



### **Business Information**

Nextiva, Inc.  
9451 East Via de Ventura  
Scottsdale, AZ 85256

### **Contact Information**

Joshua Lesavoy  
Chief Information Officer  
480-753-4763  
[jlesavoy@nextiva.com](mailto:jlesavoy@nextiva.com)

### **Overview**

In the Commission's recent release, In the Matter of Call Authentication Trust Anchor, Sixth Report and Order and Further Notice of Proposed Rulemaking, WC Docket No. 17-97 (rel. March 17, 2023) ("R&O") it is stated that all voice service providers ("VSPs") must file robocall mitigation plans ("RMPs") that, among other things, outlines "reasonable steps" taken to avoid originating illegal robocalls.

In addition to the "reasonable steps," the FCC requires that a RMP include:

- "know your customer" procedures;
- a description of any call analytics system used to identify and block illegal traffic; and
- whether a third-party vendor is used and if so, the name of the vendor.

The FCC previously stated that a RMP is sufficient if the detailed practices in the plan can reasonably be expected to significantly reduce robocalls.

### **Purpose**

Nextiva, Inc. ("Nextiva") is a Voice Service Provider dedicated to stopping illegal calls from originating in our network. As certified in the FCC's Robocall Mitigation Database, Nextiva has fully implemented STIR/SHAKEN. In compliance with the R&O, Nextiva submits this Robocall Mitigation Plan and certification.

### **Know Your Customer ("KYC")**

The accurate identification of a subscriber in the STIR/SHAKEN ecosystem is tied to a telephone number-based caller identity associated with that subscriber. A subscriber is an entity that has a business relationship with Nextiva in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.



Nextiva's KYC program involves obtaining specific subscriber information when the customer establishes service. This process includes collecting information such as:

- physical business location(s);
- contact person(s);
- nature of customer's business

### **Know Your Upstream Providers**

In accordance with the Commission's directive in Advanced Methods to Target and Eliminate Unlawful Robocalls Call Authentication Trust Anchor, Seventh Report and Order In CG Docket 17-59 and WC Docket 17-97, Eighth Further Notice of Proposed Rulemaking In CG Docket 17-59, and Third Notice of Inquiry in CG Docket 17-59 (Rel. May 19, 2023) ¶¶ 49-51, Nextiva provides the following information concerning its upstream voice carriers.

Nextiva receives voice traffic from the following upstream providers:

- 1) Intellicent  
550 West Adams Street  
Suite 900  
Chicago, IL 60661
- 2) Bandwidth Inc.  
900 Main Campus Drive  
Suite 100  
Raleigh NC 27606  
Stephen Thayer, Senior
- 3) Lumen Technologies  
100 Centurylink Drive  
Mailstop 3TCW88.2  
Monroe, LA 71203
- 4) Peerless Network, Inc  
433 West Van Buren  
Suite 410S  
Chicago, IL 60607
- 5) TSG Global, Inc.  
10 Cedar Brook Circle  
Holbrook, MA 02343

According to the Robocall Mitigation Database, Intellicent, Bandwidth, Lumen Technologies, Peerless network, and TSG Global are fully STIR/SHAKEN compliant and, to the best of Nextiva's knowledge, information, and belief, Intellicent, Bandwidth, Lumen Technologies, Peerless Network, and TSG Global have been, and will continue to,



sign calls transmitted to Nextiva, and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to Nextiva.

### **Acceptable Use Policy ("AUP")**

Nextiva maintains an AUP that subscribers must sign before being permitted to use Nextiva's system(s). Among other things, the AUP prohibits:

- Providing altered, deceptive, or false information about the identity of the sender or the origin of a message or phone call;
- Violating any applicable local, state, or federal law;
- Violating applicable industry accepted guidelines; and
- Using Nextiva's service to engage in or in connection with fraudulent activities.

Nextiva's contractual terms with subscribers specify that Nextiva may act by suspending or terminating service for violation of the AUP.

