

Robocall Mitigation Plan

Business Information

Message Logix, Inc.
60 Long Ridge Road, Suite 403
Stamford, CT 06902

Contact Information

T. Gregory Bender
President and CEO
9142208326
support@k12alerts.com

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 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

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

We provide K12 Alerts®, a premiere emergency messaging platform for K-12 schools, colleges, and universities that enables administrators to send real-time emergency messaging to students and faculty/staff.

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

Know Your Customer ("KYC")

New Message Logix subscriber accounts must provide name, telephone number, email address, U.S. based address, and country. Subscribers paying money to access and use the Message Logix platform ("platform"), a requirement in order to place outbound PSTN calls, must provide payment to Message Logix via check, credit card, or electronic payment, and provide their associated information.

New subscriber accounts provide Message Logix with a list of authorized users who will have access to the platform.

New subscribers have their outbound calls rate-limited up to twelve per second, and from time-to-time, Message Logix may adjust these rates. New subscribers placing outbound calls can only use Caller IDs which they are authorized to use.

Human contact via written notice, electronic notice, video conference, or phone call is required in order for new subscribers to gain access to the Message Logix platform ("platform") to make outbound calls. Subscribers must have a paid active account to use the platform. A subscriber must provide payment through one of the following methods:

1. by phone, calling our toll-free number, to pay by credit card.
2. by check via mail.
3. Wire / ACH / electronic payment.

Message Logix is a small company, and we have a small number of customers. As a result, we know our customers and understand their use cases. Our customers are K-12 schools, colleges, and universities wishing to send real-time emergency messages to students, parents, and faculty/staff.

When clients sign up with us, they provide us with a list of authorized caller ID phone numbers for their organization. Before they provide us with a list, we inform them that they are only allowed to use phone numbers associated with their organization, like a school's main phone number. When the client provides us with a list of caller IDs, our Support Team vets the numbers to ensure legitimacy by checking their websites and other publicly available information.

The system is available only to customers who have executed an agreement with Message Logix. Each client account has secure login credentials for each authorized user to access the system and send phone call messages. Customer logins are equipped with two-factor authentication to block any unauthorized access.

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, Message Logix provides the following information concerning its upstream voice service carrier.

Message Logix has one upstream provider from which it receives and sends voice traffic:

Bandwidth
2230 Bandmate Way
Raleigh, NC, USA 27607
Mark Vincent
mvincent@bandwidth.com

Message Logix 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 and sent from Message Logix and will abide by the Commission's STIR/SHAKEN and robocall mitigation rules in all respects when providing voice traffic to Message Logix. Message Logix 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")

Message Logix maintains an [AUP](#) that subscribers must agree to before being permitted to use Message Logix's software and services. Among other things, the AUP prohibits:

- Illegal or Non-Compliant Communications
 - Violating federal or state telecommunications rules, including the Telephone Consumer Protection Act (TCPA) or relevant privacy laws.
 - Sending fraudulent, deceptive, defamatory, or misleading messages.
- Harassing or Abusive Behavior
 - Using the System to threaten, intimidate, or harass any individual.
 - Broadcasting messages that contain discriminatory, hateful, or profane content.
- Unauthorized or Excessive Messaging
 - Sending messages to groups of contacts without proper authorization from your organization.
 - Using the System for personal, political, or promotional/advertising purposes.
 - Generating volumes of calls or messages that disrupt system availability or burden recipients.
- Security Violations
 - Attempting to bypass login security controls or gain unauthorized access to the System. This includes users logging into a profile that they did not have permission to use.
 - Uploading or transmitting malicious content.
 - Permitting unauthorized individuals to use the System, unless necessary (example: emergency/urgent situations).

Analytics for Monitoring Traffic

Message Logix, if contacted or notified, works to detect a calling pattern consistent with illegal robocalls. If such a call is detected, we will identify the party who 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.

No third-party vendors are involved in deploying Message Logix's analytics.

Investigate Suspicious Activity

When investigation and analysis of traffic indicates the presence of likely illegal robocalling, Message Logix's technology team is alerted, which follows the defined procedures on investigating such subscriber accounts.

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;
- investigating if any system issue generates the strange behavior;
- verifying that the call originating path is valid; and
- contacting representatives of the subscriber account to understand the investigated user's particular use case and validate that the activity belongs to that subscriber user.

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

Clients agree to immediately notify Message Logix, Inc. of any unauthorized access and/or use of the system. We will then immediately investigate the behavior through our account logs. We also reserve the right to shut down, refuse service and/or terminate accounts, for any reason, in our sole discretion without prior notice. This includes situations of suspected suspicious activity. Clients may not transfer or share their account credentials with any other person.

Blocking

Message Logix will promptly respond to Do Not Originate requests it receives from ITG. If Message Logix's team identifies suspicious activity after further investigation, Message Logix will take appropriate action which may include suspending or terminating the subscriber account's use of Message Logix's network. Message Logix 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.

When we set up client accounts, the client provides us with a list of Caller IDs that they wish to use as the number that appears to receivers when the client sends out phone call messages. We vet the caller IDs to ensure that the phone number(s) they want to use are legitimate numbers used by their organization.

Plan Updates

This plan, along with industry best practices, will evolve to response to the dynamic nature of mitigating illegal robocalling. Message Logix 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, Message Logix 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 T. Gregory Bender

I, T. Gregory Bender, President and CEO of Message Logix, do hereby certify, under penalty of perjury, the following:

- (1) Message Logix has fully implemented STIR/SHAKEN.
- (1) Message Logix's Business name and primary address are as follows:

Message Logix, Inc.
60 Long Ridge Road, Suite 403
Stamford, CT 06902
- (2) Message Logix has no other business names in use.
- (3) Message Logix 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) T. Gregory Bender is Message Logix's only owner and principal. He has not had any licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding.
- (6) Message Logix has one affiliate: Anonymous Alerts, LLC.
- (7) Message Logix's role in the call chain is that of a voice service provider with a STIR/SHAKEN implementation obligation serving end-users.
- (8) Message Logix has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
- (9) Message Logix is not subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.
- (10) Message Logix's Operating Company Number is 978L.

T. Gregory Bender
T. Gregory Bender

Date: 7-27-2026