

Citizens Telephone Company of Hammond, New York Robocall Mitigation Plan

Citizens Telephone Company of Hammond, New York (Citizens) 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)).

The Citizens' network is 100% non-IP. Citizens provides local service to fewer than 100,000 voice subscriber lines.

All customers are served on the Citizens non-IP network which relies on technology that cannot initiate, maintain, carry, process, or terminate SIP calls.

Robocall Mitigation Plan

All voice traffic that originates on the Citizens network is subject to the following Robocall Mitigation Plan.

Citizens monitors all originating network traffic call detail records for suspicious or abnormal call pattern, volume, or activity. Calls that meet the below qualifying factors are investigated internally to determine if the calls are legitimate or unlawful:

- High-volume voice network traffic
- Large bursts of calls in a short timeframe
- Short duration calls
- Low average call duration
- Low call completion ratios
- Sequential dialing patterns

Investigation

Citizens investigates calls identified by internal traffic monitoring as suspicious calls or those that have abnormal call volumes, patterns, or activity consistent with illegal robocalls.

If Citizens has any other reason to suspect illegal robocalling or spoofing is taking place over its network, Citizens will work internally to identify the party that is using our network to originate, route, or terminate such calls and take appropriate action.

Enforcement

Illegal robocalls and fraudulent spoofing is prohibited on our network. If it is determined a Citizens customer is using our network to fraudulently spoof calls or to originate illegal robocalls, Citizens will either warn the customer to stop such practices or terminate their service as allowed per the Citizens policy.

Know Your Customer

Citizens has procedures in place to prevent new & renewing customers from using our network to originate illegal robocalls. Citizens vets all new customers, business and residential, to validate their identity, physical location and contact person information. Citizens also asks personally identifiable questions for additional security on each account before activating new service or making changes to existing services.

Know your Upstream Providers

Citizens has confirmed that all carriers in which Citizens exchanges traffic are listed in the Robocall Mitigation Database.

Citizens monitors incoming traffic from all connected carriers for suspicious call patterns indicative of illegal robocall activity, notifies the upstream carriers of any such traffic and warns the carriers that if the traffic does not cease, the calls may be blocked from entering the Citizens network. In addition, Citizens is now incorporating traceback and prohibited traffic language in all contractual agreements with new upstream carriers.

Citizens has reviewed the connected carrier's RMPs to learn how the carriers monitor their originating traffic to mitigation illegal robocalls.

Traceback

Citizens commits to cooperating with the Commission, law enforcement, and the industry traceback consortium in investigating and stopping any illegal robocallers that we learn are using our service to originate calls. Citizens will respond to traceback requests from the Commission, civil and criminal law enforcement, and the industry traceback consortium fully and in a timely manner within twenty-four (24) hours.