



NexLink Telecom LLC maintains reasonable and effective measures designed to prevent the origination and transmission of illegal robocalls and unlawful caller ID spoofing through its Cloud VoIP services.

Customers are permitted to originate calls only through authorized telephone numbers assigned to or legitimately associated with their service. During service activation and provisioning, caller ID information and applicable call records are reviewed to verify the legitimacy and authorized use of originating telephone numbers.

NexLink Telecom LLC does not provide an automated mechanism for customers to generate high-volume outbound calls. Outbound calls are originated through human interaction by authorized users of the service.

Network-level security controls are implemented to restrict VoIP traffic to authorized customer IP addresses and approved network sources. These controls help prevent unauthorized access and the use of NexLink Telecom's network for fraudulent or abusive calling activity.

NexLink Telecom LLC also utilizes call-blocking and traffic-analytics capabilities to identify and mitigate known robocall sources, suspicious calling patterns, and potentially fraudulent or abusive traffic. Identified traffic may be blocked or otherwise restricted based on applicable security and traffic-management criteria.

These measures are part of NexLink Telecom LLC's ongoing robocall mitigation and call-authentication practices and are intended to help protect the integrity of its voice network, reduce unlawful robocall activity, and ensure that calls transmitted through its network use legitimate and authorized caller identification information.