



EASTEX CELCO, L.L.C. D/B/A EASTEX NET ROBOCALL MITIGATION PLAN AND CERTIFICATION

Eastex Celco, L.L.C. d/b/a Eastex Net (hereafter "ECL"), operating under OCN 690H, is a small, rural competitive local exchange carrier with fewer than 100,000 voice subscriber lines.

ECL relies on its parent company, Eastex Telephone Cooperative, Inc. ("Eastex"), for its network facilities and management, and therefore concurs in the Robocall Mitigation Program (RMP) that Eastex has developed, filed and certified, which is largely re-stated below for ease of reference.

As a voice service provider with a STIR/SHAKEN obligation serving end users, ECL, through Eastex, has implemented the STIR/ SHAKEN authentication framework on the IP portion of its network, and calls it originates on that portion of its network are compliant with 47 C.F.R. § 64.6301(a)(1)-(3). ECL is also a voice service provider without a STIR/SHAKEN obligation serving end users on the non-IP portions of the Eastex network. All calls that originate on Eastex's network, including calls that originate through ECL, are subject to Eastex's Robocall Mitigation Program ("RMP").

Eastex has implemented the following reasonable steps, among others, to avoid originating illegal robocall traffic as part of its RMP:

STIR/SHAKEN Implementation

- Eastex obtained an SPC Token from iconectiv, the STIR/SHAKEN Policy Administrator, which includes Service Provider Codes (SPCs) for both Eastex and ECL.
- Eastex submitted its SPC Token with a Certificate Signing Request (CSR) to Ribbon, an approved Certification Authority (CA).
- Eastex received the STIR/SHAKEN digital certificate from Ribbon, giving Eastex the ability to sign outbound calls.
- On the portions of its network on which it has implemented STIR/SHAKEN, Eastex:
 - Has implemented the Ribbon Call Trust STIR/SHAKEN solution to provide robocall analytics and reputation scoring of Eastex's outbound traffic.
 - Performs analyses of various reports to evaluate the likelihood that specific calls should be blocked.
 - Uses Ribbon's C15 Call Controllers and an SBC and Ribbon PSX using REST for Reputation Scoring service.
 - Uses its SPC Token Certificate to digitally sign calls, which are then verified throughout the network, ensuring authenticity of the Caller ID.

General Robocall Mitigation Procedures for Non-IP Portions of the network

- Throughout its network, Eastex:
 - Blocks calls originating from numbers that are not valid North American Numbering Plan (NANP) numbers, known numbers not allocated to a provider,



- and numbers not assigned to an Eastex subscriber or otherwise set aside for outbound call use.
- Investigates and identifies the sources of calls that are unlawful or illegitimate.
- Monitors all originating network traffic for suspicious or abnormal call volume or activity. Calls that meet specific qualifying factors are investigated internally to determine if the calls are legitimate or unlawful.
- Eastex and ECL offer several line-specific features which can assist customers with blocking unwanted calls. These include:
 - Anonymous Call Rejection – Allows customers to automatically reject all calls that have been “blocked” and therefore marked anonymous by the calling party. When Anonymous Call Rejection is active, the called party receives no alerting (ringing) for a call that has been rejected. The call is routed to a denial announcement and subsequently terminated.
 - Selective Call Acceptance – Permits a customer to select a maximum of eight (8) specified telephone numbers within the customer’s local calling scope, Extended Area Calling scope, or Long Distance Telecommunications Network (where facilities permit) from which the customer is receiving calls.
 - Selective Call Rejection – Permits a customer to block an incoming call and/or calls from a maximum of eight (8) specified telephone numbers within the customer’s local calling scope, Extended Area Calling scope, or Long Distance Telecommunications Network (where facilities permit), and functions as a screening service for the customer.
- Eastex is also monitoring and participating in industry working groups to address STIR/SHAKEN standards through its membership in WTA and NTCA, as well as through Eastex’s vendor partnerships with JSI, Vantage Point, Sinch, Ribbon, and others.

Traceback

ECL is committed to cooperating with the Commission, law enforcement, and the industry traceback consortium in investigating and stopping any illegal robocallers that use ECL’s service to originate calls. ECL is committed to responding fully and within 24 hours to all traceback requests from such entities. ECL has dedicated a team to respond to call traceback requests, and has established call traceback contact information on its website at <https://www.eastex.com/call-traceback/>. All robocall traceback requests should be forwarded to traceback@eastex.com.

Know your Customer

ECL has procedures in place to prevent new and renewing customers from using its network to originate illegal robocalls. ECL thoroughly vets new residential and business customers by asking personally identifiable questions for additional security on each account before activating new service or making changes to existing services.

Know your Upstream Provider

Eastex has procedures in place to know its upstream providers, including the upstream providers of ECL, to the extent they are different, to mitigate illegal robocalls. Eastex knows all the carriers from which it receives traffic and has confirmed that all of the carriers are listed in the Robocall



Mitigation Database. Eastex has also reviewed the connected carriers' RMPs to learn how the carriers monitor their originating traffic to mitigate illegal robocalls. In addition, Eastex is now incorporating traceback and prohibited traffic language in new contractual agreements with upstream carriers.

Role in the Call Chain

On behalf of itself and ECL, Eastex originates and terminates voice traffic on its own network facilities. Eastex does not act as a transiting provider, except for voice traffic originating and terminating within its own network through a tandem office.

Contractual Provisions

ECL is now incorporating traceback and prohibited traffic language into new contractual agreements with upstream carriers, where possible. In addition, Eastex has filed tariff language with the Public Utility Commission of Texas explicitly conveying that Eastex will block calls identified as illegitimate and/or malicious in intent, such as in the event of origination of illegal robocalls, and will take appropriate actions to prevent further illegitimate activity, including but not limited to termination of service. By adding this tariff language, Eastex has made clear that end users originating illegal robocalls are using the service in an unlawful manner and will be subject to call blocking procedures and possible termination of service. ECL also includes rules and regulations in its Telecommunications Tariff on file with the Public Utility Commission of Texas specifically pertaining to the use of service and facilities and prohibits customers from using service for obstructing service or conducting illegal robocall activities.

Enforcement

If it is determined an ECL customer is originating prohibited unlawful robocalls on Eastex's network, ECL and Eastex will: block the unlawful traffic, warn the customer to stop originating illegal robocalls, and if the customer does not cease originating illegal calls, terminate their service as allowed per ECL's tariffs and/or contracts that define the circumstances by which ECL will suspend or terminate service to a customer.

Customer Education

Eastex disseminates information through its newsletters and social media channels to educate both Eastex and ECL customers on how to protect themselves from becoming a victim of unlawful robocalls. These educational materials also provide the process to report complaints related to robocall activity.

Certifications

ECL hereby certifies that it has not been prohibited from filing in the Robocall Mitigation Database. ECL has not been subject to a commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing, a deficient Robocall Mitigation Database certification or mitigation program description.