



Robocall Mitigation Program

--

Version Number: 1.0

Version Date: February 2024

Version History

Version Number	Implemented By	Revision Date	Approved By	Approval Date	Description of Change
1.0	Corey Turner	02/21/2024	Nate Peace	02/21/2024	Updating documentation to reflect new FCC compliance regulations

Table of Contents

Overview	4
Scope and Goals	4
Roles and Responsibilities	5
STIR/SHAKEN Implementation	5
Robocall Mitigation Program	5

Overview

Pursuant to section § 64.6305 of the Federal Communications Commission's ("Commission's") rules, Revation Systems, Inc (DBA "LinkLive") provides this document addressing its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls.

LinkLive provides VoIP phone services to its business customers and is considered a voice service provider under section § 64.6305. Bandwidth is LinkLive's underlying voice service provider. LinkLive relies on procedures, policies, and safeguards implemented by Bandwidth to ensure that LinkLive's customers are sufficiently protected against illegal robocalls and spoofing activities.

LinkLive has fully implemented the STIR/SHAKEN authentication framework, as indicated in the Robocall Mitigation Database.

All calls that originate on LinkLive's network are subject to the Robocall Mitigation Program set forth below.

LinkLive has not been prohibited from filing in the Robocall Mitigation Database by the Commission.

LinkLive has never been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program.

Scope and Goals

This procedure outlines LinkLive's compliance with FTC Ruling § 64.6305 Robocall Mitigation and Certification. The goals of this procedure are as follows:

- Define methods used by LinkLive to implement STIR/SHAKEN.
- Outline LinkLive's Robocall Mitigation Program

Roles and Responsibilities

Role	Responsibilities
Chief Information Security Officer (CISO) and/or designee	The CISO is responsible for, but not limited to, the following activities: • Revisions, implementation, workforce education, interpretation, and enforcement of this procedure. • Ensure that mechanisms/methods utilized for implementing STIR/SHAKEN are in place. • Outline and define the Robocall Mitigation Program.
Management	Management will provide support through active enforcement, funding, and resources needed to meet the requirements of this procedure.

STIR/SHAKEN Implementation

Bandwidth, LinkLive's underlying voice service provider, has fully implemented STIR/SHAKEN and utilizes it to authenticate all LinkLive calls, providing A-Level Attestation for all inbound and outbound communication.

Robocall Mitigation Program

LinkLive relies on Bandwidth as its SIP provider to provide STIR/SHAKEN authentication in compliance with FCC regulations.

In accordance with 47 CFR 64.6305(d)(2)(ii), (e)(2)(ii), and (f)(2)(ii), LinkLive takes the following reasonable steps to avoid originating, carrying, or processing illegal robocall traffic:

- Whitelist on IP addresses to communicate to our trunk in both directions. Typically, this is only for connectivity to our PSTN carriers.
- We only listen on specifically configured port numbers for voice trunks, not necessarily well-known port numbers.
- Client admin and user do not have access to modify voice trunk. Only designated LinkLive admins have full access to voice trunk.
- Only authorized admins have access to the admin site.
- Utilization is monitored as part of billing and usage.
- Limit the number of concurrent calls for each trunk – based on the contracted agreement. The event log is triggered and communicated whenever the maximum concurrent call is reached.

- Restriction for both incoming and outgoing dial digits.
- Restriction on outbound calls per contracted agreement. I.e., no international calls unless it's in the contract.

LinkLive is committed to cooperating with the Commission, law enforcement, and the industry traceback consortium to investigate and stop any illegal robocallers we learn are using our service to originate calls.

LinkLive will respond fully within 24 hours to all traceback requests from the Commission, law enforcement, and the Industry Traceback Group (ITG) and cooperate with such entities in investigating and stopping any robocallers that use its service to carry, process, or originate illegal robocalls.

LinkLive's underlying voice services provider, Bandwidth, is also committed to responding fully and within 24 hours to all traceback requests made by ITG, law enforcement authorities, and government agencies to investigate and address suspected unlawful robocalls originated or passed to Bandwidth. LinkLive has agreed to cooperate with Bandwidth in responding to ITG traceback requests, as detailed above.

LinkLive and Bandwidth are committed to fully complying with the Commission's robocall blocking requirements, and Bandwidth has confirmed that it will block all calls and provider traffic that: (1) are identified in any public notice or order released by the FCC; (2) are substantially similar to the types of traffic identified in any public notice or order released by the Commission; or (3) include a caller ID number or name that is on DNO list issued by ITG. Momentum also blocks the traffic of all foreign providers and gateway providers not registered in the Robocall Mitigation Database.

Customer & Upstream Vetting

To prevent the origination, routing, and termination of illegal robocalls throughout our network, LinkLive shall apply the following procedures to all new and existing business relationships:

All potential customers must provide:

- Legal business name and physical address
- Principal business type and industry
- Valid business registration documents
- Tax identification number

- Authorized point of contact information
- Intended call traffic patterns and volumes
- Intended use cases for voice services

All customers will be subject to ongoing monitoring, including but not limited to the following:

- Quarterly reviews of calling patterns
- Regular verification of contact information
- Annual re-certification or compliance procedures
- Periodic audits of consent records for marketing calls
- Continuous monitoring for suspicious calling patterns

Prior to establishing a connection with upstream providers, LinkLive will verify:

- Provider's registration in the FCC Robocall Mitigation Database
- Implementation of STIR/SHAKEN or equivalent call authentication
- Provider's own robocall mitigation procedures
- History of regulatory compliance
- Industry reputation and references

Upstream provider relationships will be monitored through:

- Monthly analysis of traffic patterns and anomalies
- Tracking of consumer complaints related to traffic from provider
- Regular verification of continued RMD registration
- Annual review of provider's updated robocall mitigation procedures
- Documentation of traceback cooperation

Identifying Information

Revation Systems, Inc. (DBA LinkLive)
535 Mission Street, San Francisco, CA 94105

Upstream Provider Contact

- **Vendor:** Bandwidth
- **Contact:** Trevor Parker
- **Phone:** 919-726-6428
- **Email:** tparker@bandwidth.com
- **Address:** 2021 Edwards Mill Road, Raleigh, SC 27607

Compliance Contact

- **Name:** Corey Turner
- **Title:** Information Systems Security Manager
- **Department:** Operations
- **Phone:** 507-366-8240
- **Email:** cturner@linklive.ai