



Robocall Mitigation Efforts and Procedures

Loop Start Technologies has developed several processes and procedures in an effort to respond quickly to reports of fraud and Spam/RoboCalling, as well as track repeat offenders for banning from the Loop Start Technologies network.

Awareness of Customer Usage Patterns:

At this time, Loop Start Technologies does not engage with any clients that operate an outbound call center utilizing automated “predictive dialing” technology, and our Terms of Service specifically ban clients from engaging in such activity unless specific in-writing approval is granted. We reserve the right to ban/limit/restrict any clients that violate these policies. Prior to onboarding a new client, we adhere to a comprehensive procedure to familiarize ourselves with that client and their specific Unified Communications needs, to ensure they won’t abuse our policies.

Automated Protection Mechanisms:

Loop Start’s Unified Communications systems prevent customers from manually entering Caller ID details. Instead, Caller ID is derived from numbers ordered against and assigned to customers’ accounts, pending port in, or otherwise having a “proof of ownership” on file for a number ineligible for porting into our systems. We do permit customers to forward calls from their primary desk phone to their mobile devices, and in doing so, we do present the originating caller’s information, but this is achieved through conforming methods (such as PAI). We further restrict Caller ID from being selected that violates the FCC’s requirements regarding Caller ID delivery (such as, blocking calls that are presenting with Caller ID that is a Toll-Free Number instead of a LANI), or presenting malformed Caller ID outside of the E.164 standard). These restricted Caller ID standards also apply to calls forwarded from the user’s extension to a mobile device, so outside parties with non-conforming Caller ID aren’t extended back to the PSTN either.

Traceback Requests:

Loop Start Technologies commits to fully cooperate with the FCC and Law Enforcement within a reasonable timeframe (usually 24 hours) to all traceback requests, for both investigative and mitigation purposes. Loop Start further commits to conform to laws regarding access to such information.

Internal trace details are logged by our Unified Communications systems, and stored in accordance with our data retention policies. Loop Start Technologies utilizes top-tier 3rd party Carriers for their PSTN connectivity, and can submit requests to those parties when traces require additional PSTN details beyond what our systems capture.

Loop Start Technologies utilizes the following PSTN Carrier(s):

1. Company Name: **Bandwidth**
2. Company Address: **2230 Bandmate Way, Raleigh, NC 27607**
3. Company Contact: **(800) 808-5150**
4. Company Reporting URL: **<https://www.bandwidth.com/legal/>** (Select “Report A Number”)
5. Company Email: **ticketing@bandwidth.com**



The above-referenced Carriers fully comply with the FCC's STIR/SHAKEN standards and robocall mitigation regulations in all aspects when delivering voice traffic. Loop Start Technologies, in collaboration with its underlying providers, works diligently to prevent illegal robocalls, ensuring strict adherence to regulatory requirements. Additionally, Loop Start Technologies and its providers are committed to cooperating full in direct response to traceback requests, assisting authorities in identifying and addressing sources of fraudulent calls.

Procedure:

If a RoboCall has been reported by a recipient (or their authorized agent/representatives), or by a destination Carrier, Loop Start Technologies will follow the following process:

- Identify the originating Customer Domain of the RoboCall...
- Disable the originating Customer Domain of the RoboCall...
- Contact the Technical Point-of-Contact (PoC) on-record for the Customer Domain of the RoboCall, advising them of the disabled Customer Domain, and the reason for it. Loop Start Technologies will also provide call records (CDR), and trace data as requested by the Technical PoC, to assist in them identifying the specific reason for the RoboCalls.
- Respond, as necessary, to the initial reporter(s) of the RoboCall, notifying them that the originating Customer Domain has been disabled, and to confirm they are no longer receiving any additional calls that must also be addressed.
- Work with the Technical PoC to ensure all RoboCall attempts have been blocked.
- Check the Ticketing System to confirm the Technical Contact has not had multiple RoboCall reports within a 365 day period. Pursuant to the Terms & Conditions signed at the time of service activation, multiple reports could result in the Technical PoC (and possible their Customer Domain(s)) being banned from the Loop Start Technologies network.
- Reinstate the Customer Domain, only after it has been confirmed that RoboCalling for that domain has been prevented.
- Update the Abuse Ticket (which was auto generated with the initial report), indicating the results of the investigation,

Reporting a RoboCall Event:

Email: abuse@loopstart.net

NOTE: This email address will automatically open a high-priority ticket within the Loop Start Technologies Ticketing System

Service Level Agreement:

All reports of RoboCalling will be responded to within 24 hours. Investigations will begin within that time as well.