



ROBOCALL MITIGATION PLAN

Corporate Information

Service Electric Cablevision, Inc. ("SECV"), a Pennsylvania Corporation, is a reseller that partners with Alianza, Inc., a Delaware Corporation, to provide Voice Over Internet Protocol (VoIP) to our residential customers. Commercial customers are provided VoIP through a partnership with Ironton Telephone Company, a Pennsylvania Corporation. Both partners are listed in the Robocall Mitigation Database and have their own Robocall Mitigation Plans.

In accordance with 47 CFR §64.6305(e), SECV has designated a point of contact to receive notice of any illegal robocall mitigation-related issues. That person's name, title, address, phone, and email address are available in the Robocall Mitigation Database.

Stir/Shaken Certification

SECV's customers use Alianza and Ironton Telephone's networks. Both certify that all voice traffic originating on its network is authenticated, in accordance with 47 CFR §64.6301.

Know Your Upstream Provider

Both partners have existing agreements with Tier-1 carrier service providers, from which it facilitates the provision of carrier services to SECV. All those carriers are listed in the RMD.

Know Your Customer

SECV requires all customers to provide valid government-issued identification, including legal name, birthdate, address of service, address for mailing if different, as well as a social security number.

Policy Against Illegal Robocalling

SECV requires all customers to sign service agreements that outline the policies, terms, and conditions of service. All agreements contain a provision that services shall not be used for any unlawful purpose or for any use for which Customer or user has not obtained all required governmental consents, approvals, authorizations, licenses, and permits. SECV reserves the right to act immediately and without notice to terminate or suspend the services.

Specific Reasonable Steps Taken to Avoid Originating Illegal Robocall Traffic

- SECV, through its partner, Alianza, has implemented a proprietary fraud detection process for its residential customers that analyzes high-volume network traffic to evaluate compliance with a variety of fraud detection indicators and fraud prevention best practices. The fraud detection system triggers a notification to SECV as to the specific residential account where fraudulent activity may be occurring.
- SECV, through its partner, Ironton Telephone, uses Ribbon Communications' Session Border Controllers ("SBC") and PSX policy server for all SIP traffic and is utilizing Neustar as part of its mitigation plan for the remaining amount of TDM traffic for its commercial customers. Ribbon PSX and Ribbon analytics monitors high-volume network traffic to evaluate compliance with a variety of fraud detection indicators and fraud prevention best practices. Daily, weekly, and monthly reporting provides data on the volume of completed and failed transactions per customer. Geo Fraud profiles block IP traffic from non-US addresses unless specifically requested for use.
- SECV requires all customers to adhere to the terms and conditions of phone service agreements that contain provisions regarding acceptable or fair usage of services and allow for termination of services in the event of misuse of services.

Commitment to Traceback Cooperation

SECV, as a reseller and in conjunction with its partners, commits to responding fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium. SECV will cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.