

Robocall Mitigation Plan

Business Information

LIMEBOX Networks, LLC
5 Perina Blvd
Cherry Hill, NJ 08003

Contact Information

Charles Phillips
CTO
856-942-4079 x120
crsvc@limeboxnetworks.com

Overview

In the Commission's 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) ("R&O") it is stated that all voice service providers ("VSPs") must file robocall mitigation plans ("RMPs") that, among other things, outline "reasonable steps" taken to avoid originating illegal robocalls. In addition to the "reasonable steps," the FCC requires that a RMP include know your customer (KYC) procedures, a description of call analytics systems used to identify and block illegal traffic, and whether a third-party vendor is used and if so, the name of the vendor.

The FCC previously stated 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 described in its filing.

Purpose

LIMEBOX Networks (LIMEBOX) is dedicated to combating illegal calls by actively monitoring all call activity, traversing our network, and responding swiftly to mitigate potential issues. As certified in the FCC's Robocall Mitigation Database, LIMEBOX has fully implemented the STIR/SHAKEN framework to enhance call authentication and prevent Caller ID spoofing. In compliance with the FCC's Report and Order (R&O), we submit this Robocall Mitigation Plan (RMP) and certification to affirm our commitment to ensuring network integrity and supporting industry efforts to eliminate unlawful robocalls.

Know Your Customer (KYC)

LIMEBOX is a small, focused Voice Service Provider (VSP) dedicated exclusively to offering IP Communication services. Our customer base consists of long-standing relationships established through referrals from trusted agents. We do not serve retail customers. Our referral-only business model, combined with a rigorous onboarding process, ensures a thorough understanding of each customer's business, use case, intended use of the services we provide, and overarching goals. This approach allows us to:

- Gain deep insight into the unique needs and operations of each customer.
- Tailor our services to align with their specific requirements.
- Maintain a strong, trust-based partnership with all clients.

During the onboarding process, LIMEBOX collects the following information to verify and support our KYC practices:

1. Business identity and ownership details.
2. Contact information for authorized representatives.
3. Intended use of IP Communication services.
4. Compliance documentation as required by regulations.

This comprehensive onboarding ensures a higher standard of service and reinforces our dedication to responsible and ethical operations.

Know Your Upstream Providers

LIMEBOX operates under Master Service Agreements (MSA) with the following upstream providers:

- Inteliquent (Sinch)
1 North Wacker Drive
Suite 2500
Chicago, IL 60606-2825
- Bandwidth.com
2230 Bandmate Way
Raleigh, North Carolina 27607

Acceptable Use Policy (AUP)

LIMEBOX customers operate under master service agreements, including general policies, terms, and conditions mandating compliance with our Acceptable Use Policy (AUP). These agreements ensure that all customers adhere to standard and legitimate business use of our IP-based communication services.

In addition to general usage guidelines, our policies specifically address the following areas:

- Prohibited Activities – Clear restrictions against illegal robocalling, fraud, or other abusive practices.

- Compliance Requirements – Adherence to applicable laws, regulations, and industry standards, including those set by the FCC and other regulatory bodies.
- Network Integrity – Prohibition of activities compromising network security, performance, or reliability.
- Caller ID Policies – Ensuring customers use authorized and accurate Caller ID information.

By enforcing these policies, LIMEBOX maintains a secure and reliable network while promoting ethical and lawful usage of its services.

Traffic Monitoring and Call Analytics

At LIMEBOX, we proactively monitor all voice traffic originating from our network to prevent the origination of illegal robocalls. Our system analyzes call patterns such as short-duration dialing, failure type trends, and other indicators associated with fraudulent activities.

Upon identifying suspicious calls, we promptly investigate to determine whether unlawful calls were attempted. If evidence of such activity is found. This may include:

- Conducting traceback investigations to trace the source of the call.
- Verifying that the originating subscriber owns or is authorized to use the Caller ID number.
- Suspending or terminating the offending party's ability to originate calls on our network.

Our call analytics and monitoring are conducted entirely in-house, with no involvement from third-party vendors, ensuring the integrity and security of our network operations.

Taking Action

LIMEBOX swiftly and decisively addresses suspected unlawful calling activities. We promptly respond to Do Not Originate requests received from the Industry Traceback Group (ITG) and rely on our internal analytics to automatically block suspicious calls.

When our monitoring systems detect robocalling patterns, we confirm these findings through further investigation. If confirmed, appropriate actions may include:

- Suspending or terminating the subscriber's access to LIMEBOX's network.
- Blocking calls that exceed established calls-per-minute/second thresholds.
- Blocking calls that fail to use an authorized Caller ID.

LIMEBOX is committed to full cooperation with investigative bodies, including the FCC and the ITG, to address unlawful calling practices. We maintain thorough documentation of requests and actions taken in response, ensuring accountability and transparency in combating fraudulent and illegal robocalling activities.

Plan Updates

LIMEBOX recognizes that combating illegal robocalling requires continuous adaptation. This plan and our adherence to industry best practices will evolve to address the dynamic nature of robocall mitigation. We are committed to monitoring and implementing industry advancements to enhance our internal processes and ensure our systems remain effective against emerging challenges. In the event of any material changes to this plan:

- LIMEBOX will promptly republish the updated plan to employees, consultants, and contractors.
- The updated plan will also be filed with the FCC Robocall Mitigation Database to maintain compliance and transparency.

Our ongoing efforts underscore our dedication to staying ahead in the fight against illegal robocalls.

Certification of Charles Phillips

I, Charles Phillips, the CTO of LIMEBOX Networks, do hereby certify, under penalty of perjury, the following:

1. LIMEBOX has fully implemented STIR/SHAKEN in the IP portions of its network.
2. LIMEBOX is committed to responding within 24 hours to any and all requests.
3. LIMEBOX's Business name and primary address are as follows:
LIMEBOX Networks, LLC
5 Perina Blvd.
Cherry Hill, NJ 08003
4. LIMEBOX has no other business names in use.
5. LIMEBOX has not previously used any other business name.
6. The name, title, business address, telephone number, and email address of the individual responsible for addressing robocall-related issues is listed in the attached robocall mitigation plan.
7. The following is the list of LIMEBOX's owners with more than 10% interest:
 - Louis Bucelli
 - Charles Phillips
8. None of the persons in item 7 above have had their licenses denied/revoked by the FCC or been subject to an FCC enforcement proceeding.
9. LIMEBOX's role in the call chain is that of a voice service provider with a STIR/SHAKEN implementation obligation serving end users.
10. LIMEBOX has not been prohibited from filing in the Robocall Mitigation Database due to an enforcement action.
10. LIMEBOX is not subject to a commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.



Charles Phillips