

Robocall Mitigation Plan

Business Information

Distributed Computing, Inc.
1700 Union Ave.
Suite B
Baltimore, MD 21211

Contact Information

Tom McDonnell
VP Operations
(856) 505-4909
tmcdonnell@ten4.us

Overview

In the Commission's 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;
- "know your upstream provider" procedures;
- ownership information;
- 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 an 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

Distributed Computing, Inc. ("DCI") is a small VSP dedicated to stopping illegal calls from originating in our network and monitoring the calls traversing our network. In compliance with the R&O, DCI 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 DCI in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

DCI's KYC program involves obtaining specific subscriber information to which customers must agree before using DCI's services. This KYI program is summarized as follows: All new customers are verified with a combination of electronic and manual verification systems, credit reviews, references from trusted industry members, and previous experiences with customer executives and employees.

Acceptable Use Policy ("AUP")

DCI maintains an AUP that subscribers must agree to before being permitted to use DCI'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 law;
- violating applicable industry-accepted guidelines; and
- using DCI's service to engage in or in connection with fraudulent activities.

DCI's contractual terms with subscribers specify that DCI may take action up to suspension or termination of service for violation of the AUP.

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, DCI provides the following information concerning its upstream voice service carriers:

1. PayG LLC dba SkySwitch Arborcrest 1
295 Madison Ave
New York, NY 10017
Jennifer Nading
Email: Jnading@skyswitch.com
2. CoreDial LLC
751 Arbor Way
Suite 150
Blue Bell, PA 19422
Douglas Fetcher
Phone: 215.297.4400
Email: cdsupport@skyswitch.com
3. Bandwidth Inc.
2230 Bandmate Way
Raleigh, NC 27607
Luke Stowers
Phone: 855.864.7776
Email: lstowers@bandwidth.com
4. Telnyx LLC
515 N State St
14th Floor
Chicago, IL 60654
Olive Morris
Phone: (312) 945-7420
Email: regulatory@telnyx.com

DCI and its upstream providers have agreed to work together 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 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 DCI and/or obtained by DCI from one of DCI’s underlying carriers for use by the subscriber.

If a subscriber wishes to use a TN as a caller identity and that TN is not directly managed by DCI, 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, DCI will attest calls originated with these TNs.

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

Monitoring With Analytics

DCI works with its upstream carriers to analyze high-volume voice traffic in order to identify and monitor patterns consistent with robocalls. If DCI detects a calling pattern consistent with illegal robocalls, we will identify the party 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 system.

There are no third-party vendors involved in deploying DCI’s analytics.

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, DCI follows certain procedures for 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 unusual 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.

DCI follows Industry Traceback Group (“ITG”)-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, DCI devotes sufficient resources to provide prompt and complete resources to traceback requests. DCI will respond to traceback requests within 24 hours of being notified of same.

Blocking

DCI will implement Do Not Originate requests it receives from the ITG. DCI works with its upstream carriers to block suspicious calls. If DCI and/or its upstream carriers identify suspected robocalling patterns that are confirmed with further investigation, DCI will take appropriate action which may

include suspending or terminating the subscriber's use of DCI's network. DCI will cooperate with Investigative Bodies (provide a single point of contact to address traceback requests from law enforcement including state attorneys general offices), and the FCC, 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. DCI 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, DCI 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 Tom McDonnell

I, Tom McDonnell, Vice President of Operations of Distributed Computing, Inc. ("DCI") do hereby certify, under penalty of perjury, the following:

- a. DCI's business name and primary address are as follows:

Distributed Computing, Inc.
1700 Union Ave.
Suite B
Baltimore, MD 21211

- b. DCI's d/b/a name is Ten4pbx.com.
c. Except as listed above, DCI has not previously used any other business names.
d. 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.
e. The following persons own 10% or more of DCI: Brooke Frank and Scott Klemm, who are also DCI's sole principals. DCI has no affiliates or subsidiaries.
f. DCI's role in the call chain is that of a voice service provider that is exempt from STIR/SHAKEN implementation due to its lack of control over the necessary infrastructure.
g. DCI is not prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
h. DCI has not been subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
i. DCI is not required to, nor does it have, an Operator Code Number.



Tom McDonnell