

## Robocall Mitigation Plan

Fastmetrics  
1 Hallidie Plaza Ste 800  
San Francisco, CA 94102  
415-778-5100

Contact Information  
Andreas Glocker  
President  
415-778-5103  
[suport@fastmetrics.com](mailto:suport@fastmetrics.com)

Feb 16, 2022

### Overview

The FCC requires that all small voice service providers (“VSPs”) certify in the Robocall Mitigation Database that they have implemented a Robocall Mitigation Plan (“RMP”) to ensure that they are not originating illegal robocalls.

The FCC requires that VSPs develop a RMP that:

- details the reasonable steps taken to avoid originating illegal robocalls;
- demonstrates a commitment to respond to traceback requests to cooperate with investigators and stopping illegal robocalls; and
- is filed in the Robocall Mitigation Database.

The FCC states 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

Fastmetrics is dedicated to stopping illegal calls from originating in our system and monitoring the calls coming into our system. This document delineates Fastmetrics 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 Fastmetrics in which we transmit, originate, and/or terminate calls based on behalf of the subscriber.

Fastmetrics KYC program involves obtaining specific information from its subscribers. This process includes collecting such information such as:

- physical business location;
- contact person(s); and
- nature of customer’s business.

### **Acceptable Use Policy (“AUP”)**

Fastmetrics maintains an AUP that subscribers must agree to before being permitted to use Fastmetrics' system. 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; and
- using Fastmetrics' service to engage in or in connection with fraudulent activities.

Fastmetrics' terms of service with subscribers specify that Fastmetrics may take action up to suspension or termination of service for violation of the AUP.

### **Monitoring**

Fastmetrics works with its upstream carrier Inteliquent to analyze high-volume voice traffic in order to identify and monitor patterns consistent with robocalls. If Fastmetrics detects a calling pattern consistent with illegal robocalls, we will identify the party 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 system.

### **Investigate Suspicious Activity**

When traffic analysis indicates the presence of likely illegal robocalling, Fastmetrics follows these procedures when 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.

Fastmetrics is familiar with and uses best efforts to follow the Industry Traceback Group (“ITG”)-recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, Fastmetrics will devote sufficient resources to provide prompt and complete resources to traceback requests.

### **Blocking**

Fastmetrics will implement Do Not Originate requests it receives from the ITG. Fastmetrics has procedures to block suspicious calls. If Fastmetrics identifies suspected robocalling patterns that are confirmed with further investigation, Fastmetrics will take appropriate action which may include suspending or terminating the subscriber's use of Fastmetrics' system. Fastmetrics will cooperate with Investigative Bodies (provide a single point of contact to address traceback requests from law

enforcement (including the state attorney general's office), to 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 respond to the dynamic nature of mitigating illegal robocalling. Fastmetrics 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, Fastmetrics 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.