



Company Name: Blaze Broadband

Company Address: 6670 Cabin Branch Rd
Marshall, VA 20115

Company Phone Number: (540) 905-4049

Pursuant to 47 C.F.R. § 64.6305, Blaze Broadband submits this report on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls. This report describes the status of its implementation of STIR/SHAKEN and the practices and procedures Blaze Broadband has in place to mitigate illegal robocalls as of December 31, 2024. Blaze Broadband may modify, add, delete or otherwise alter any of the policies and procedures described in the plan at any time in order to respond to changes in its business, its capabilities and its needs.

As of December 31, 2024, Blaze Broadband voice traffic is SIP.

The current status of its STIR/SHAKEN implementation is:

- ☒ My traffic is fully attested
- ☐ My traffic is partially attested
- ☐ None of my traffic is attested yet

Blaze Broadband has fewer than 100,000 end users. Blaze has never had a robocall incident. Blaze has not been removed by FCC action from the FCC Robocall Mitigation Database (RMD) and is not prohibited from filing in the RMD.

Blaze Broadband is dedicated to stopping illegal phone calls from originating on our network. As such, all calls originating on our network are subject to our robocall mitigation program and this program meets FCC requirements for the mitigation of robocalls. Blaze has implemented the following robocall mitigation plan to address unlawful robocall traffic.

Blaze Broadband has a Know Your Customer (KYC) policy. Our robust customer authentication procedures include the collection of the following information for each customer:

- Customer identity, including business TAX ID when the customer is a business
- Service Address
- Customer's right to use the telephone number presented on calls

Blaze does not provide phone service to customers located outside of the United States. Blaze does not accept customers who are in the business of making robocalls and customers are not permitted to resell phone service provided by Blaze. International dialing is disabled by default requiring customers to specifically request international calling capability and each request is reviewed.

Blaze Broadband has enforceable terms of use and/or an acceptable use policy noted in its contracts. If a pattern of questionable activity is detected, Blaze Broadband will require its customer to remedy the problem and, if effective action is not taken, service to the customer may be suspended and/or terminated.

All phones and equipment employed by Blaze to provide phone services to our customers have been installed and configured by Blaze personnel on the customer's premise where calls will originate. Our customers cannot forge Caller IDs using Blaze provided equipment. Our customers have calling channel capacity limitations to prevent large scale outbound calling beyond what is expected of a given residence or business. Customer usage patterns

are analyzed regularly and call frequency which is unusual for a given customer, or for a given customer type, are flagged for review.

Blaze Broadband only accepts calls for termination from upstream phone service providers with valid registrations in the FCC Robocall Mitigation Database. Our current upstream phone service provider has implemented a number of technical robocall identification and mitigation policies and procedures that effectively become an integral part of our mitigation plan including:

1. Upstream provider has a Know You Customer (KYC) policy.
2. Upstream provider monitors and has real-time alerting to abnormal spikes in call quantity/frequency i) from a given device, ii) to international numbers, iii) of very short duration, iv) which fail to complete.
3. Upstream provider requires extensive documentation confirming our end user has the right to use each phone number presented on calls.
4. Upstream provider only completes calls with companies with a valid registration in the FCC Robocall Mitigation Database and partners with third-party vendors that offer Do Not Originate (DNO) lists as well as have their own DNO lists.
5. Upstream provider operates both proprietary and third party honeypots to proactively block unwanted SIP traffic from known malicious actors.

Blaze Broadband has designated an individual as a dedicated point of contact for addressing trace back requests. It either has provided the ITG with the contact information and business hours for those individuals, or will do so upon receipt of the first request from the ITG. See <https://www.ustelecom.org/the-industry-traceback-group-itg/for-providers/>.

Blaze Broadband will respond promptly within 24 hours to inquiries from the Industry Traceback Group (ITG). Requests from the ITG must be submitted in writing and include the following information:

1. Company Name
2. Company Address
3. Requestor's Name
4. Requestor's Title
5. Requestor's Phone number
6. Requestor's E-mail
7. Documentation/evidence of robocall/suspicious calling activity

Blaze Broadband will cooperate with state and federal regulators to prevent any and all illegal robocalls. Requests from the valid agency must be submitted in writing and include the following information:

1. Law Enforcement Agency Name
2. Agency Address
3. Agency phone number
4. Requestor's Name
5. Requestor's Title
6. Requestor's Phone Number
7. Requestor's E-mail
8. Subpoena associated with request, with authority of signatory identified and contact information provided

Blaze Broadband will provide valid law enforcement, regulatory agencies, and Industry Traceback Group members with the relevant non-proprietary and non-confidential information in response to reasonable and legitimate requests about illegal robocalls and suspicious activities, and implement mandated robocall mitigation procedures to the fullest extent possible with the goal of maximizing the mitigation of illegal robocalls. As mandated by the FCC, Blaze Broadband will always maintain the confidentiality and security of customer's Proprietary Information (PI), which includes both Customer Proprietary Network Information (CPNI) and Personally Identifiable Information (PII).