



ServerPlus LLC 555
S State St.
Orem Utah 84058

Outlined below is Serverplus LLC's Robocall Mitigation Plan in compliance with the Traced Act.

Serverplus LLC's is committed to protecting its customers from illegal and spoofed robocalls and has implemented robust measures to identify and stop illegal robocallers from using ServerPlus services to originate such calls. The purpose of this Robocall Mitigation Program (the "Program") is to outline these measures and ensure organizational alignment on the processes and principles set forth herein. The Program also outlines remedial measures that ServerPlus will undertake if ServerPlus system is being used to originate illegal and spoofed robocalls or if a ServerPlus customer alerts ServerPlus to potential fraudulent activity on their account.

The Program will be reviewed yearly and updated as necessary by ServerPlus to ensure that it remains responsive to current robocalling threats, scam calling threats and fraud mitigation, conforms with applicable law, and addresses any changes to ServerPlus' network architecture and services as well as any organizational changes that may occur from time to time.

ServerPlus LLC commits to respond to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, within 24 hours and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

Traceback requests can be addressed to:

Primary: it@serverplus.com

Alternate: quality@serverplus.com

Alternate: support@serverplus.com

Detection of the origination of illegal robocall traffic:

a) We vet our clients at signup to ensure that their usage is for legitimate business or personal use only.

b) We require all clients to sign an attestation form stating they have the right to use their phone number and caller ID, and giving us permission to use it for outbound calls.

Prevention of the origination of illegal robocall traffic:

- a) All clients and employees are limited in the number of concurrent calls that they can create or accept.
- b) All clients and employee traffic must come from an authenticated source. Authentication credentials are provisioned securely in all our use cases to prevent illegitimate use.
- c) ServerPlus validates customer authorization for the use of presented caller ID numbers. All clients are required to sign an attestation form stating that they are authorized to use the telephone numbers and caller ID information presented on outbound calls.
- d) All outbound PSTN traffic is routed through ClearIP. ClearIP provides STIR/SHAKEN call authentication services and is configured to apply A-level attestation for authenticated outbound PSTN traffic in accordance with configured authentication policies and industry standards.
- e) Internal calls that remain entirely within the ServerPlus network, including extension-to-extension communications, are not transmitted to the PSTN and are therefore not subject to STIR/SHAKEN authentication requirements.

Mitigation of the origination of illegal robocall traffic:

- a) Upon detection or reasonable suspicion of illegal robocall traffic, caller ID spoofing, fraudulent telecommunications activity, or misuse of ServerPlus services, the affected account, service, or calling capability may be suspended pending investigation.
- b) ServerPlus may restrict outbound calling capabilities, notification campaigns, callback functionality, caller ID presentation, or other telecommunications services while investigations are conducted. Repeated violations or confirmed unlawful activity may result in permanent termination of services.
- c) Parties found to be originating illegal robocall traffic or engaging in unlawful telecommunications activity may be reported to appropriate regulatory authorities, law enforcement agencies, traceback organizations, carriers, or other appropriate authorities.

Monitoring and data retention

- a) SIEM and XDR systems, monitor servers for unusual activity and known threats.
- b) Starting in 2025 we will be retaining all call data logs for up to 2 years to facilitate any TRACED data requests.