

Robocall Mitigation Plan

Business Information

LRM-COM, Inc.
6140-K6 South Gun Club Road
Suite 238
Aurora, CO 80016

Contact Information

Sean Monger
CTO
303.590-1502
admin@lrncom.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 (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, 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";
- 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

LRM-COM, Inc. ("LRM") is a small VSP dedicated to stopping illegal calls from traversing the network and monitoring the calls coming into our network. LRM is a "pure reseller" that has no control over the infrastructure necessary to implement STIR/SHAKEN. The R&O requires that pure resellers such as LRM now file RMPs. This document delineates LRM's RMP.

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 LRM in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

LRM's KYC program involves obtaining specific subscriber information when payment is made for services. This process includes collecting such information such as:

- physical business location;
- contact person(s);
- nature of the customer's business.

Acceptable Use Policy ("AUP")

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

LRM's contractual terms with subscribers specify that LRM 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, LRM provides the following information concerning its upstream voice service carrier.

Lumen Technologies, Inc.
100 CenturyLink Drive
Monroe, LA 71203
Philip Linse
303-707-3844
philip.linse@lumen.com

LRM and its upstream provider work together to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests. LRM's upstream provider is listed as STIR/SHAKEN compliant in the Robocall Mitigation Database.

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 LRM and/or obtained by LRM from one of LRM's underlying carriers for use by the subscriber. In most cases, LRM directly manages the TNs used by its subscribers. LRM tracks these numbers in its inventory system and monitors the assignment of these numbers. In these cases, TN validation is the inherent result of LRM'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 LRM, 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, LRM will attest calls originated with these TNs.

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

Call Monitoring Analytics

LRM has a monitoring and reporting system in place to analyze high-volume voice traffic to identify and monitor patterns consistent with robocalls. Our server-based monitoring system alerts us to calling patterns with unusual spikes, traffic patterns, or attempted use of non-validated ANIs to detect patterns consistent with illegal robocalls.

If LRM detects a calling pattern consistent with illegal robocalls, we will identify the party that is using our network to originate those calls 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 network.

The third-party vendor that provides LRM's analytics is Sangoma Carrier Services.

Investigate Suspicious Activity

When traffic analysis indicates the presence of likely illegal robocalling, our 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.

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

Blocking

LRM will implement Do Not Originate requests it receives from the ITG. LRM has mechanisms to automatically block suspicious calls using internal analytics. If LRM's monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, LRM will take appropriate action which may include suspending or terminating the subscriber's use of LRM's network. LRM will cooperate with Investigative Bodies (provide a single point of contact to address traceback requests) including state attorneys general offices, the FCC, and 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. LRM 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, LRM 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 Sean Monger

I, Sean Monger, Chief Technology Officer of LRM-COM, Inc. ("LRM"), do hereby certify, under penalty of perjury, the following:

- a. LRM, 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. LRM's Business name and primary address are as follows:

LRM-COM, Inc.
6140-K6 South Gun Club Road
Suite 238
Aurora, CO 80016

- c. LRM has two d/b/a: Mallcom Networks and Office First Networks.
- d. LRM has previously used the above-referenced d/b/a.
- 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. LRM is 100% owned by Larry Monger. LRM has no parent companies, subsidiaries, or affiliates
- g. LRM's role in the call chain is that of a voice service provider without a STIR/SHAKEN obligation.
- h. LRM has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- i. LRM is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- j. LRM is not required to, nor does it have, an operator company number



Sean Monger 4/5/2024