

Robocall Mitigation Program Certification for Rainbow Communications, LLC

Rainbow Communications, LLC hereby certifies that we have implemented the STIR/SHAKEN authentication framework on a portion of our network, and the remainder of the calls that originate on our network are subject to a robocall mitigation program described below.

Our prior certification has not been removed by Commission action, and we have not been prohibited from filing in the RMD by the Commission. We have no foreign ownership. Rainbow Communications, LLC is a cooperative with a wholly owned subsidiary of Rainbow Telecommunications, Inc. Our general manager/CEO is Jason Smith.

Traceback

We respond to all traceback requests from the Federal Communications Commission, law enforcement, and the registered traceback consortium and cooperate with such entities in investigating and stopping any illegal robocallers that use our service to originate calls, and we commit to continuing to do so within 24 hours.

STIR/SHAKEN

We are a voice service provider that is compliant with STIR/SHAKEN requirements. The portion of the voice traffic that originates on our network that is not subject to STIR/SHAKEN is subject to the robocall mitigation program described below. Rainbow has taken the following specific reasonable steps to avoid originating illegal robocall traffic as part of its robocall mitigation program.

Robocall Mitigation Program

We use TNS Call Guardian analytics technologies and services to monitor traffic on our network and identify potentially unlawful call origination activity. The TNS Call Guardian analytics technologies and services analyzes call patterns from telephone numbers registered to our Service Profile Identifier (SPIDS). While analyzing the call patterns TNS assigns a reputation score to each number and provides a report of all numbers with a negative reputation score to our Network Manager for further investigation.

In addition to TNS, we also use our engineering firm, RVW Inc., to analyze call patterns and detect suspicious activity. RVW's process for robocall mitigations is as follows: our switch pushes files to an ftp site that RVW can access twice a day at roughly 1:00 a.m. CDT and 1:00 p.m. CDT.

RVW downloads the files around 8:00 a.m. CDT each business day. Weekend and holiday files are processed on the next business day.

Each business day, RVW converts the switch files into a standardized RVW LAMA format.

During this conversion, call patterns are monitored, and suspicious call patterns are identified

(e.g., originating calls from a single telephone number which exceed established thresholds based on prior usage). RVW can then run additional analyses on the data and produce detailed reports which include the originating and terminating numbers along with call times and call duration. These detailed reports are then forwarded to our General Manager, Director of Operations, and Network Manager for further investigation to determine whether these calls are legitimate, such as mass callings made by schools and civil defense organizations.

We immediately investigate any identified patterns and telephone numbers with negative reputation scores to determine if the caller is attempting to originate unlawful robocalls. If we determine the calls are unlawful, then we either warn the caller to stop the calls or we terminate their service as appropriate.

We have taken the following steps to prevent illegal originating robocalling traffic:

1. We confirm the identity of all our customers and collect their physical location information, type of business and individual contacts during the signup process. We also do all of our own installs onsite for voice services.
2. We collect identity and location information from our customers when renewing contracts or adding new lines/services.
3. We have provisions in our terms and conditions notifying customers that they agree to ensure that all uses by them or any other user, whether authorized by the customer or not, comply with all applicable laws, regulations, and written and electronic instructions for use. We reserve the right to act immediately and without notice to terminate or suspend services from any customer whose use does not conform to the requirements in the agreement, determines that such use interferes with our ability to provide services to customers or other, or reasonably believes that such use may violate any laws, regulations, or written and electronic instructions for use.

We require new residential and commercial customers to provide at least one form of identification prior to subscribing to new services.

We have a “know-your-customer” policy through which we exercise due diligence in ensuring that our services are not used to originate illegal traffic. Although our business customers generally do not generate a high volume of calls, if we receive a request for high-volume origination services, we will exercise caution and extensively investigate such customers before granting access to the services. Specifically, we would collect information such as their physical business location, contact person(s), state or country of incorporation, federal tax ID, and the general nature of their business.

We follow the best practices for vetting caller identity described by the NANC Call Authentication Trust Anchor Working Group. (<https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>)