

Robocall Mitigation Plan

Business Information

ACP CreativIT d/b/a TLX Communications
851 Commerce Court
Buffalo Grove, IL 60089

Contact Information

Linda Dobinson
Director of Operations
218.740.2815
linda.dobinson@tlxpro.com

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 (released March 17, 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 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

ACP CreativIT d/b/a TLX Communications ("ACP") is a small VSP dedicated to stopping illegal calls from originating in our network and monitoring the calls coming into our network. ACP is a "pure reseller" that has no control over the infrastructure necessary to implement STIR/SHAKEN. As such, ACP was previously exempt from the FCC's STIR/SHAKEN rules. The R&O requires that pure resellers such as ACP now file RMPs. This document delineates ACP's RMP. Because ACP does not have access to the necessary infrastructure, it relies on its upstream carrier to assist in robocall mitigation. As delineated herein, ACP works closely with its upstream provider to carry out the required mitigation functions.

Know Your Customer

The identification of a subscriber in the STIR/SHAKEN ecosystem is tied to a telephone number-based caller identity associated with that subscriber.

New Subscribers

ACP only sells services to verified business customers. Subscribers provide, as needed based on the product or service entered into, their name, email address, credit card information and contact phone number to ACP. If necessary, ACP is able to communicate with its underlying network to identify a customer.

Acceptable Use Policy

ACP maintains an Acceptable Use Policy ("AUP") that subscribers must agree to before being permitted to use ACP's network. The AUP is here: <https://www.citon.com/wp-content/uploads/2023/01/AUP.pdf>

ACP's AUP specifies that ACP may take action, including suspension or termination of service, for violation of same.

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, ACP provides the following information concerning its upstream voice service carrier. ACP's upstream provider is:

Nextera Communications
325 1st St W
Duluth, MN 55802
Becky Parker
bparker@nextera.net

ACP and its upstream provider have no contractual provisions regarding robocall mitigation. But, ACP and its upstream provider work together to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests. ACP's upstream provider is listed as STIR/SHAKEN compliant in the Robocall Mitigation Database.

Analytics for Monitoring Traffic

ACP works with its upstream provider to identify behaviors which indicate illegal call activity. Examples of calling patterns monitored:

- anomalies in cost generated by calls from a single customer;
- multiple overlapping calls on the same account is a risk of not having a single subscriber using the service;
- velocity on initiate calls (synchron intervals, quick dialing back-to-back calls);
- recent volumes (last 60 min) vs weekly trends;
- number of unique destination numbers in a time frame (total account level);
- number of unique source numbers in a time frame (total and account level); and

- anomalies in call duration distribution (most calls having similar duration is not representative for residential service usage).

No third-party entities are involved in deploying ACP's analytics.

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, ACP works with its upstream provider to follow 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 particular use case and validate that the activity belongs to that subscriber.

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

ACP works with its upstream provider to investigate suspicious activity found by the carrier's monitoring systems or reported to ACP by subscribers or third parties. The investigation could potentially result in opening a traceback request or with ACP contacting a subscriber to correct improper use of the applicable platform, or, if the subscriber does not respond or comply, to notify its upstream provider to block their use of the platform.

Blocking

ACP will implement Do Not Originate requests it receives from the ITG. ACP's upstream provider has mechanisms to automatically block suspicious calls using internal analytics. If ACP and/or its upstream carrier identifies suspected robocalling patterns that are confirmed with further investigation, ACP will take appropriate action which may include suspending or terminating the subscriber's use of ACP's service. ACP will cooperate with Investigative Bodies (provide a single point of contact to address traceback requests from law enforcement (including the state attorneys general offices), 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 response to the dynamic nature of mitigating illegal robocalling. ACP 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, ACP 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 Linda Dobinson

I, Linda Dobinson, Director of Operations of ACP CreativIT d/b/a TLX Communications ("ACP"), do hereby certify, under penalty of perjury, the following:

- a. ACP, by virtue of its status as a "pure reseller" does not have access to the necessary infrastructure to implement STIR/SHAKEN, and therefore has not implemented STIR/SHAKEN in the IP portions of its network.
- b. ACPs Business name and primary address are as follows:

ACP CreativIT d/b/a TLX Communications
851 Commerce Court
Buffalo Grove, IL 60089
- c. Except for TLX Communications. ACP has no other business names in use related to its voice service provider business.
- d. ACP 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. ACP's role in the call chain is that of a voice service provider without a STIR/SHAKEN obligation.
- g. The entities with 10% or more ownership interest in ACP are The Zaf Group LLC and Zaf ACP Next Generation LLC. ACP does not have a parent company, subsidiaries, or affiliates.
- h. ACP has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- i. ACP is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- j. ACP is not required to, and does not have, an operator company number.



Linda Dobinson