

Trifecta Solutions Inc (FRN: 0019169630) Robocall Mitigation Plan

Trifecta Solutions Inc is dedicated to stopping illegal calls from originating in our network and monitoring the calls coming into its network, in accordance with FCC regulations.

Know Your Customers

New Customers: Trifecta Solutions Inc is engaged in a business-to-business sales model and screens all new customer opportunities.

All of our customers have corporate offices in the United States. Existing numbers are ported into Bandwidth.com and only terminate or originate calls with Tier 1 Carriers that all have their own internal robocall mitigation processes and protocols.

All Active Trifecta Solutions Inc Customers: All Trifecta Solutions Inc active customers can request us to block calls by using CallerID details.

In addition, all users are configured by our support team to known devices (phones and fax adapters). The only exception is a few trunk lines we have that are in businesses that we are very familiar with that have little to no risk of robocalling (like school districts and hotels). We will never configure an auto-dialer on our system unless we have confirmed verification from the customer that the dialer is used for legal purposes and we will have that in writing, on file. Currently, none exist on our system.

Trifecta Solutions Inc periodically reviews Call Detail Records for suspicious behavior and patterns that are indicative of robocalls that are in violation of our Terms and Conditions on our website. Trifecta Solutions Inc reserves the right to terminate service of any Customer for numerous violations, including but not limited to unlawful Robocalls.

Know Your Upstream Provider

All of our calls originate with numbers existing on the Bandwidth.com network. These calls enter our system via our Sansay SBC's which prevent traffic from any other sources. Any calls leaving our system route through our SBC's and are then routed first to the TransNexus ClearIP platform which handles Telecom Fraud Prevention, Robocall and TDoS prevention, STIR/SHAKEN caller ID authentication and verification. Only after calls are verified via ClearIP will calls be allowed through to our outbound carriers. Any calls that are

identified as fraudulent or robocalling are automatically blocked and our support team is notified of the blocked caller. We only release the caller after verifying that the calls are legitimate. Any callers that violate robocalling regulations will be blocked from calling until any concerns are rectified.

Traceback

Trifecta Solutions Inc is committed to respond fully and within 24 hours to any and all requests from CALEA, the Industry Traceback Consortium, and all law enforcement agencies who officially and properly subpoena customer records.

Trifecta Solutions Inc certifies that it will cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

Trifecta Solutions Inc certifies that all voice traffic which originates on its network is subject to this robocall mitigation program.

Trifecta Solutions Inc certifies that as part of its robocall mitigation efforts it is taking these specific reasonable steps to avoid originating illegal robocall traffic:

1. All our customers have a rate limit set on each group, extension, and outbound number.
2. We provision all devices on our system and will never provision an auto-dialer (robocaller) without first clarifying the purpose and getting written confirmation that the device will be used for legal purposes.
3. Periodic reviews of Call Detail Records for suspicious behavior.
4. Removal of any capability which might permit unauthorized calling number use.

Trifecta Solutions Inc certifies that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and that it has fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it originates are compliant with 47 CFR § 64.6301(a)(1) and (2).

STI Authentication and Verification processes have been implemented and are in full production status for all calls.