



Key Components of Our Robocall Mitigation Strategy

1. Call Limits

We recognize the importance of limiting call volumes to prevent spam and nuisance calls. Our strategy includes the following call limits:

- **Outbound Call Rate Limit:** We enforce a maximum outbound call rate to prevent excessive traffic and mitigate the risk of robocalls.
- **Inbound Call Rate Limit:** We monitor incoming call rates to identify anomalies and promptly address any suspicious activity.

2. Contract Terms and Conditions

Our contract terms and conditions explicitly prohibit the use of our services for illegal or abusive purposes, including robocalls. We actively enforce these terms and take appropriate action against violators by terminating their relationship and use of our services

3. Single Carrier Approach

To streamline our operations and enhance security, we exclusively partner with Bandwidth as our carrier. Bandwidth implements the STIR/SHAKEN caller ID authentication framework across its network, ensuring that all call traffic undergoes rigorous verification. Bandwidth approach: “To combat the abuses of robocalling, Bandwidth is actively working to implement the most robust call authentication framework possible, while also working diligently to stop illegal number spoofing. We have adopted a three-pronged operational approach (prevent, detect, and mitigate) to stop and prevent illegal robocalls, while also expanding on industry efforts and best practices, as well as aligning with the Federal Communications Commission’s (FCC) guidance:

- FCC Adopts Rules to Help Block Illegal Robocalls
- Robocall Blocking NPRM and NOI

Here's the summary of our operational procedures to stop and prevent illegal robocalls:

Prevention

Bandwidth is working vigorously to prevent unlawful robocalls originating from our network. We have implemented a stringent screening process that prevent companies with potentially fraudulent robocalling traffic from becoming Bandwidth customers. We have also informed and empowered our customers with the information necessary to identify these unlawful calls, as defined by the FCC.

Detection

Bandwidth has an extensive fraud mitigation team dedicated to identifying and analyzing potential robocall campaigns on our network, and determining if they are lawful or not. In alignment with the FCC rules, Bandwidth is in the midst of augmenting its robocall detection technology that identifies and blocks unlawful robocalls from traversing our network.

Mitigation

Once an unlawful robocall campaign is detected, Bandwidth takes several steps to stop all

current and future unlawful calls. We have developed call blocking tools that prevent calls with specific unlawful ANI/'FROM' TN characteristics from traversing the Bandwidth network. Bandwidth personnel regularly analyzes network traffic looking for unlawful robocall campaigns and utilizes our call blocking tools when appropriate. We work diligently with our customers to stop all detected unlawful robocall campaigns and proactively communicate with those customers that may be in the path of unlawful robocalls. Bandwidth utilizes several systems and proprietary processes to detect and block unlawful robocalls that have the following types of ANIs, defined by the FCC as unlawful:

- **UNALLOCATED:** A valid NPA NXX XXXX in the North American Numbering Plan (NANP), but NOT assigned to a carrier, nor in the LERG. Any call that contains a phone number in the ANI / From field that has not yet been released for public consumption from the NANP.
- **INVALID NUMBER:** A complete telephone number (TN) that is NOT VALID, but of the correct format [2-9][0-9][0-9] [2-9][0-9][0-9] [0-9][0-9][0-9][0-9] (i.e., 10 digits in length, 1st and 4th are [2-9] all others are [0-9]. Any call that contains a character string of digits or letters that doesn't fully comply with E.164 formatting and the Local Exchange Routing Guide (LERG). This includes ANI / From fields with all digits of the same number, or anything less than 10 valid digits assigned from the NANP.
- **INVALID DIGITS:** The calling party number is numeric, but doesn't fit into a category defined above (i.e., all 1's, all 0's, partial entries <10 digits etc.).
- **INVALID ALPHA-NUMERICS:** Invalid alphanumeric strings used to misdirect, impersonate, disguise, or deceive SIP signaling.

For fraud prevention, detection, and mitigation, Bandwidth:

- Uses machine-learning technologies to detect voice network traffic anomalies, cost anomalies, and geographic traffic abnormalities in its fight against unlawful robocalls, as well as domestic and international toll fraud.
- Leverages industry-sanctioned and industry-sourced SPAM filter technologies to stop all forms of SPAM from reaching the text messaging ecosystem. Bandwidth doesn't allow text messages/campaigns that contain illicit content or have transmission behaviors that violate the Cellular Telecommunications and Internet Association (CTIA) guidelines. Bandwidth supports long code P2P, long code A2P, toll-free A2P, and short code texting. All of these types of messaging pass through our SPAM filtering technologies, where SPAM can be detected and blocked for industry defined SPAM and/or AUP violations.

We recommend customers follow our best practices for toll-free (A2P) messaging and the CTIA messaging principles and best practices.

- Subscribes to several internationally sanctioned databases of fraudulent telephone numbers used in international revenue sharing fraud (IRSF). These industry-sanctioned databases of fraudulent telephone numbers then become the foundation for blocking fraudulent international calls at Bandwidth.
- Monitors high-cost areas around the world. If traffic is destined for areas that are unusual or suspicious, Bandwidth monitors it carefully and immediately alerts and collaborates with its customers regarding suspicious calls that terminate into such areas. While FCC regulations mandate that carriers support effective communication traffic exchange and deliver legal traffic to its intended destination, when it's confirmed that calls are in fact fraudulent, Bandwidth diligently works to shut down these unlawful calls as soon as possible.
- Actively participates and leads in industry organizations and industry efforts to stop illegal robocalling. Even prior to the establishment of the Robocall Strike Force, Bandwidth was engaging the FCC and the FBI in efforts to stop consumer fraud in the form of toll-free traffic pumping, and participating in the USTA-sponsored traceback efforts to identify robocall originators and support enforcement.

Bandwidth has direct working relationships with the FCC, FTC, FBI, and IRS, among others in the government and law enforcement. Bandwidth is also actively engaged in working groups and at the board of director level at SIPForum, CTIA, and Incompas, and is an active participant in these organizations' efforts to address the consumer threat of robocalling.

Bandwidth is a member of the North American Numbering Council (NANC), several STIR/SHAKEN working groups, and has been selected to be the Incompas representative on the ATIS STI-GA Board overseeing the procurement of vendors for the critical components of the STIR/SHAKEN framework, such as the Certificate Authority and the Policy Administrator. Finally, Bandwidth is also a paid member and participant in the Communications Fraud Control Association (CFCA)."

4. Monitoring and Reporting

We continuously monitor call traffic, analyze patterns, and promptly address any deviations. Our reporting mechanisms include:

- Real-time Analytics: Monitoring call volumes, origins, and destinations.
- Exceptions logged and reportable

5. Education

We educate all new customers on Robocalling prior to purchase, then throughout their onboarding journey, and during their subscription period with us.

Conclusion

Our comprehensive Robocall Mitigation Strategy aligns with the FCC's guidelines and industry standards. By implementing call limits, enforcing contract terms, partnering with a single carrier, and embracing STIR/SHAKEN, we contribute to a safer and more reliable communication ecosystem.