

ConnectTo Communications, Inc.

Robocall Mitigation Plan

(December 2024)

Introduction

This Robocall Mitigation Plan (RMP) details the reasonable steps and actions taken by ConnectTo Communications, Inc. ("ConnectTo") to mitigate and eliminate illegal robocalling. ConnectTo has implemented STIR/SHAKEN, and has an ongoing commitment to identify and help alleviate illegal robocalling by pre-qualifying prospective customers, monitoring existing customers for traffic patterns indicative of prohibited robocalls, and working with other providers and regulatory agencies in combatting fraudulent voice activity.

All calls that originate on its network are subject to a robocall mitigation program. All telecom services rely, in part, on ConnectTo's underlying providers for STIR/SHAKEN implementation and other robocall mitigation efforts.

The Company is not a foreign voice service provider.

The Company does not sell services to international call originators using North American Numbering Plan Numbers.

Compliance History

In the past two years, the Company has not been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

No prior RMD certification has been removed by the Commission. The Company has not been prohibited from filing in the Robocall Mitigation Database by the Commission.

The person within the Company responsible for addressing all robocall mitigation-related issues, is:

Name: Aram Ter-Martirosyan

Title: CTO/CIO

Department: IT

Telephone Number: (818) 546-4601

Email Address: aram@connectto.com

STIR/SHAKEN Implementation

ConnectTo has fully implemented the STIR/SHAKEN authentication framework across the entire IP portion of its network, and all calls it originates are compliant with § 64.6301(a)(1) and (2). This compliance is due, in part, to ConnectTo's underlying service providers being STIR/SHAKEN compliant within the IP portions of their networks.

The Company uses a third-party vendor/underlying carrier to sign its calls and ConnectTo has its own token. ConnectTo does not allow its customers to spoof CallerID, so any outgoing CallerID can easily be traced back to ConnectTo's customer.

In addition to analytics provided by its underlying service provider(s), the Company uses a third-party call analytics vendor, Transnexus. ConnectTo utilizes AI-driven call analytics systems to monitor and flag suspicious patterns, such as high-volume short-duration calls or calls to disconnected numbers. Calls flagged as likely illegal are automatically blocked.

Traceback Requests

The Company 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: Aram Ter-Martirosyan

Title: CTO/CIO

Department: IT

Telephone Number: (818) 546-4601

Email Address: aram@connectto.com

Know Your Customer

ConnectTo has implemented Know Your Customer (KYC) policies when onboarding new or renewing customers to ensure that such customers and providers do not or are not likely to engage in any prohibited conduct. Post-onboarding, ConnectTo continuously monitors call traffic for unusual patterns or violations of its terms of service.

ConnectTo's KYC practices include:

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. Payment Limits: Payments are monitored, and suspicious activity, such as unusually large or frequent transactions, is flagged for review.
4. Ongoing Monitoring: Customer call traffic is continuously analyzed for compliance, and accounts exhibiting irregular patterns are reviewed.
5. Account Vetting: ConnectTo reviews business use cases to ensure services are used only for legitimate purposes, terminating accounts if illegal activity is detected.

Additionally, prospects are required to agree to ConnectTo's strict Acceptable Use Policies (AUP) prohibiting, among other things, the act of fraudulent voice activity as a condition of doing business with ConnectTo.

ConnectTo 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.

Telephone Number Validation:

A Telephone Number ("TN") based caller identity is the originating phone number included in call signaling used to identify the caller for screening purposes that is uniquely associated with the subscriber. A subscriber is permitted to use a TN as a caller identity if a TN is directly managed by ConnectTo and/or obtained by ConnectTo from ConnectTo's underlying carrier for use by the subscriber.

For subscribers with multi-line telephone systems, ConnectTo and its underlying provider(s) only allow calls to be connected if the originating number matches one of the TN's assigned to the subscriber. This screening capability enables an automated and secure method of validating originating telephone numbers.

Ongoing Robocall Mitigation

ConnectTo monitors and examines customer traffic to detect suspicious call activity and/or calling patterns. When ConnectTo and/or its underlying providers detect network usage patterns consistent with illegal robocalls or suspect illegal robocalling is taking place, ConnectTo will immediately seek to identify the party that is originating, terminating, or routing these calls so that it may take appropriate action. The actions taken may include, but are not limited to, initiating a traceback investigation; verifying that the originating customer owns or is authorized

to use the Caller ID number; determining whether the Caller ID name sent to a receiving party matches the customer's corporate and/or d/b/a name; block (or initiate third-party blocking) the party's ability to originate, terminate, or route calls on the network; and/or providing notice to law enforcement authorities.

As part of its plan to mitigate and prevent any originating robocalls, ConnectTo is committed to early identification and investigation of possible robocalling conditions. Among other things, ConnectTo watches for higher-than-normal subscriber traffic volume, including large bursts of traffic in small timeframes or spikes in usage. ConnectTo also monitors for originating calls of short duration and low call completion percentages and originating calls with sequential "called to" number dialing patterns.

Updating ConnectTo's RMD Submission and RMP

Consistent with FCC Regulations, 47 C.F.R. § 64.6305(d)(5), (e)(5) and (f)(5), ConnectTo will update its submission in the RMD within 10 business days of any change to the applicable information it must provide and update in the RMD.

The Company's RMP continues to develop as the Company and the industry gain expertise and deploy new robocall mitigation strategies and will be supplemented in future updates.