

**The New Knoxville Telephone Company
Goldstar Communications, LLC**

ROBOCALL MITIGATION PLAN

The New Knoxville Telephone Company, an incumbent local exchange carrier, and its affiliate Goldstar Communications, LLC (together, “Company”), have adopted the robocall mitigation plan to attempt to limit the potential for the origination of unlawful robocalls by its customers on its network.

Caller Authentication

Company has implemented the STIR/SHAKEN call authentication framework for the calls that originate in IP. Company qualifies for an extension of the deadline to implement STIR/SHAKEN with respect to the non-IP portions of its network (which utilize Time Division Multiplexing technology) pursuant to Sections 64.6304(d) and 64.6303(a) of the FCC’s rules and is participating, through its membership in ACA Connects, in the ATIS Non-IP Authentication Task Force that is working to develop a non-internet Protocol caller identification authentication solution.

Know-Your-Customer Policies

Subscriber Vetting: Company vets the identity of its customers when approving an application and entering into an agreement to provide telephone service. As part of this vetting process, Company visits each location where service will be provided and collects the customer’s legal name and address and other contact information. Company’s services are provided to fixed locations and services are installed on location by its personnel, so it knows the actual location of its customers. This information enables Company to validate the identity of potential customers prior to provisioning of service. Service will not be provided if a new customer’s identification cannot be verified.

Contractual Terms: Company’s terms of service terms of service prohibit the use of its telephone service for fraudulent or unlawful acts or purposes, and permits Company to terminate a customer’s service for violations of its terms.

Use of Call Analytics to Identify and Block Unlawful Traffic

Company uses software provided by TransNexus to monitor outbound voice traffic in real time to attempt to detect and prevent the origination of illegal robocalls. The software provides detailed reporting identifying suspected illegal robocalls and alerts for calls where the calling number is invalid, unallocated, on a Do Not Originate list, in the FCC consumer complaint database, or has a poor reputation. Company promptly investigates identified calls to determine if the caller was attempting to originate unlawful robocalls. Company also uses call detail records to gauge typical call volume and potential reasons for significant deviations from the typical call volume. If Company determines that a caller was attempting to originate unlawful robocalls, it will take action commensurate with the severity of the customer’s offense,

including, but not limited to, providing the customer with a warning or terminating the customer's service.

Cooperation with the Traceback Group, Law Enforcement and Government Agencies

Company commits to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement authorities, government agencies, and the Industry Traceback Group (ITG) to investigate and address suspected unlawful robocalls originated on its network.

Company committed to fully complying with the Commission's robocall blocking requirements. Company confirms that it will block calls and traffic within its control that: (1) are identified in any public notice or order released by the FCC; (2) are substantially similar to the types of traffic identified in any public notice or order released by the Commissions; or (3) include a caller ID number or name that is on the DNO list issued by the ITG.

Knowledge of Upstream Providers

Company utilizes only a small number of well-known, reputable upstream providers and has verified that each of them are registered in the Robocall Mitigation Database.