

Robocall Mitigation Plan

Business Information

Callcentric, Inc.
11 Broadway – Suite 1015
New York, NY 10004

Contact Information

Stephen Irwin
VP of Operations
(212) 379-4038
stephen@Callcentric.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 the origination of illegal robocalls and the VSP complies with the practices it describes in its filing.

Purpose

Callcentric, Inc. ("Callcentric") is dedicated to stopping illegal calls from originating in our network and monitoring the calls coming into our network. Callcentric is fully STIR/SHAKEN compliant. In compliance with the R&O, Callcentric submits this RMP and certification.

Know Your Customer

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

New Subscribers

1. To create an account and purchase services, all customers are required to provide info including (but not limited to): name, location, email address, payment information, etc. [REDACTED]

[REDACTED]

4. All new subscriber accounts are limited to being able to place a maximum of 3 concurrent outbound calls at a time. To increase this limit, subscribers are required to complete a manual verification process which requires providing additional subscriber information and supporting documentation

5. Callcentric does not allow unchecked "spoofing" on calls placed via its service. Callcentric only allows its customers to use the following for outbound caller ID on calls placed through its network: (a) On-network numbers assigned to the customer by Callcentric; and (b) verified/validated third-party numbers.

Existing Subscribers

[REDACTED]

Acceptable Use Policy

Callcentric maintains an Acceptable Use Policy ("AUP") that subscribers must sign before being permitted to use Callcentric's network. Among other things, this 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 Callcentric's service to engage in (or in) connection with fraudulent activities.

Callcentric's contractual terms with subscribers specify that Callcentric may take action, up to suspension or termination of service for violation of the AUP. See <https://www.callcentric.com/terms/>

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, Callcentric provides the following information concerning its upstream voice carriers.

Callcentric receives voice traffic from the following upstream provider:



This upstream provider abides by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to Callcentric. Callcentric and its upstream provider work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests.

Telephone Number Authorization

A Telephone Number ("TN")-based caller identity is the originating phone number included in call signaling used to identify the 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 Callcentric and/or obtained by Callcentric from one of Callcentric's underlying carriers for use by the subscriber. In most cases, Callcentric directly manages the TNs used by its subscribers. Callcentric tracks these numbers in its inventory system and monitors the assignment of these numbers. In these cases, TN validation is the inherent result of Callcentric's assignment of the TN to its subscriber.

If a subscriber wishes to use a TN as a caller identity and that TN is not directly managed by Callcentric, then TN validation is necessary. Subscribers are required to either submit documentary evidence and/or complete a proprietary verification process prior to being given the ability to use a TN not directly managed by Callcentric on outbound PSTN calls. On outbound PSTN calls, Callcentric's network only allows customers to use either a TN that Callcentric has assigned to the customer (on-network) or verified numbers; and will only attest to calls placed from on-network or verified numbers (unchecked spoofing is not allowed nor supported).

Mitigation Through Contracts

All subscribers agree to participate in traceback requests (this is part of the Terms and Conditions which users must agree to when creating an account with Callcentric).

During Service

All subscribers can report any suspicious call connected through their account and measures can be set to prevent future calls from the number(s) in question (blacklisting). These features, which are free and available to all customers, include (but are not limited to):

- Inbound call blocking (and/or routing capabilities; *i.e.*, direct to error messages, voicemail, etc.) for specific numbers, number patterns, etc.
- Inbound call blocking (and/or routing capabilities. *i.e.*, direct to error messages, voicemail, etc.) utilizing freely provided third-party caller reputation data.

Callcentric's Network only allows subscribers to place outbound calls using:

- TNs that are directly managed by Callcentric
- TNs that have been verified for use on Callcentric's Network (verification procedures are detailed in the prior section)

Monitor Traffic with Analytics

[REDACTED]

[illegible]

Callcentric will investigate suspicious activity found by its monitoring systems or reported to Callcentric by subscribers or third parties. The investigation could potentially result in opening a traceback request or with Callcentric contacting a subscriber to correct improper use of the platform, or, if the subscriber does not respond or comply, to block their use of the platform.

For all new and renegotiated Callcentric contracts governing the transport of voice calls, Callcentric will use best efforts to contractually require Callcentric's subscribers to cooperate in traceback investigations by identifying the upstream provider from which the suspected illegal robocall entered our network.

Blocking

Callcentric will implement Do Not Originate requests it receives from the ITG. If Callcentric's monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, Callcentric will take appropriate action which may include suspending or terminating the subscriber's use of Callcentric's network. Callcentric will cooperate with Investigative Bodies (provide a single point of contact to address traceback requests from law enforcement, the state attorney general's office, etc.), to the FCC and/or the 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. Callcentric 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, Callcentric 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 Stephen Irwin

I, Stephen Irwin, Vice President of Operations of Callcentric, Inc. ("Callcentric") do hereby certify, under penalty of perjury, the following:

- a. Callcentric has fully implemented STIR/SHAKEN in the IP portions of its network. Callcentric directly signs all its calls. All traffic is signed as "Telengy - 473G." Callcentric uses Neustar's Certified Caller Solution for its in-house STIR/SHAKEN Implementation.
- b. Callcentric's business name and primary address are as follows:

Callcentric, Inc.
11 Broadway – Suite 1015
New York, NY 10004

d. [REDACTED]

- e. None of the persons/entities listed above have had licenses revoked by the FCC or have been subject to FCC enforcement actions.
- f. Callcentric does not have any other business name.
- g. Callcentric has not previously used any other business name.
- h. 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.
- i. Callcentric's role in the call chain is that of a voice service provider with a STIR/SHAKEN implementation obligation to serve end-users.
- j. Callcentric has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- k. Callcentric is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- l. Callcentric's Operator Code Number is 473G.


Stephen Irwin