

Cybertex Solutions - Robocall Mitigation Compliance with TRACED Act

Cybertex Solutions Inc. (the "Company") is committed to cooperating with the Federal Communications Commission (FCC), law enforcement, and the industry traceback consortium in investigating and stopping any illegal robocallers that it learns are using our service to originate calls or transit calls into the United States and Territories.

The Company has fully implemented STIR/SHAKEN.

The Company commits to fully responding within 24 hours to all traceback requests from the ITG, the TPTG, the FCC, and law enforcement. The Company shall cooperate with these groups to investigate and stop any illegal robocallers from using the Company's service to carry or process illegal calls. When notified by the FCC's Enforcement Bureau, Company shall block and report identified illegal traffic, and any substantially similar traffic, on an ongoing basis (unless Company's investigation determines that the traffic is not illegal) when The company receives actual written notice of such traffic from the Enforcement Bureau. If Company determines that the identified traffic is not illegal, Company shall provide the Enforcement Bureau with an explanation as to why Company reasonably concluded that the identified traffic is not illegal, and what steps it took to reach that Conclusion.

The Company utilizes a combination of internal tools and third-party solutions to check for Do Not Originate (DNO) numbers. In addition, the Company utilizes a combination of internal tools and third-party solutions to detect invalid phone number formats, area codes and unassigned number blocks. The Company also utilizes data analytics to detect and investigate irregular and unexpected calling patterns, originating number use against customer profiles.

The Company uses data systems for analytics and reviews to identify illegal robocalling in addition to a Know Your Customer (KYC) requirement to access the Company's networks. The process includes:

- Monitoring the network to identify suspicious traffic patterns.
- Limiting customers' capacity via call per second and/or concurrent session limits.
- Regularly checking call patterns for possible abusive traffic.
- All new customers are verified with a combination of electronic and manual verification systems, credit reviews, references from trusted industry members, and previous experiences with customer executives and employees. The Company severely limits the capabilities of new accounts until these appropriate processes are Complete.

The Company reserves the right to refuse traffic from any party at any time where robocalling or use of originating numbers that are not valid or they are not authorized to use has occurred or is suspected. The Company is able to block the originating number(s), terminating numbers(s), trunk(s) or customer, including termination of customer relationship to prevent robocalling, invalid originating number or spoofed origination number transiting the Company's networks.

Cybertex Solutions has two upstream providers, which receives voice traffic:

1. PayG LLC dba SkySwitch
Arborcrest 1, 751 Arbor Way
Suite 150
Blue Bell, PA 19422
Phone: 747.777.8100
Email: support@skyswitch.com

2. Bandwidth.com
2230 Bandmate Way,
Raleigh, NC 27607
Phone: 855.864.7776
Email: support@bandwidth.com

Here's the summary of Bandwidth operational procedures to stop and prevent illegal robocalls [1]:

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.

- Encourages customers to build their own proprietary URL shorteners and strongly discourages the use of the following public URL shorteners since fraudulent bad actors like to use free URL shorteners in sending illegal and unsolicited telemarketing text Messages:

- bit.ly (Bandwidth currently Blocks all messages with bit.ly)
- goo.gl (Google is phasing out this URL Shortener)
- tinyurl.com
- Tiny.cc
- lc.chat
- is.gd
- soo.gd
- s2r.co
- Clicky.me
- budurl.com
- bc.vc

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).

[1] Reference: <https://support.bandwidth.com/hc/en-us/articles/360020104374-Bandwidth-s-policies-to-combat-robocalls-scam-calls-toll-fraud-SPAM-and-more>