

Robocall Mitigation Program Description

Overview

Bradford Broadband implements a robocall mitigation program designed to prevent the origination and transmission of illegal robocalls on its network. The program incorporates customer vetting, traffic monitoring, call authentication technologies, and enforcement procedures consistent with guidance from the **Federal Communications Commission** and industry best practices.

The company maintains policies and procedures intended to identify, prevent, and mitigate unlawful robocall traffic originating from its network.

Customer Vetting and Onboarding

Bradford Broadband performs reasonable due diligence when onboarding customers who are capable of originating voice traffic. These procedures include:

- Verification of customer identity and contact information
- Verification of business legitimacy for business VoIP customers
- Confirmation that the customer has lawful authority to use any telephone numbers assigned or provisioned
- Review of the customer's intended calling use cases when high-volume calling capabilities are requested

Customers are required to agree to acceptable use policies prohibiting illegal robocalling and spoofing.

Monitoring and Detection

The network is monitored for indicators of potential illegal robocalling, including:

- Abnormal call volume patterns
- Short duration call attempts associated with robocalling campaigns
 - Rapid sequential dialing patterns
- Customer complaints or traceback requests

Traffic analytics and carrier feedback are used to identify suspicious call behavior.

STIR/SHAKEN and Caller Authentication

Bradford Broadband implements caller authentication consistent with the **STIR/SHAKEN framework** where technically feasible. Calls originating from authenticated endpoints are signed when possible, and authentication information is preserved when passing calls through the network.



Where STIR/SHAKEN cannot be applied (such as certain legacy or non-IP segments), Bradford Broadband applies alternative robocall mitigation procedures described in this program.

Response to Suspected Illegal Robocalls

If potentially unlawful robocalling activity is detected:

1. Traffic patterns are reviewed and analyzed.
2. The customer responsible for the traffic may be contacted for clarification.
3. Suspicious or unlawful traffic may be blocked or limited.
4. Accounts responsible for illegal robocalls may be suspended or terminated.

Bradford Broadband responds promptly to traceback requests from authorized industry traceback organizations.

Cooperation with Industry Traceback Efforts

Bradford Broadband cooperates with traceback efforts coordinated by the **U.S. Telecom Industry Traceback Group** and responds to traceback requests in a timely manner. Records related to call origination are retained as necessary to assist in identifying the source of suspected illegal robocalls.

Record Retention

The company maintains call detail records and relevant logs for a reasonable period of time sufficient to support traceback investigations and compliance with regulatory obligations.

Continuous Improvement

Bradford Broadband periodically reviews and updates its robocall mitigation policies and monitoring tools to remain compliant with evolving guidance from the **Federal Communications Commission** and industry best practices.