### **Telephone Number Authorization**

A Telephone Number ("TN")-based caller identity is the originating phone number included in call signaling used to identify an outbound caller for screening purposes that is uniquely associated with the subscriber. A subscriber is permitted to use a TN as a caller identity if a TN is directly managed by Nextiva and/or obtained by Nextiva from one of Nextiva's underlying carriers for use by the subscriber.

In most cases, Nextiva directly manages the TNs used by its subscribers. Nextiva tracks these numbers in its inventory system and monitors the assignment of these numbers. Nextiva denies the ability for customers to input any TN other than those assigned to the account as outbound caller identity.

If a subscriber wishes to use a TN as a caller identity and that TN is not directly managed by Nextiva, then TN validation is necessary. If a subscriber's end-user can provide a valid letter of authorization that they are the authorized user of such TNs, Nextiva will attest calls originated with these TNs.

Nextiva provides information on its implementation of STIR/SHAKEN and requirements to register a number not directly managed by Nextiva at the following url: <https://www.nextiva.com/support/articles/stir-shaken-faqs.html>.

### **Analytics for Monitoring Traffic**

Nextiva works with its upstream carrier to analyze high-volume voice traffic in order to identify and monitor patterns consistent with robocalls. If Nextiva or its carrier partners detect a calling pattern consistent with illegal robocalls, we will identify the party and take appropriate action. Appropriate action may include, but is not limited to, 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 our system.

Nextiva utilizes Sansay NSS (Number-lookup for Stir/Shaken) for TN Attestation and Verification implementation.

### **Investigate Suspicious Activity**

When traffic analysis or automated alerting via Equinix indicates the presence of likely illegal robocalling, Nextiva's risk prevention team is alerted which follows the defined procedures on investigating such subscribers.

The procedures established include but are not limited to:

- checking recent and past call detail records and benchmark against expected trends;
- checking recent and past account activity and purchases;
- investigating if any system issue generates the strange behavior;
- verifying that the call originating path is valid; and
- contacting the subscriber to understand his or her particular use case and validate that the activity belongs to that subscriber.

Nextiva follows Industry Traceback Group ("ITG")-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, Nextiva devotes sufficient resources to provide prompt and complete resources to traceback requests.

### **Blocking**

Nextiva will implement Do Not Originate requests it receives from the ITG. Nextiva has procedures to block suspicious calls. If Nextiva identifies suspected robocalling patterns that are confirmed with further investigation, Nextiva will take appropriate action which may include suspending or terminating the subscriber's use of Nextiva's systems. Nextiva will cooperate with investigative bodies, provide a single point of contact to address traceback requests from law enforcement, including state attorneys general offices, FCC, and ITG; as well as documenting requests & actions taken in response thereto.

### **Plan Updates**

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



In the event of any material change to this plan, Nextiva will republish it to employees, consultants and contractors and file such an update to the FCC Robocall Mitigation Database within ten (10) days of such update.



### **Certification of Joshua Lesavoy**

I, Joshua Lesavoy, Chief Information Officer of Nextiva, Inc. ("Nextiva") do hereby certify, under penalty of perjury, the following:

- (1) Nextiva has fully implemented STIR/SHAKEN in the IP portions of its network
- (2) Nextiva's business name and primary address are as follows:

Nextiva, Inc.  
9451 East Via de Ventura  
Scottsdale, AZ 85256

- (3) Nextiva has no other business names in use.
- (4) Nextiva has not previously used any other business name.
- (5) The name, title, department, business address, telephone number and email address of the individual responsible for addressing robocall-related issues are listed in the above robocall mitigation plan.
- (6) Nextiva's role in the call chain is that of a voice service provider with a STIR/SHAKEN implementation obligation serving end-users.
- (7) Nextiva has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (8) Nextiva is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.

---

Joshua Lesavoy  
Chief Information Officer