

Robocall Mitigation Plan

Business Information

DCI Telecom, 100-1500 Morin Street, Montreal, Quebec, Canada, H4L 5M7

Contact Information

Jack Birnbaum President (514) 856-8585 admin@dcitelecom.com

Overview

DCI Telecom 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 WC Docket No. 17-97 (rel. March 17, 2023), DCI submits this robocall mitigation plan (RMP) and certification.

Know Your Customer ("KYC")

DCI's KYC program involves obtaining specific subscriber information to which customers must agree before using DCI's services. This KYC 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. In addition, most of our customers have been with DCI for more than 10 years.

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.

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. Voxbeam Telecommunications Inc.
6314 Kingspointe Pkwy Suite 1, Orlando Fl 32819
Steve Kay, clcc@voxbeam.com

2. DIDWW Ireland Limited
10/13 Thomas Street, The Digital Hub, Dublin, Ireland
Ligita Chochlova, legal@didww.com

3. Anveo Inc.
148 East Street Road #107, Feasterville, PA 19053
Ivan Chukhryaev, compliance@anveo.com

4. IDT Telecom Inc.
13034 SE 206TH PL Kent WA 98031
Anthony Davidson, Anthony.Davidson@idt.net

5. QuestBlue Systems Inc.
1947 Evans Rd Cary NC 27513
Kevin Masse, carriersupport@questblue.com

6. DID Logic Inc.
906 W. 2nd Ave STE 100, Spokane WA 99201
Nikita Malyshev, carrierrelations@didlogic.com

DCI and its upstream providers 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 or CLECs for use by the subscriber. 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. This 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.

Blocking

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.

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.