

Leap Telecom, LLC
Robocall Mitigation Program
V.1 February 2024

STIR/SHAKEN Implementation

Leap Telecom, LLC (“Leap” or “Company”) is an innovative global VoIP service provider (“VSP”) offering secure, scalable solutions for small businesses to carrier resellers. Leap’s global IP network contains multiple redundant Network Operation Centers, offering 100% uptime. Leap has fully implemented STIR/SHAKEN and on October 15, 2021 submitted its certification that all voice traffic originating on its network is authenticated with STIR/SHAKEN consistent with 47 C.F.R. §64.6301(a). Leap Telecom, LLC is a “Voice Service Provider”. As such, Leap Telecom submits this Robocall Mitigation Program (“RMP”) and certification into the Robocall Mitigation Database. This RMP includes the obligations outlined in the Commission’s recent release, *In the Matter of Call Authentication Trust Anchor, Sixth Report and Order and Further Notice of Proposed Rulemaking*, WC Docket No. 17-97 (rel. March 17, 2023).

ROBOCALL MITIGATION

Background

The FCC Order requires that a RMP include the following affirmative obligations for voice service providers:

- Outline reasonable steps VSP has taken to avoid originating illegal robocall traffic;
- Commitment to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the Industry Traceback Consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls;
- Know Your Customer procedures;
- Describe any call analytics system used to identify and block illegal traffic

Traceback

Leap is committed to ensuring its network is not utilized for the origination or terminating of illegal robocalls. Leap commits to responding fully and within twenty-four (24) hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperating with such entities in investigating and stopping any illegal robocallers that use its service to originate calls. Leap Telecom is also actively involved in the ITG Traceback Group.

Leap utilizes multiple reports that are built into their systems that will display calls related to the DNO and DNC lists statistically by customer. The results of this analysis may result in tickets being opened to the customer. In extreme cases the Company may suspend the customer’s ability to transit traffic across the network until the issue can be thoroughly investigated and resolved directly with the customer.

The following describes the procedures Leap adheres to when conducting the investigations and to determine if the calls are actually illegal robocalls:

Leap has a multi-step approach designed to efficiently and effectively identify, analyze, and mitigate suspected illegal robocalls. This process leverages various tools and criteria to ensure compliance with legal standards and protect consumers from fraudulent and unwanted calls. This includes statistical analysis, velocity analysis and other computational methods for detection and mitigation of illegal robocalls :

Receipt of Traceback Request

- **Notification:** Leap receives a traceback request from the ITG, FCC, or law enforcement. This notification usually provides details about the suspected illegal call(s), including timestamps, originating numbers, and destination numbers.
- **Acknowledgment:** Leap acknowledges receipt of the request and may provide an initial estimate of the investigation timeline.
- **Reporting:** Leap will report back to the ITG or other requesting entity within 24 hours.

Leap provides the following name, title, email address of the individual within Leap that handles robocall mitigation-related issues as well as responding to traceback requests from the FCC, ITG, and law enforcement agencies:

Traceback Contact Information

Name	Title	Email address
Doug Davis	Operations	doug.davis@teliax.com
Jered Morgan	Support Engineer	Jered.morgan@teliax.com
Nick Essex	Tier 2 VoIP Support Engineer	Nick.essex@teliax.com

[Call Blocking/Analytics for Monitoring Traffic:](#)

The Company has implemented its own call analytics to identify unlawful traffic that may originate on its network. These call analytics aid to identify behaviors that are consistent with illegal robocalling. If the Company identifies such calling patterns, it will take appropriate action to address the situation, including blocking such calls. As part of its analysis and monitoring procedures, the Company can utilize a real-time lookup system to detect where the calling number is invalid, unallocated, or on a Do Not Originate (“DNO”). If Leap’s system detects any of these issues, a call will be released and a report is generated that provides the relevant details presented. Leap will then work with the customer to further investigate the issue and bring it to conclusion. Leap also monitors the Robocall Mitigation Database to verify all traffic is from a carrier that has registered in the database.

[Know Your Customer Protocols](#)

Leap Telecom has implemented affirmative, effective measures to prevent new & renewing customers from using its network to originate illegal robocalls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal calls. The Company has implemented Know Your Customer (“KYC”) protocols when onboarding new or renewing customers. Leap Telecom will not provide service if a new customer’s identification cannot be verified. These protocols include, but are not limited to the following:

- Initial Contact: When a new customer applies for a service they are required to provide personal identification information. This typically includes name, address, date of birth, and government-issued identification numbers (e.g., SS# in the U.S., Aadhar in India, or Passport #) of the requesting party or entity
- Document Verification: The customer must submit copies of official documents for verification. Examples include a government-issued ID card, passport, driver's license, utility bills for address verification, and other relevant personal or corporate documents.
- Risk Profiling: Based on information provided, the carrier assesses the risk level of the customer. Factors such as the customer's location, the services they are requesting, and their financial considerations can influence their risk profile.
- Monitoring and Reporting: High-risk customers may be subject to more stringent monitoring of their account activities. This may include but are not limited to periodic reviews with the customer of their traffic, risk profile and analysis.
- Transaction Monitoring: Leap monitor transactions and use patterns for any unusual or suspicious activity that deviates from the customer's typical behavior.
- Update Customer Information: Leap periodically request customers to update their information to keep records current. This process may involve re-verifying identity documents and conducting additional checks for high-risk customers.
- Compliance Checks: Regular checks against local and international watchlists, including those for sanctioned individuals and entities, to ensure compliance with anti-money laundering (AML) and counter-terrorism financing (CTF) regulations.

Validating Customer's Right to Use Telephone Numbers:

Leap Telecom has procedures in place to authenticate the proper use of telephone numbers associated with calls routed over its network. Leap assigns customers numbers that are registered to Leap Telecom, and are assigned from the Company's direct inventory of numbers secured directly from NANPA. Leap does not provide a service where a customer can bring its own phone number from a 3rd party network, but must port-in a number to Leap to gain service.

Acceptable Use Policy

The Company has specific Terms and Conditions within the customer contract to aid its customers to understand the intended and permissible uses of our service, and to prevent exploitation, fraud, and abuse of our calling plans and features. These terms include providing the Company the ability to pause, suspend, or otherwise terminate a customer found to be participating in any illegal activity, including generation of illegal robocalls.

CONCLUSION

The Company submits this Robocall Mitigation Program consistent with FCC Regulations, 47 C.F.R. §64.6305 (a)(1) & (d)(5). Leap Telecom will update its submission in the RMD within 10 business days of any change to the applicable information it must provide in the RMD, including its RMP.