

Custom Network Solutions, Inc.

Robocall Mitigation Plan

(Updated September 2025)

Introduction

This Robocall Mitigation Plan (RMP) details the reasonable steps and actions taken by Custom Network Solutions, Inc. ("CNS") to mitigate and eliminate illegal robocalling. CNS 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.

CNS provides retail voice and data services. All calls that originate on its network are subject to a robocall mitigation program. All telecom services rely extensively on CNS's underlying provider(s) for STIR/SHAKEN implementation and other robocall mitigation efforts. CNS's underlying carrier partner is Verizon.

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 (and/or any entity for which the filing entity shares common ownership, management, directors, or control) 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: Gregory Rozar

Title: Director of Network Operations

Department: Network Operations

Telephone Number: (201) 845-4555 X502

Email Address: grozar@cnsny.net

STIR/SHAKEN Implementation

All telecom services are provided on a resale-only basis. The company is, therefore, exempt from the requirement to implement STIR/SHAKEN because, as a reseller, it lacks control over the network infrastructure necessary to implement STIR/SHAKEN. See First Caller ID Authentication Report and Order, 35 FCC Rcd at 3241, para. 40; 47 CFR Section 64.6304(b). As further detailed herein, the Company has taken steps appropriate for, and required of, a reseller to mitigate robocalling.

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

The Company does not use a third-party call analytics vendor (not including analytics provided by its underlying service provider(s)).

Traceback Requests

The Company commits, in connection with its underlying service provider, to respond fully and in a timely manner 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, CNS initiates blocking of all traffic from the offending customer.

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

Name: Gregory Rozar

Title: Director of Network Operations

Department: Network Operations

Telephone Number: (201) 845-4555 X502

Email Address: grozar@cnsny.net

Know Your Customer

CNS has implemented Know Your Customer 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. The Company requires agreements to be signed by an authorized person. E911 locations are recorded for each phone number. A physical business location and local contact person is required for service with the Company.

CNS will not activate clients that provide anonymous information or where data mismatches are found. Additionally, CNS is implementing strict Acceptable Use Policies (AUP) prohibiting the act of fraudulent voice activity as a condition of doing business with CNS.

Prospects or current customers who have been known to act improperly or otherwise be involved in fraudulent robocalling will cause their companies to be rejected by CNS as a customer and any existing customer relationships could potentially be severed.

Further, CNS's new AUP will require 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 high percentage of the Company's clients are local. The Company provides a physical, on-site install for customer projects. Representatives from the Company visit the address of non-local customers.

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 CNS and/or obtained by CNS from CNS's underlying carrier for use by the subscriber.

For subscribers with multi-line telephone systems, CNS 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

CNS, in connection with its underlying service provider, monitors and examines customer traffic to detect suspicious call activity and/or calling patterns. When CNS and/or its underlying providers detect network usage patterns consistent with illegal robocalls or suspect illegal robocalling is taking place, CNS 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, CNS, in connection with its underlying service provider, is committed to early identification and investigation of possible robocalling conditions. Among other things, CNS watches for higher-than-normal subscriber traffic volume, including large bursts of traffic in small timeframes or spikes in usage. CNS also monitors for originating calls of short duration and low call completion percentages and originating calls with sequential “called to” number dialing patterns.

Updating CNS’s RMD Submission and RMP

Consistent with FCC Regulations, 47 C.F.R. § 64.6305(d)(5), (e)(5) and (f)(5), CNS 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.