



Robocall Mitigation Program Description

Overview

The FCC requires that all 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 an 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 an 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

Internos Group, a VSP, utilizing Bandwidth.com for all voice services, is committed to comply with the FCC's requirements for mitigating illegal robocalls. Internos Group is dedicated to stopping illegal calls from originating in our networks and monitoring the calls traversing our networks.

Internos Group works with our upstream vendor, Bandwidth.com, and has fully implemented the STIR/SHAKEN framework across its IP-based voice network to ensure that caller ID information is authenticated and helps prevent robocalls.

Know Your Customer (“KYC”)

Internos Group’s KYC program involves obtaining and validating specific subscriber information when the subscriber is onboarded. This process includes collecting and validating such information as:

- Contact Person(s)
- Physical Location Address
- Business Information
 - Corporate Name
 - Entity Type
 - Employer Identification Number
 - Business website and Social Media Handles
 - Industry Specific License and Permits (When Applicable)
 - Request Business References

Internos Group utilises this information to perform a comprehensive assessment of the subscriber’s business and reputation. This analysis includes:



- Contact Information and Physical Address
 - Verification of contact details and physical address is conducted through onsite visits or by leveraging tools such as Google Maps (Street View) to confirm their accuracy and ensure operations align with disclosures.
- Business Registration and Licensing
 - Official government databases are used to search by name and location, verifying the business registration details and legal identity.
 - Appropriate regulatory agencies are consulted to confirm that the company holds all required industry-specific licences and permits.
- Business Reputation
 - Independent review sites, including the Better Business Bureau (BBB), Trustpilot, Google Reviews, and Clutch.co, are checked for unbiased customer reviews and complaints.
- Online Presence
 - The business's website and social media accounts are reviewed for professionalism, visibility of contact details, and insights into the company's history.
- Business References
 - Business references are contacted, and testimonials are solicited to validate ongoing activities.

Once all business information is reasonably validated and the risk associated with the subscriber's account is assessed as low, the account is approved and the customer onboarding process proceeds.

Additionally, Internos Group conducts an annual review. Businesses are requested to re-validate the originally provided information and a similar analysis is performed to ensure there has been no significant increase in the overall risk associated with providing voice services to the subscriber.

Acceptable Use Policy ("AUP")

Internos Group maintains an AUP that subscribers must accept and sign before being permitted to use Internos Groups' systems and services. The AUP is incorporated with Internos Group's Master Service Agreement ("MSA") and Services Guide ("SG"). The AUP as incorporated into the MSA and SG prohibits such things as:

- Providing false identity or falsifying the origin of a message or phone call
- Violating any applicable law or industry-accepted guidelines
- Using Internos Groups' services to engage in or in connection with fraudulent

Monitoring - Traffic Analysis & Industry Collaboration

Internos Group works with bandwidth.com to actively monitor high-risk international destinations and participate in traceback efforts to identify patterns consistent with robocall sources.

If Internos Group identifies and or detects calling patterns consistent with robocalls, we will identify the party and will take appropriate action which 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 the party's ability to originate calls on our systems.



Investigate Suspicious Activity

Upon detecting suspicious activity, Internos Group investigates the recent and past call detail records and notifies the offending party for a legitimate use case. Until Internos Group does not receive the legitimate use case (if any), the account is suspended. If the use case is not considered legitimate, i.e. if the offending party has not responded or has not been able to show its legitimacy, the account is terminated.

We work closely with Bandwidth.com and use best efforts to follow the Industry Traceback Group (“ITG”) recommended best industry practices and cooperates in traceback and trace forward investigations. To allow for timely and comprehensive responses, Internos Group will devote sufficient resources to provide prompt and complete resources to traceback requests.

Blocking

Internos Group will implement Do Not Originate requests it receives periodically from the ITG. Internos Group works with its upstream carrier, bandwidth.com, to block suspicious calls. If Internos Group and/or bandwidth.com identify suspected robocalling patterns that are confirmed with further investigation, Internos Group will take appropriate action which may include suspending or terminating the subscriber’s use of our services.

We will cooperate with the Investigative bodies of the FCC, and/or the ITG; as well as documenting requests & actions taken in response thereto.

Blocking

This plan and industry best practices must evolve to respond to the dynamic nature of mitigating illegal robocalling. Internos Group will monitor industry best practices and continuously improve our internal processes to ensure this plan and our systems adapt to this ever-changing issue.

In the event of any material change to this plan, Internos Group 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.

Contact Information

For inquiries related to this Robocall Mitigation Program, please contact:

Ronny Delgado, Partner

Email: rdelgado@gointernos.com

Phone: (305) 590-5333

