

## **Robocall Mitigation Plan**

### Business Information

CallCurrent, Inc.  
1 Sansome St, Suite 1400 10104,  
San Francisco, CA 94104

### Contact Information

Anna Nazarenko  
Controller  
206.656.3471  
[an@omnivoice.ai](mailto:an@omnivoice.ai)

### 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 the origination of illegal robocalls and the VSP complies with the practices it describes in its filing.

### Purpose

CallCurrent, Inc. ("CallCurrent") is a VSP dedicated to stopping illegal calls from originating in our network and monitoring the calls traversing our network. As certified in the FCC's Robocall Mitigation Database, CallCurrent has fully implemented STIR/SHAKEN. In compliance with the R&O, CallCurrent submits this RMP 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 CallCurrent in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

CallCurrent's KYC program requires subscribers to abide by its Terms of Service and confirms same by mandating that they accept the Terms of Service before commencing service. CallCurrent confirms a subscriber's identity by vetting a subscriber directly or through a third-party vetting service. The vetting process includes collecting such information such as:

- physical business location;
- contact person(s);
- nature of the 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, CallCurrent provides the following information concerning its upstream voice service carrier.

CallCurrent has one upstream provider from which it receives voice traffic:

Bandwidth Inc.  
900 Main Campus Drive  
Suite 100  
Raleigh NC 27606  
Stephen Thayer  
(855) 864-7776  
[voicsecurity@bandwidth.com](mailto:voicsecurity@bandwidth.com)

CallCurrent has a master service agreement with its upstream provider and has received assurances that it has, and will continue to, sign calls transmitted to CallCurrent, and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to CallCurrent. CallCurrent and its upstream providers have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

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

CallCurrent maintains an AUP that subscribers must accept before being permitted to use CallCurrent's network. 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 CallCurrent's service to engage in or in connection with fraudulent activities.

CallCurrent's contractual terms with subscribers specify that CallCurrent may take action up to suspension or termination of 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 CallCurrent and/or obtained by CallCurrent from one of CallCurrent's underlying carriers for use by the subscriber. In most cases, CallCurrent directly manages the TNs used by its subscribers. CallCurrent tracks these numbers in its inventory system and monitors the assignment of these

numbers. In these cases, TN validation is the inherent result of CallCurrent's assignment of the TN to its subscriber.

When originating a call, CallCurrent checks the calling party number against CallCurrent's inventory and will not attest the call unless the calling party number is a TN that has been properly validated.

#### Analytics for Monitoring Traffic

CallCurrent has a monitoring and reporting system in place to analyze high-volume voice traffic to identify and monitor patterns consistent with robocalls. Our server-based monitoring system alerts us to calling patterns with unusual spikes, traffic patterns, and related matters.

If CallCurrent detects a calling pattern consistent with illegal robocalls, we will identify the party that is using our network to originate those calls and will take appropriate action. Taking 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 network.

No third-party vendors are involved in deploying CallCurrent's analytics.

#### Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, our 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; and
- contacting the subscriber to understand his or her particular use case and validate that the activity belongs to that subscriber.

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

#### Blocking

CallCurrent work with other carriers to abide any Do Not Originate requests it receives from the ITG. CallCurrent will cooperate with Investigative Bodies (provide a single point of contact to address traceback requests from law enforcement and regulatory entities such as state attorneys general, the FCC, and/or ITG; as well as documenting requests & actions taken in response thereto.

#### Plan Updates

This plan and industry best practices must evolve to response to the dynamic nature of mitigating illegal robocalling. CallCurrent 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, CallCurrent 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.

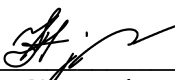
**Certification of Anna Nazarenko**

I, Anna Nazarenko, Controller of CallCurrent, Inc. ("CallCurrent") do hereby certify, under penalty of perjury, the following:

- a. CallCurrent has fully implemented STIR/SHAKEN in the IP portions of its network.
- b. CallCurrent's business name and primary address are as follows:

CallCurrent, Inc.  
1 Sansome St, Suite 1400 10104,  
San Francisco, CA 94104

- c. CallCurrent has two other business names in use: MightyCall and Omnivoice.
- d. CallCurrent has not previously used any other business name.
- e. 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.
- f. CallCurrent's parent company is Infratel, Inc. (BVI); subsidiary is MightyCall LLC; owners with shares of 10% or more are Ilya Zubarev and Serg Bell; director is Dmitriy Lepikhov.
- g. CallCurrent's role in the call chain is that of a voice service provider with a STIR/SHAKEN
- h. implementation obligation serving end-users.
- i. Neither CallCurrent nor any of the interest holders listed above have been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- j. CallCurrent and its interest holders have not subject been to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- k. CallCurrent's Operator Code Number is 012K.

  
\_\_\_\_\_  
Anna Nazarenko