

[USA-Connect.net](https://usa-connect.net)
ROBOCALL MITIGATION PLAN

I. Background

Under the authority Congress granted the Federal Communications Commission (“FCC” or “Commission”) in the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, the Commission has adopted rules requiring voice service providers, like USA-Connect Inc. (“USA-Connect”), to implement STIR/SHAKEN caller ID authentication technology in the Internet Protocol (IP) portions of their networks. 47 CFR § 64.6301.

The FCC requires that all voice service providers certify, by June 30, 2021, in the Commission’s [Robocall Mitigation Database](#) whether they have implemented STIR/SHAKEN or, if subject to an applicable extension, that they have documented and instituted a robocall-mitigation plan to help combat the origination of illegal robocalls on their networks.^[1] The Commission has explained that a robocall-mitigation program is sufficient if the detailed practices in the plan can “reasonably be expected to significantly reduce the origination of illegal robocalls” and the voice service provider complies with the practices it describes in its filings.

USA-Connect is dedicated to stopping illegal calls from originating on its network and undertaking commercially reasonable efforts to monitor the calls coming into its network, consistent with FCC regulations and its “[Best Practices](#)” guidance.

This document outlines [USA-Connect.net](https://usa-connect.net) Robocall Mitigation plan.

II. [USA-Connect.net](#) Know Your Customer (“KYC”) Standards

USA Connect is a voice service provider that provides mostly in the New York City area. All prospective customers participate in an in-person or telephonic enrollment process.

[USA-Connect.net](#) customers, before entering into a written agreement, participate in a telephone enrollment process, verify the customer’s business name, physical address, contact person.

Whenever possible, our installer will plug in the physical phones onsite at the customer’s office.

Almost all the physical phones are configured in our office by [USA-Connect.net](#) techs, or installers, make test calls to ensure that the outbound caller id numbers are what were assigned to that customer.

III. USA-Connect Acceptable Use Policy

As part of its customer-onboarding process, all of USA Connect customers contractually agree to various terms and conditions, including a commitment to comply with USA-Connect policy. Among other things, this prohibits:

- Using the Services to engage in any activities that are illegal, abusive, false, fraudulent calls.

USA-Connect’s contracts with its customers stipulate that USA-Connect is authorized to suspend and/or terminate all Services in the event of a policy violation.

IV. Telephone Number Authorization and STIR-SHAKEN Capabilities

We have abnormal traffic monitoring tools/scripts in place, which monitor the number of calls per hour, any excessive traffic will alert us to investigate immediately, and block the offending customer.

[USA-Connect.net](#) uses multiple tools, scripts to monitor fraudulent/abnormal traffic and automatically block the offending customer.

V. Proactive Network Monitoring

[USA-Connect.net](#) has various monitoring and reporting systems in place to analyze the traffic on our network for potentially suspicious patterns that are associated with illegal robocalls, for example, any excessive traffic results in automatic suspension of the customer's outbound phone traffic, majority of the customers are only allowed from US ip addresses, and have ACLs in place.

VI. Commitment to Traceback Cooperation

USA-Connect commits to timely cooperating with and responding to Traceback requests from the ITG (or any successor entity designated by the FCC), trace-forward investigations, and other valid law enforcement and government demands, subpoenas, and other valid legal processes. USA-Connect will dedicate sufficient resources to provide prompt and complete responses to such requests. USA-Connect will investigate suspicious activity found

by its monitoring systems or reported to it by consumers or third parties and take appropriate action.

[1] See <https://docs.fcc.gov/public/attachments/DA-21-454A1.pdf>.