

Robocall Mitigation Plan for Santorini Solutions (Updated 12/15/2024)

Introduction:

This document describes Santorini Solutions (SS) Robocall Mitigation Plan, which will be submitted to the Federal Communications Commission's (FCC) Robocall Mitigation Database. Santorini Solutions is fully committed to mitigating unlawful robocalls and complying with Federal Communications Commission (FCC) regulations to ensure integrity of telecommunications networks pursuant to 47 C.F.R. § 64.6305 for STIR/SHAKEN call authentication framework. This document sets forth SS current policies and procedures designed to reduce or eliminate outbound illegal robocalls originating on its network.

Santorini Solutions views these policies and procedures as constituting “reasonable steps” to avoid the origination of illegal robocalls on its network and in addition to following these steps the Provider commits to responding to all traceback requests from the FCC, law enforcement, and the Industry Traceback Group (ITG), and to cooperate with such entities in investigating and stopping any illegal robocallers that may use its service to originate calls.

Compliance

Santorini Solutions certifies that all calls that it originates on its network are subject to a robocall mitigation program. No prior certification has not been removed by Commission action and it has not been prohibited from filing in the RMD as of filing of this plan.

Traceback Requests

Santorini Solutions commits to respond fully within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls. If a traceback exposes an existing customer as the source of fraudulent robocalls, or as having transmitted fraudulent robocalls, a demand for an explanation and verification of mitigation of the traffic is issued to the customer. If the fraudulent traffic is not remediated, ConnectTo initiates blocking of all traffic from the offending customer.

The Company's point of contact to handle traceback requests is:

Name: Leni Thomas

Title: Chief Technology Officer (CTO)

Telephone Number: (469) 643-4000

Email Address: contact@santorinisolutions.com

Call Analytics Systems

a. Calls with short duration are monitored, notified, and reported by the service provider when a predetermined ratio/threshold is reached.

b. Call logs are regularly analyzed for anomalies for every account: unusual number of short calls, unusual call volume, unusual time of calling. Whenever an anomaly is detected, the end user is notified and is required to provide written explanation.

Upstream Providers

Santorini Solutions partners with Telnyx to ensure upstream compliance:

- a) Telnyx is fully compliant with STIR/SHAKEN and all calls originating on its network receive attestation. Telnyx has been approved by the STI-PA to participate in the SHAKEN/ STIR framework and are fully SHAKEN/STIR compliant, authenticating every outbound call with a valid U.S. Caller ID that originates on the Telnyx platform.
- b) Telnyx passes on SHAKEN/STIR headers of customers who have their authorization tokens along the PSTN. Inbound calls with A attestation and a valid token have the 'verstat' parameter added to P-Asserted-Identity headers.
- c) The verstat parameter is included in the P-Asserted-Identity SIP header and includes information about the caller identity validation and attestation level.
- d) Telnyx has introduced the following two additional values to the verstat parameter in SIP headers to improve the SHAKEN/STIR framework, providing us with more granular information regarding originating Caller ID attestation and verification results.
 - 1. TN-Validation-Passed-B: Identity header verification is successful, and the caller has a B attestation
 - 2. TN-Validation-Passed-C: Identity header verification is successful, and the caller has a C attestation
- e) No calls originate using numbers not purchased from us, ported to us, or verified through us and whitelisted in the provider's system.

STIR-SHAKEN IMPLEMENTATION STATUS

Furthermore, Santorini Solutions will be partnering with a third-party vendor/underlying carrier to sign its calls with Santorini's own token if full compliance is required end-to-end. It should be noted that Santorini Does not allow our customers to spoof CallerID, so any outgoing CallerID can easily be traced to our customer.

KNOW YOUR CUSTOMER (KYC)

Santorini Solutions has strict Know Your Customer (KYC) policies for all new or renewing customers to ensure that such customers and providers do not or are not likely to engage in any prohibited conduct. Once a customer is vetted, Santorini Solutions continuously monitors call traffic for unusual patterns or violations of its terms of service.

Additionally, prospects are required to agree to Santorini Solutions strict Acceptable Use Policies (AUP) prohibiting, among other things, the act of fraudulent voice activity as a condition of doing business with Santorini Solutions. Furthermore, Santorini Solutions requires all customers to comply with the Telephone Consumer Protection Act and its implementing

regulations, the Telemarketing Sales Rule, regulations implementing the FCC's national Do-Not-Call registry, and all other rules and regulations governing the sending of telemarketing calls and/or robocalls.

Our general practices are as follows:

1. Customer Information: Potential clients must provide government-issued identification, proof of business registration, contact details, and a valid tax ID
2. Caller ID Restrictions: Customers are required to use valid, non-spoofed caller IDs. Invalid or unverified caller IDs are blocked.
3. Caller ID Restrictions: Customers are required to use valid, non-spoofed caller IDs. Invalid or unverified caller IDs are blocked.
4. Payment Limits: Payments are monitored, and suspicious activity, such as unusually large or frequent transactions, is flagged for review.
5. Ongoing Monitoring: Customer call traffic is continuously analyzed for compliance, and accounts exhibiting irregular patterns are reviewed.
6. Account Vetting: ConnectTo reviews business use cases to ensure services are used only for legitimate purposes, terminating accounts if illegal activity is detected.

What we do if we notice Suspicious Activity

When our monitoring systems detect activity consistent with illegal robocalls or when there is reason to suspect such behavior, Santorini Solutions will act immediately to identify the source. This process involves tracing the origin, routing, or termination points of the suspicious traffic within our network.

Once the responsible entity is identified, Santorini Solutions will implement appropriate measures, including: Validating TN Authorization: Verifying whether the originating party is authorized to use the identified TN. If fraudulent or unauthorized use is confirmed, immediate steps will be taken to revoke or suspend the TN's usage.

Suspending Call Operations: If necessary, will suspend the originating, routing, or terminating capabilities of the party responsible for the suspicious traffic to halt further illegal activity and protect consumers from harm caused by robocalls and spoofing.

This Robocall Mitigation Plan will be continuously updated to incorporate new technologies and practices, ensuring proactive measures to safeguard the integrity of our network and protect Consumers.