

CASTLEBERRY TELEPHONE COMPANY, INC.

P.O. BOX 37
CASTLEBERRY, ALABAMA 36432
251-966-2110

ROBOCALL MITIGATION PLAN

April 17, 2024

Castleberry Telephone Company, Inc. (“Castleberry”) is a rural telephone company, as defined in 47 U.S.C. § 153, and an Incumbent Local Exchange Carrier (“ILEC”), as defined in 47 U.S.C. § 251(h) and is authorized to provide Telecommunications Services in the State of Alabama.

Pursuant to a final rule effective January 8, 2024, the Federal Communications Commission (“FCC”) updated its Robocall Mitigation Database (“RMD”) certification requirements. *See FCC Report and Order*, CG Docket No.17-59, FCC 23-37, 88 Fed. Reg. 43446 (May 19, 2023).

Pursuant to those rules, “all providers, regardless of whether they are required to implement STIR/SHAKEN—including all intermediate providers and providers that lack control over the network infrastructure necessary to implement STIR/SHAKEN—are now required to file certifications and robocall mitigation plans to the [RMD].” *See Public Notice*, DA 24-73, WC Docket No. 17-97 (Jan. 25, 2024).

Castleberry is subject to a continuing exemption from implementation of STIR/SHAKEN because its network “rel[ies] on technology that cannot initiate, maintain, carry, process, and terminate SIP calls.” *See* 47 CFR § 64.6304(d). Castleberry is in the process of upgrading its network to comply with the requirements of 47 CFR § 64.6303(a)(1) and intends to fully

implement the STIR/SHAKEN framework as required in § 64.6301 throughout its network once that upgrade is complete.

As a small business entity, Castleberry acknowledges that, because the FCC recognizes the burden and economic impact of its final rule, it has “allowed flexibility where appropriate to ensure that small providers, can determine the best approach for compliance based on the needs of their networks.” *See FCC Report and Order*, at ¶ 76.

Pursuant to 47 CFR § 64.6305(d)(1), the FCC requires all voice service providers certify in its RMD one of three (3) options: 1) fully implemented STIR/SHAKEN; 2) partially implemented STIR/SHAKEN and have instituted a robocall mitigation program to ensure that they are not originating illegal robocalls; or 3) not implemented STIR/SHAKEN but have instituted a robocall mitigation program to ensure that they are not originating illegal robocalls.

As of April 17, 2024, Castleberry has not implemented STIR/SHAKEN on any portion of its network but has instituted the following mitigation program:

1. Castleberry will respond within 24 hours to all traceback requests from the FCC, law enforcement, and the industry traceback consortium and will cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

2. Castleberry will take steps to mitigate illegal traffic when notified by the Enforcement Bureau.

3. Castleberry will take affirmative, effective measures to prevent new and existing customers from making or originating illegal robocalls.

4. Castleberry will increase business-oriented steps until STIR/SHAKEN can be implemented including investigating with the customer if specific traffic is legitimate or illegitimate.

5. Castleberry will increase due diligence related to reviewing call volumes. The Company is aware that knowledge of our customers and due diligence related to call volumes is critical until STIR/SHAKEN is implemented.

6. Castleberry will make every effort, to the best of our abilities, to block a call if it is highly likely to be illegitimate such as:

a. The originating telephone number should be network-blocked because it shows up on a Do-Not-Originate list or is an unallocated, unused, or invalid number.

b. Because reasonable analytics indicated the call is likely malicious in intent. For example, a significant change in a business' originating traffic patterns to suddenly become high volume, very short duration calls might indicate they have been hacked.

7. Castleberry has language in the Company's Terms and Conditions which require compliance "with all applicable federal, state and local laws, rules and regulations" and an Acceptable Use Policy which "prohibits service uses and activities that are illegal, infringe on the rights of others, or interfere with or diminish the use and enjoyment of the service by others."

8. Castleberry utilizes a combination of internal tools and third-party solutions to check for Do Not Originate ("DNO") numbers. In addition, the Company utilizes a combination of internal tools and third-party solutions to detect invalid phone number formats, area codes, and unassigned number blocks. The Company also utilizes data analytics to detect and investigate irregular and unexpected calling patterns, originating number use against customer profiles.

9. Castleberry uses data systems for analytics and reviews to identify illegal robocalling. In addition, we follow the best practices for vetting caller identity described by the North American Numbering Council ("NANC") Call Authentication Trust Anchor Working Group!¹ The process includes: 1) Monitoring the network to identify suspicious traffic patterns; 2)

¹ See <https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>.

limiting customers' capacity via call per second and/or concurrent session limits; and 3) regularly checking call patterns for possible abusive traffic.

10. Castleberry has implemented an "Red Flag" identity theft prevention program to detect suspicious activity and mitigate identity theft.

11. The company utilizes the mitigation technique of "Know Your Customer." The company is a small, long-established provider that maintains a close relationship with its subscribers and knows its customers. Its customers are generally "mom and pop" users and few of its total customer base have enough call paths to generate the high volume of traffic associated with robocalling allowing us to use targeted in-house analytics to monitor, alert and apprehend suspected robocalling activities.