to continuously dial or place outbound calls) without prior validation or permission.

Primevox has the right to suspension or terminate service, with or without notice. Primevox has the right, but not the obligation, to take further action as it deems to be appropriate under the circumstances to eliminate or preclude repeated violations.

Mitigation and Prevention:

Primevox allows the spoofing of telephone numbers only if a customer is (a) actively moving their service to Primevox's network or (b) can provide documentation that the telephone numbers are owned and controlled by customer.

Outbound concurrency limits are placed on all channels to monitor for fraud and suspicious activity. If a concurrency limit is reached, system alerts notify engineering staff immediately.

Suspicious activity is investigated using the following procedures:

- Referencing of call history logs and patterns;
- Checking for any system issues that may be generating the strange behavior;
- Verifying that the calls are coming from a valid number controlled by Primevox or previously validated as owned by a customer.
- Contacting the customer to understand their particular use case and validate that the activity belongs to that customer.

Traceback:

Primevox will respond to all traceback requests from the Federal Communications Commission, law enforcement, and the registered traceback consortium within the required 24 hours. Primevox will cooperate with such entities in investigating and stopping any illegal robocallers including implementing any Do Not Originate Requests.