

Robocall Mitigation Plan

Business Information

Newby Technologies
107 49th ST W
Bradenton, FL 3409

Contact Information

Randy Newby
President
941-840-1412
randy@newbytechnologies.com

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

Newby Technologies, LLC is dedicated to stopping illegal calls from originating in our network and monitoring the calls coming into our network. This document delineates Big Fish Voice’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 Newby Technologies, LLC in which we transmit, originate, and/or terminate calls on behalf of the subscriber.

Newby Technologies, LLC’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")

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

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

Monitoring

Newby Technologies, LLC works to detect a calling pattern consistent with illegal robocalls. If such a call is detected 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.

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.

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

Blocking

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