



Robocall Mitigation Plan for Rock Solid Technology Solutions (RSTS)

RSTS offers VoIP services internally and to client companies and their end users. RSTS verifies the business entity, business activity and physical location of every client customer.

RSTS works with VoIP Carriers that either have fully implemented STIR/SHAKEN or plan on implementing STIR/SHAKEN. The bulk of Inbound and Outbound Terminations are provided by Carriers which are STIR/SHAKEN Compliant.

RSTS is a Small Service Provider, serving fewer than 100,000 voice service subscriber lines and therefore qualifies for an extension until June 30, 2023 of STIR/SHAKEN Implementation under 47 C.F.R. §64.6304(a).

RSTS commits to respond to all trace back requests from the Commission, law enforcement, and industry trace back consortium(s), and to cooperate with such entities in investigating and immediately stopping any illegal robocalls that use its service(s) to originate calls.

RSTS has taken the following specific steps to prevent originating robocall traffic:

- RSTS only provides call terminations placed on our managed networks and servers.
- All devices able to make calls on our networks are authenticated at multiple levels.
 - Server
 - Trunk
 - Virtual Private Network (VPN)
 - Session Border Controller (SBC)
 - User Device
- Call termination is limited to known, verified, and directly connected approved IP addresses.
- Anonymous traffic is strictly prohibited and blocked by default.
- Voice network traffic is continually monitored for unusual traffic patterns.
- Call Thresholds are set and monitored to blacklist traffic that exceed regular traffic standards.
- Regular checks are performed to ensure that outbound call volume via our services is consistent with expected volumes. Any anomalies are investigated.
- All Systems are patched and updated regularly to stay current with known security issues.

RSTS will take the following steps to mitigate illegal robocalling when detected:

- Determine the source of the illegal robocalling and blacklist any IP Addresses at risk.
- Perform internal investigation as to the source and scope of the robocalls.
- Ongoing audits of security measures to determine how to prevent future robocall activity.

