



1801 North Himes Avenue | Tampa, Florida 33607 | 813-232-4887 Fax 813-236-0014 | <http://www.rapidsys.com>

STIR/SHAKEN Robocall Mitigation Plan

RM Contact: Denise Hamilton
Phone: 813-232-4887x150
denise@rseng.net

Rapid Systems Inc. is a Wireless Internet Service, VoIP, Web and DNS hosting provider, serving the central Florida area. We have a clientele of less than 100,000 voice service subscribers. We have partially implemented STIR/SHAKEN by working with our backend provider [REDACTED] to keep abreast of any solutions that must be in place in order to maintain compliance with carrier regulations in lieu of the FCC's requirements.

As of December 2024, Rapid Systems Corporation, nor any of our executives or principals have any history of illegal robocall violations or enforcement actions, and we have not been prohibited from filing a certification in the Robocall Mitigation Database. We use the measures listed below to prevent the transmission of illegal robocalls.

Know your customer

We speak with each of our customers regarding their intentions to utilize our service, and confirm that they will not use the service for any malicious intent. Our voice customers purchase VoIP solutions that are often bundled with a fixed-location broadband service. Therefore, we know these customers and are aware of their businesses and purpose for utilizing the service. The PBX system that our customers use are hosted at our data center in Tampa, Florida as a cloud solution. Our PBX solutions only work with endpoints (IP phones) that we provide. In rare cases, our customers will purchase IP phones that will only work with our service if fully configured and provisioned by Rapid Systems. IP-based access control lists are implemented across all of our PBX systems and network firewalls to limit access and control intrusion across the entire network. We do not offer any form of SIP trunking service ourselves, as we are receiving trunking services through our backend provider [REDACTED]. Any customer making robocalls may have their service terminated under the terms and conditions of our website. <https://www.rapidsys.com/about/terms-of-service/>

Traceback Requests

Rapid Systems has, and will continue to respond fully within 24 hours of any traceback request from the FCC, law enforcement agencies and the industry traceback consortium. We vow to cooperate with these agencies by investigating and stopping any and all illegal robocallers that use our service to originate calls. Our point of contact to handle all traceback requests is:

Dustin Jurman
813-232-4887x103
dustin@rseng.net

AND/OR

Denise Hamilton
813-232-4887x150
denise@rseng.net

AND/OR

abuse@rapidsys.com

If contacted for a traceback request, we will work with our in-house VoIP engineering teams and backend provider [REDACTED] and fully comply to facilitate any necessary data requested.



Robocall Mitigation Program

Rapid Systems assigns correct calling DID(s) to each customer manually upon initiation of service. We also will add CDR records to properly identify businesses who use our service to prevent unintentional call blocking. Our customers do not have the ability to modify or override their outbound/calling DID(s) or CDR, and have no authorization to utilize any DID(s) other than the ones that we provide from our backend provider [REDACTED]. If we and/or our backend provider (Vitelity) detect any sign of network usage patterns consistent with illegal robocalls, or suspect illegal robocalling is taking place, we will immediately identify the party that is originating, terminating or routing these calls, and we will initiate a traceback investigation to determine where the traffic originates, and block and disable the traffic immediately. If the traffic is deemed illegal and/or if it continues to be an issue, Rapid Systems will completely erase the affected PBX equipment and rebuild under a separate IP address. If the traffic is in any way end-user initiated, Rapid Systems will consider termination of the end users VoIP service.

Among other things, our backend provider [REDACTED] parent company [REDACTED] utilizes the following tools to combat illegal robocalls:

- Randomizer: Utilized for customer traffic which is sent to Inteliquent via a Least Cost Routing ("LCR") engine. Based on calling party telephone number analytics, an announcement is played to the calling party that requires the calling party to enter two randomly generated digits to complete the call. If the correct digits are not entered, the call will not proceed (machine generated calls presumably are unable to enter the randomly generated digits).
- Automatic Number Identification ("ANI") Management: Utilized for customer traffic which is sent to [REDACTED] via an LCR engine. ANI Management is used to identify and block originating telephone numbers from sending calls that are believed to be unlawful based on repeat attempts to reach the Inteliquent network.
- Proactive Blocking: Applied to all traffic. Per rules adopted by the Commission, [REDACTED] blocks calls from phone numbers on Do-Not-Originate ("DNO") lists from US Telecom, SOMOS and Neustar. In certain circumstances, [REDACTED] also blocks calls that originate from invalid, unallocated, or unused numbers. [REDACTED] customers may also place certain of the inbound-only telephone numbers they use on the DNO list.
- No Treatment: This treatment is applied to lawful robocalls so that they can complete. Call types eligible for this treatment include debt collections, political calls, surveys, non-profit, emergency notifications, and other lawful call types.
- Whitelist: [REDACTED] "whitelists" telephone numbers that it knows originate legitimate calls (i.e., are valid). For example, some law enforcement and emergency calls originate from numbers where the entire telephone number is composed of zeroes. While appearing to be an unallocated number, [REDACTED] knows based on call history that the call is originating from a federal law enforcement agency or a local police department. Such calls also originate from older or misconfigured PBXs (private branch exchanges). Another example would be collection calls by Bank of America or calls to known numbers used for emergency county-wide or municipal alerts.

Knowledge of Upstream Providers

All Rapid Systems VoIP calls are carried by [REDACTED], who are fully registered in the Robocall Mitigation Database under [REDACTED], and are maintaining complete STIR/SHAKEN implementation. We have received written assurances from their officials that they have, and will continue to sign calls at A-Level attestation whilst we maintain communication through their provided DID's and are properly registered with the Robocall Mitigation Database



1801 North Himes Avenue | Tampa, Florida 33607 | 813-232-4887 Fax 813-236-0014 | <http://www.rapidsys.com>

STIR/SHAKEN Robocall Mitigation Plan

and are compliant and followin the rules and regulations set forth by the FCC. Rapid Systems will work hand-in-hand with [REDACTED] in any event of an illegal robocall discovery and cooperate fully when receiving traceback requests.

Additional steps Rapid Systems takes to fortify our service include:

- Maintaining a dedicated primary firewall over our entire network which is limited to allow VoIP traffic only through specific IP ranges fro [REDACTED]
- Utilizing secondary firewall and intrusion detection solutions from our PBX provider to further enhance security on the PBX system itself.
- Processing weekly software/firmware updates across all of our PBX systems.
- Processing emergency updates within a moment's notice across all of our PBX systems.
- All of our clients are individually reviewed by our VoIP engineer prior to installation, confirming they will utilize our service for general business or personal use, and NOT to engage in robocalling activities.
- We are actively reviewing any issues pertaining to suspicious traffic broadcasted from any of our PBX systems, and in the event there are complications, we are contacting the client directly to review and determine the root cause. We will immediately disable/block any malicious IP address sending this traffic directly from our primary firewall until the issue is completely resolved.

The VoIP division of our service is a relatively small branch of our company, and consists of mostly local businesses and residential services. The overall service does not have a significant traffic flow at any given time.

10 Day Update Commitment

If at any time Rapid Systems is aware of any changes or updates to this plan, we are fully affirming to commit to updating our Robocall Mitigation Database filing within 10 days of implementation.

Regards,
Denise Hamilton
VP, CFO