

Robocall Mitigation Plan

Business Information

Telcan Networks Inc
1712 Pioneer Ave Suite 500
Cheyenne, WY 82001

Contact Information

Zuly Ortegon
Vendor and Carrier Management
6472585271
zuly.ortegon@telcan.net

Overview

In the Commission's recent release, *Call Authentication Trust Anchor*, Sixth Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd. 2573 (2023) ("R&O"), it is stated that all voice service providers ("VSPs") must file robocall mitigation plans ("RMPs") that, among other things, outline "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";
- 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

Telcan Networks Inc. ("Telcan Networks") is a small VSP dedicated to stopping illegal calls from traversing the network and monitoring the calls coming into our network.

As certified in the FCC's Robocall Mitigation Database, Telcan Networks has fully implemented STIR/SHAKEN. In compliance with the R&O, Telcan Networks submits this RMP and certification.

Know Your Customer ("KYC")

Telcan Networks utilizes KYC procedures during onboarding to verify business identity and contact information, enforce its strict Terms of Service that prohibit illegal robocalling, and leverage STIR/SHAKEN implementation to ensure Telcan Networks knows who is using its network and prevent the unauthorized use of Caller IDs.

New Telcan Networks subscribers must provide name, telephone number, email address, and country. Subscribers putting money onto the Telcan Networks platform ("platform"), a requirement in order to place outbound PSTN calls, must also provide their credit card number and associated information.

New subscribers have their outbound calls rate-limited to one per second, and human contact via phone call or in-person is required in order to increase that rate. New subscribers placing outbound calls can only use Caller IDs which have been purchased through our platform or ones validated through automated-number-validation voice call. All pay-by-card subscribers have limits placed on the number of payments they may make per day and the size of those payments. Both are kept low unless we have had human contact with the customer via phone call or in-person. Pay-by-invoice is allowed only for subscribers who we know well, with human contact via phone call or in-person at the very least, and credit and associated checks having taken place.

Human contact via phone call or in-person is required in order for new subscribers to gain access to the Telcan Networks platform ("platform") to make outbound calls. Subscribers deposit money into the platform via pay by invoice, which is a requirement before a subscriber can place outbound PSTN calls. A subscriber must provide payment through one of the following methods:

1. by phone, calling our toll-free number.
2. by check via mail.
3. online via our payment site.
4. through autopay by filling out our ACH form and providing the required information.

Telcan Networks is a small company, and we have a small number of customers. As a result, We know our customers and understand their use cases.

Know Your Upstream Providers

In accordance with the Commission's directive in *Advanced Methods to Target and Eliminate Unlawful Robocalls*, and *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, 38 FCC Rcd 5404 (2023), at ¶¶ 49-51, Telcan Networks provides the following information concerning its upstream voice service carrier.

Telcan Networks has one upstream provider from which it receives voice traffic:

Business Telecommunications Services, Inc. dba BTS
2620 SW 27 Avenue
Miami FL 33133
David Vila Olloqui
dvila@bts.io

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

Acceptable Use Policy ("AUP")

Telcan Networks maintains an AUP that subscribers must agree to before being permitted to use Telcan Networks' software and services. Among other things, the AUP prohibits:

- using Telcan Networks' service or devices in any way that is illegal, fraudulent, improper or inappropriate;
- using any automated means to manipulate Telcan Networks' service;
- using Telcan Networks' service to violate any law, rule, regulation or any third party's intellectual property or personal rights;
- transmitting any unlawful, harmful, threatening, abusive, libelous, vulgar, obscene, profane, hateful, or otherwise objectionable information; and
- making illegal robocalls.

Violation of the AUP will result in immediate suspension and/or termination of Telcan Networks' services.

Telephone Number Authorization

New subscribers placing outbound calls can only use Caller IDs which have been purchased through our platform or ones verified through automated-number-validation voice call. Subscribers can sign a form allowing them to use Caller IDs not purchased through our platform or verified by validation call for outbound calls, functionality that is restricted to customers with whom we've had human contact by phone call or in-person. This form:

- prohibits the sending of outbound traffic via the PSTN with Caller IDs not owned by the customer or the customer's subscribers; and
- states that, if Telcan Networks receives notice that the Customer's outbound calls through our platform are deemed to be spam, Telcan Networks has the right to disconnect the service immediately and without notice.

Analytics for Monitoring Traffic

We continuously monitor outbound call traffic for suspicious patterns through Traffic Analysis and Monitoring, are committed to a Timely Response to all legitimate Traceback Requests from industry partners and law enforcement, and provide Full Cooperation with investigations by sharing relevant information and call records.

If a calling pattern consistent with illegal robocalls is detected, we identify the party who is using our network to originate those calls and 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 Telcan Networks' analytics.

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, Telcan Networks' 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.

Telcan Networks follows Industry Traceback Group (“ITG”)-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, Telcan Networks will devote sufficient resources to provide prompt and complete resources to traceback requests. Telcan Networks commits to responding to traceback requests fully within 24 hours.

Blocking

Telcan Networks will promptly respond to Do Not Originate requests it receives from ITG. Telcan Networks has mechanisms to automatically block suspicious calls using internal analytics. If Telcan Networks’ monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, Telcan Networks will take appropriate action which may include suspending or terminating the subscriber’s use of Telcan Networks’ network. Telcan Networks will cooperate with investigative bodies (provide a single point of contact to address traceback requests from law enforcement including state attorneys general offices), to the FCC, and/or ITG; as well as documenting requests and actions taken in response thereto.

Plan Updates

This plan, along with industry best practices, will evolve to response to the dynamic nature of mitigating illegal robocalling. Telcan Networks will monitor industry best practices and continuously improve our internal processes to ensure this plan, and our system adapts to this ever-changing issue.

In the event of any material change to this plan, Telcan Networks 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 Mamoon Rashid

I, Mamoon Rashid, President of Telcan Networks, do hereby certify, under penalty of perjury, the following:

- (1) Telcan Networks has fully implemented STIR/SHAKEN in the IP portions of its network.
- (1) Telcan Networks' Business name and primary address are as follows:

Telcan Networks Inc
1712 Pioneer Ave Suite 500
Cheyenne, WY 82001
- (2) Telcan Networks has no other business names in use.
- (3) Telcan Networks has not previously used any other business name.
- (4) 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.
- (5) The following persons/entities own more than 10% of Telcan Networks each: Mamoon Rashid, Siva Sanmuga.
- (6) The following persons exercise management and control over Telcan Networks: Mamoon Rashid, Siva Sanmuga.
- (7) Telcan Networks has the following affiliates: Telcan Inc. (Ontario, Canada), Callture Inc. (Ontario, Canada).
- (8) None of the persons/entities in items 5 – 7 above have had any licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding.
- (9) Telcan Networks' role in the call chain is that of a voice service provider with a STIR/SHAKEN implementation obligation serving end-users.
- (10) Telcan Networks has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (11) Telcan Networks is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- (12) Telcan Networks' Operating Company Number is 971L.

Mamoon Rashid

Mamoon Rashid

12/09/2025