

Robocall Mitigation Plan

Business Information

Emitrr, Inc.
16192 Coastal Highway
Lewes, Delaware 19958

Contact Information

Pulkit Gambhir
Chief Technology
Officer
210-941-4696
hello@emitrr.com

Overview

The FCC requires that, by June 30, 2021, 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 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

Emitrr, Inc. ("Emitrr") is a small VSP dedicated to stopping illegal calls from originating in our network and monitoring the calls coming into our network. This document delineates Emitrr's RMP.

Know Your Customer

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

New Subscribers

All new subscribers go through identity verification protocols which are a mixture of algorithmic check and manual call back. A risk score is developed to ensure the authenticity of a new subscriber. This score checks the identity marker collected during an account registration process. These include but are not limited to: name, email address, credit card information and contact phone number.

These identity markers are validated for accuracy against public and paid tools. All new subscriber activity is monitored as further explained below.

Existing Subscribers

Emitrr requires updates of subscribers' information on all their orders. Each order's identity markers are verified again to ensure the account is not compromised and is being used for its intended purpose.

Acceptable Use Policy

Emitrr maintains an Acceptable Use Policy ("AUP") that subscribers must sign before being permitted to use Emitrr's network. Among other things, this 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 Emitrr's service to engage in or in connection with fraudulent activities.

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

Telephone Number Authorization

A Telephone Number ("TN")-based caller identity is the originating phone number included in call signaling used to identify the 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 Emitrr and/or obtained by Emitrr from one of Emitrr's underlying carriers for use by the subscriber. In most cases, Emitrr directly manages the TNs used by its subscribers. Emitrr tracks these numbers in its inventory system and monitors the assignment of these numbers. In these cases, TN validation is the inherent result of Emitrr'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 Emitrr, 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, Emitrr will attest calls originated with these TNs.

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

Mitigation Through Contracts

All subscribers agree to participate in traceback requests (this is part of the Terms and Conditions which users must agree to when creating an account with us).

During Service

All subscribers can report any suspicious call connected through their account and measures are set to prevent future calls from/to that individual numbers for all subscribers (none routed by the platform from that moment on - blacklisting). These features are:

- VoIP originated calls are signed with subscriber caller ID only after TN authorization (as discussed above); and

- Requiring authentication to initiate any call.

Monitor Traffic with Analytics

Dynamic Traffic Analysis identifies 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 are not representative for residential service usage).

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 particular use case and validate that the activity belongs to that subscriber.

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

Emitrr will investigate suspicious activity found by its monitoring systems or reported to Emitrr by subscribers or third parties. The investigation could potentially result in opening a traceback request or with Emitrr contacting a subscriber to correct improper use of the platform, or, if the subscriber does not respond or comply, to block their use of the platform.

For all new and renegotiated Emitrr contracts governing the transport of voice calls, Emitrr will use best efforts to contractually require Emitrr's subscribers to cooperate in traceback investigations by identifying the upstream provider from which the suspected illegal robocall entered our network.

Blocking

When it is administratively feasible, Emitrr will implement Do Not Originate requests it receives from the ITG. Emitrr has mechanisms to automatically block suspicious calls using internal analytics. If Emitrr's monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, Emitrr will take appropriate action which may include suspending or terminating the subscriber's use of Emitrr's network. Emitrr 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. Emitrr 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, Emitrr 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.