

Date	On behalf of	Change Summary
February 21, 2024	Chazy and Westport Telephone Company	Update for compliance with the Sixth Report and Order

This mitigation plan is submitted on behalf of Chazy and Westport Telephone Company (“CWT”), an incumbent local exchange carrier serving rural communities in the state of New York.

I. Implementation and Extension Status

Extensions Received Under 47 C.F.R. §64.6304

CWT is eligible for the continuing extension of the STIR SHAKEN implementation deadline as a small voice service provider (§64.6304 (a)(2) that has non-IP portions within its network §64.6304(d).

CWT is a member of NTCA who participates on the ATIS Non-IP taskforce working group which developed the (ATIS Solutions) non-IP call authentication solutions and serves as CWT’s third-party representative on the ATIS Non-IP taskforce working group

Status of STIR/SHAKEN Implementation

All CWT traffic is TDM and therefore not yet authenticated and verified under STIR/SHAKEN. Its traffic remains subject to its robocall mitigation plans.

CWT will implement a call authentication protocol for voice calls delivered over the non-IP portions of its network that do not use SIP technology when such a protocol is fully developed and finalized by industry standards and the necessary equipment and software is available on the commercial market.

II. Robocalling Mitigation

CWT is a voice service provider who leases its switch functions from a third party carrier. All calls that originate on its network are subject to the company’s robocall mitigation plan. CWT uses Call Analytics and Know Your Customer to prevent the origination of robocall traffic on its network. While CWT is not directly connected to any carriers, all carriers with whom it exchanges traffic appear on the Robocall Mitigation Database and their traffic is subject to the same mitigation plan as that of its own end users.

Analytics

CWT purchases switching and connectivity through its network vendor, Westelcom Network, LLC who uses analytics to monitor all voice traffic in real-time to prevent the origination or transit of illegal robocalls. Any suspected robocalling activity identified as originating from a CWT end user is referred to CWT to determine if the caller was attempting to originate or transit unlawful robocalls. If CWT determine that the traffic was likely unlawful, CWT then warns them to stop sending such traffic. If they continue to send traffic that appears to be unlawful, then CWT terminate their service.

Know Your Customer

CWT utilizes the mitigation technique of “Know Your Customer.” CWT is a small long established provider that maintains a close relationship with its subscribers. Its customers are generally “mom and pop” users and few of its total customer base have enough call paths to generate the high volume of

traffic associated with robocalling allowing us to use targeted in-house analytics to monitor, alert and apprehend suspected robocalling activities.

CWT has a screening for new customers requesting service at or above large volume calling capability levels:

- CWT will not deploy large volume calling capability as a residential service or at an address shown in the company records as being residential
- Businesses requesting large volume calling capability must provide a tax ID and verification as to the nature of the business
- CWT verify addresses to look for overlapping / multiple deployed voice path subscriptions
- A CWT representative may visit the premise of the business to verify the number of users at the location is appropriate for the volume of calling

CWT serves a small number of long-time business end users with large volume calling capability that are being directly contacted to review with them CWT's policies and efforts to prevent the CWT network from being used for illegal robocalling.

General Prohibition

CWT end user services are subject to restrictions contained in its published legal notices and all executed services orders include the requirement that service is provided pursuant to its terms of service ("TOS") requirements.

Its existing TOS prohibit activities normally associated with Robocalling including, but not limited to:

- providing altered, deceptive, or false information about the identity of the sender or the origin of a message or phone call;
- violating any applicable local, state, or federal law; using the CWT service to engage in or in connection with fraudulent activities

In addition, the company is updating its TOS to expressly reference the prohibition on robocalling and all current subscribers will receive notice of the publication of its updated TOS.

CWT's end users are notified that CWT may take action up to suspension or termination of service for violation of the TOS.

III. Traceback and Enforcement Cooperation

CWT will actively participate the traceback community including the FCC, law enforcement, and The Industry Traceback Group (ITG). CWT commitments to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium and will cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

IV. Additional Certifications

Neither CWT nor any entity which shares common ownership, management, directors, or control has 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.

.