

Giggle Fiber, LLC
Robocall Mitigation Plan
FRN 0023638414

Designated Contact:

Albert Bueno
NOC Supervisor
911 S Primrose Av, Ste E, Monrovia, CA 91016
Email: abueno@gigglefiber.com
Tel: (323) 908-1073
Mob: (626) 500-9289

Introduction

Giggle Fiber, LLC (“we”, “us”, “our”) is a small internet and voice service provider with under 100,000 subscribers and is committed to stopping illegal calls from originating in our network and monitoring the calls coming into our network.

We submit this report on our implementation of our plan to prevent and mitigate the origination of illegal robocalls from our network. We describe below our practices and procedures that are currently in place to achieve the goal of robocall mitigation.

Assessment of Risk

We periodically assess the risks that are associated with our voice business, evaluate the effectiveness of our policies and procedures, and strengthen our capabilities to support the measures outlined in this document. As such, we may modify this document from time to time in response to changes in our business, capabilities and needs.

Giggle Fiber is a service provider offering a variety of calling plans, and our customer profile includes both residential and small business customers who do not originate high volume of calls. To date, we have not received information suggesting that robocalls have originated from our network, and we consider our network to be at very low risk of originating these illegal robocalls.

We do not provide for transit calls, any call not destined to an active number or originating on our switch is rejected, and not passed on to the next carrier, thereby assisting the global community in further mitigation. We only permit analog interface to PBX and those connections are still connected through our hardware devices and are subject to the same limitations as all other calls.

We maintain positive control over the hardware in our network by encrypting the configurations and maintaining complex password schemes for the registration process and not permitting foreign hardware connection to the voice network.

Giggle Fiber, at its inception took these factors into consideration and chose this hardware vs software method specifically to prevent fraud and illegal access to the voice network, even though it prevented implementation of a full-service business class offering. We feel that by limiting the number of concurrent originations, permitting only one trunk per DID, limiting to only hardware-based devices, rejecting transit calls and labeling all originations with A valid P-Asserted Identity, work effectively in mitigating illegal robocalls.

Measures to Identify and Prevent Illegal Robocalls

Due Diligence: Know Your Customers

Giggle Fiber conducts due diligence of new and renewing customers, requiring proof of identity and/or organizing documents, as applicable. Service addresses are verified and confirmed, and physical installation of devices at customer premises is supervised by our own technicians.

All new Customers go through identity verification protocols as follows:

- Residential customers are required to provide proof of identity and service/billing address.
- For small and medium business customers, we use best efforts to confirm their identity by collecting information, which may include the following: physical business location, contact person(s), state or country of incorporation, federal tax ID, and understanding the nature of the customer's business including if/how they will employ auto-dialers or other robocall style tools in the conduct of their business.
- We currently do not cater to large enterprises, call centers, wholesale customers and we do not have foreign-based customers.

We regularly update customer information in our system; each contact with end users is documented by our in-house customer service representatives and serves as opportunity to confirm/validate customer information whenever an end user calls into our customer service number.

Acceptable Use Policy (AUP)

In addition to incorporating robocall mitigation language into our service agreements, terms and conditions, and other documents where applicable, we have in place an Acceptable Use Policy prohibiting the use of our services to conduct illicit or fraudulent activities, including making illegal robocalls. In addition, this AUP prohibits the following:

- 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 standards
- Using Giggle Fiber's network or service to engage in or in connection with fraudulent activities.

Our terms and conditions specify the actions we may take against end users violating this AUP, and penalty includes suspension and/or termination of service.

Contractual Agreements as a Mitigation Tool

- In addition to the mitigation language in our terms and conditions, our customers agree to participate in traceback requests.
- We deal entirely with vendors and service providers who have already certified as to their compliance to the Robocall Mitigation requirements and are listed 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 the caller for screening purposes that is uniquely associated with the customer. A customer is permitted to use a TN as a caller identity if a TN is directly managed by us and/or obtained by us from one of our underlying carriers for use by the customer. In ALL cases, we directly manage the TNs used by our customers. We track these numbers in its inventory system and monitor the assignment of these numbers. TN validation is the inherent result of the assignment of the TN to our customer.

We do not permit numbers not directly managed by us. Even if the numbers are hosted by our underlying carrier, we still maintain control and inventory status over that number via the switch. We do not permit unvalidated DID’s to register on our switch.

When originating a call, we check the calling party number against our inventory and will not originate the call unless the calling party number is a TN that has been properly validated.

As of this filing, Giggle Fiber has completed the implementation of its STIR/SHAKEN protocols and is fully compliant.

Monitoring and Analytics

We conduct traffic analysis to identify patterns indicative of illegal call activity, such as intermittent bursts of high activity, suspiciously low call completion rates/short call times, and evidence of systematic calling, or “war dialing.” Abnormally high-volume call patterns from a commercial customer are also timely investigated as it is a common sign of illegal robocalling.

Cooperation with Law Enforcement and Industry Body

We designated a single point of contact to address traceback requests from law enforcement, the FCC, or the Industry Traceback Group (“ITG”); as well as to document requests & actions taken in response thereto.

We will implement Do Not Originate requests that we receive from the ITG. We have mechanisms to automatically block suspicious calls using internal analytics. In the event that our monitoring systems identify suspected robocalling patterns that are confirmed with further investigation, we will take appropriate action which may include suspending or terminating the customer’s use of our network and services.

Giggle Fiber, LLC certifies that we have the ability and agrees to provide for traceback requests and as always, agrees to fully cooperate with any empowered authorities request to assist in abatement.

Giggle Fiber, LLC has completed the stir/shaken certification process, and is now compliant with STIR/SHAKEN.

Date: January 13, 2026