

Robocall Data Mitigation Plan
Citizens Telephone Company of Kecksburg and Citizens Telecom
Solutions, LLC. (Citizens)

FRN: 0003735867

Filing Date: February 19, 2024

The following documentation is to serve as the Robocall Mitigation Program of Citizens Telephone Company of Kecksburg (OCN 0156) and Citizens Telecom Solutions, LLC. (OCN 050A) and their ongoing compliance with the Traced Act.

(47 CFR § 64.6304a) – Non-IP networks allows for those portions of a voice service providers' network that rely on technology that cannot initiate, maintain, and terminate SIP calls are deemed subject to a continuing extension. A voice service provider subject to the foregoing extension shall comply with the requirements of 47 CFR § 64.6303 as to the portion of its network subject to the extension.

Citizens hereby certifies the following information:

Citizens has implemented the STIR/SHAKEN authentication framework on the IP portion of its network and all calls it originates on that portion of its network are compliant with 47 CFR § 64.6301(a)(1) and (2).

Citizens (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 Citizens transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

Citizens hereby certifies to the implementation of the following practices:

I. Implementation of STIR/SHAKEN call authentication

- a. Citizens, as both an ILEC and CLEC is compliant with the IP portion of its voice network using TNS Call Guardian Authentication Hub integrated into its Metaswitch Class 5 switching platform.

II. Traceback Requests

- a. Pursuant to 47 CFR § 64.6305(B)(4), Citizens has designated a point of contact to receive notice of any incidents of illegal robocall traffic. This person's name, title, address, phone number, and email address is available in the RoboCall Mitigation Database portal.
- b. This individual will be the main contact responding to all traceback requests from the Commission, law enforcement, and the registered traceback consortium. Citizens will respond fully and within 24 hours to traceback requests from such entities and will cooperate in investigating and stopping any illegal robocallers that use its network to originate calls.

III. Subscriber Vetting Process

- a.** Citizens will vet the identity of residential, retail, and wholesale subscribers through its normal business practices and will obtain contact information, service address information, physical business location, state or country of incorporation, federal tax ID and general nature of the customers business as appropriate.
- b.** Citizens will complete an additional review of any outbound call centers or high-volume origination services within its network that may include a stricter application review process.
- c.** Citizens Acceptable Use Policies, VoIP Terms and Conditions and Terms of Service are published on Citizens website and will be updated as necessary to reflect our stance on illegal robocalling.

IV. Telephone Validation Process

- a.** A subscriber is permitted to use a telephone number as their caller identity, if a number is directly managed by Citizens and/or obtained by Citizens via an underlying partner. Citizens has established a process for ensuring subscribers are utilizing only telephone numbers assigned to them or have been authorized for use. For subscribers with a single line service, the Metaswitch Class 5 switch has been setup to only accept calls from the number assigned to that subscriber, for services connected via IP, at the time-of-service origination. For subscribers with multi-line telephone systems (MLTS), for services connected via IP, Citizens screens all originating calls and only allows the call to be connected if the originating telephone number matches one of the assigned numbers to that MLTS subscriber.
- b.** Citizens uses the Metaswitch Service Assurance Server (SAS) to track and analyze subscriber originating and terminating calls.

V. Network Monitoring and Mitigation

- a.** Analyze and Monitor Network Traffic via Metaview SAS. Analyze high-volume network traffic to identify and monitor patterns consistent with robocalls.
- b.** Investigate Suspicious Calls and Calling Patterns via Metaview SAS. Taking appropriate action to identify any party that is suspected of illegal robocalling or spoofing over its network.
- c.** Citizens uses TNS Call Guardian as a third-party validation service to provide analytics to identify the origination or termination of illegal robocalls.
- d.** Citizens may at its discretion impose network-level constraints to include throttling the rate at which the customer can initiate calls, potential suspension of all non-emergency (911) outbound calling services during investigation of reported robocalling and/or initiate a permanent termination of service.
- e.** Citizens currently is registered with and sending the required monthly reports to the Reassigned Number Database per the Second Report and Order on Advanced Methods to Target and Eliminate Unlawful Robocalls (FCC-18-177A1).

VI. Know-Your-Upstream Provider

a. As a rural provider of voice services, Citizens has a long standing relationship with the interconnected carriers from which it directly receives traffic and has confirmed that all carriers with which it exchanges traffic and from which it receives traffic are listed in the Robocall Mitigation Database.

Basic identification information, such as physical business location, contact person(s), state of incorporation, and nature of business, are collected for all of Citizens's interconnected upstream providers. Going forward, all interconnection agreements will include prohibited traffic and traceback language.