

DISH Wireless L.L.C. Robocall Mitigation Program (Updated Oct. 31, 2024)

DISH Wireless L.L.C. (“DISH”) submits this Robocall Mitigation Program as required by 47 C.F.R. § 64.6305.

DISH has certified that all voice traffic that originates on its network is authenticated with STIR/SHAKEN, pursuant to 47 CFR § 64.6301(a). As detailed below, DISH has taken a number of reasonable steps to avoid originating, carrying, or processing illegal robocall traffic on its network. 47 C.F.R. § 64.6305(a).

1. “Know-Your-Customer” Procedures

DISH takes reasonable steps to prevent new and renewing customers from originating illegal calls, including through its “know-your-customer” procedures.

Additionally, all subscribers are subject to DISH’s fraud prevention program. In its terms and conditions, DISH makes clear that a subscriber’s account is for personal use only and cannot be used for commercial purposes such as telemarketing, autodialing, or monitoring or for sending spam, mass automated communications. DISH also prohibits subscribers from impersonating others, using fake or forged headers, fabricating domain names, and other types of deceptive addressing and spoofing. DISH reserves the right to suspend or terminate an account without notice for engaging in any of those prohibited practices. DISH also has the ability to block voice traffic when necessary.

2. “Know-Your-Upstream Provider” Procedures

DISH executed a Master Services Agreement (“MSA”) with Peerless Network, Inc. (“Peerless”) as DISH’s exclusive voice service aggregator for both upstream and downstream traffic. Thus, Peerless is DISH’s only upstream provider. Peerless certified complete STIR/SHAKEN implementation in the Robocall Mitigation Database and filed a Robocall Mitigation Program as a gateway provider in November 2023. The MSA contains the following provisions to protect DISH’s network from robocalls:

- DISH and Peerless will work together to meet regulatory obligations and provide information required for FCC forms and other state or local regulatory filings;
- Auto-dialers, continuous call session connectivity, fax broadcasting, fax blasting, mass calling or any other blasting activities are not permitted. If such activity is detected, Peerless reserves the right to take curative action;
- Peerless shall provide 365 day / 7 days a week / 24 hours per day fraud monitoring and will offer fraud monitoring and detection and mitigation processes and capabilities for both national (e.g. Robocalling) and international calls (e.g., proactively blocking high risk destinations to avoid potential risk and exposure or proactively shutting down traffic if a threshold is exceeded on a particular destination);
- DISH and Peerless will work to address unlawful use in a timely manner and will work cooperatively with industry, law enforcement, governmental entities,

regulatory entities, and other carriers, to address issues related to illegality, fraud and abuse;

- DISH will use commercially reasonable efforts to prevent unauthorized, illegal, or fraudulent use of the services provided by Peerless, and shall terminate any unauthorized, illegal, or fraudulent user access;
- Peerless must cooperate fully with traceback requests;
- Peerless may take commercially reasonable action on offending numbers in order to minimize misuse; and
- Peerless shall require connecting carriers to provide STIR/SHAKEN for VoIP calls in a manner that is consistent with Commission requirements.

In December 2023, DISH executed an Amendment to the MSA to utilize Peerless' robocall mitigation product, TNS Call Guardian. TNS Call Guardian is deployed on Peerless' network and tags incoming calls with a reputation score to protect DISH's customers from unwanted robocalls. Calls with a reputation score below a certain threshold will be tagged as "spam likely" for the end user, who can then use this information to determine whether to answer the call. Pursuant to Peerless' contractual obligations, Peerless must employ commercially reasonable efforts to tag calls identified as spam and/or fraudulent.

3. Call Analytics Systems

In addition to Peerless' TNS Call Guardian tool, DISH also uses a DISH programmed fraud management tool to monitor network-based voice traffic to identify potentially fraudulent activity. Specifically, DISH programmed the tool to look for the following scenarios:

- Detect a high number of outgoing voice calls with a small duration and with a high destination dispersion in a single day;
- Detect a high number of incoming calls with a high origin dispersion in a single day;
- Identify calls with a destination number that belongs to a risky list number.

Once a certain threshold is met, the fraud management tool will set off an alarm that triggers an investigation by a fraud analyst. If necessary, the analyst can suspend or terminate the user/account responsible for originating the fraudulent activity.

4. Commitment to Respond Fully to Traceback Requests

DISH commits to fully respond to traceback requests from the Federal Communications Commission, law enforcement, and the industry traceback consortium within 24 hours, pursuant to 47 CFR § 64.1200(n)(1); 47 CFR § 64.6305(a)(2). DISH also commits to fully cooperating with such entities in investigating and stopping illegal robocallers that use its service to carry or process illegal calls. 47 CFR §§ 64.6305(a)(2), 64.6305(d)(2)(iii).

5. *Company Information*

DISH Wireless L.L.C. is a limited liability company and is a wholly owned, indirect subsidiary of DISH Wireless Holding L.L.C. DISH Wireless Holding L.L.C. is a wholly owned subsidiary of DISH Network Corporation. On December 31, 2023, DISH Network Corporation was acquired by EchoStar Corporation (“EchoStar”).

The principals that may exercise management or control of DISH Wireless L.L.C. are:

- Charles W. Ergen, Co-founder and Chairman of the Board
- Cantey Ergen, Co-founder and EchoStar Director
- Hamid Akhavan, President, Chief Executive Officer and EchoStar Director
- Dean Manson, Chief Legal Officer and Secretary
- Gary Schanman, Executive Vice President and Group President, Video Services
- George R. Brokaw, EchoStar Director
- Jim DeFranco, Co-founder and EchoStar Director
- John Swieringa, President, Technology and Chief Operating Officer
- Kathleen Q. Abernathy, EchoStar Director
- Lisa W. Hershman, EchoStar Director
- Milton (Trip) von Minden, Vice President, Tax
- Paul Gaske, Chief Operating Officer, Hughes
- Paul W. Orban, Executive Vice President and Chief Financial Officer, DISH (Principal Financial Officer of EchoStar)
- R. Stanton Dodge, EchoStar Director
- Stephen Bye EchoStar Director
- Tom Ortolf, EchoStar Director
- William D. Wade, EchoStar Director

CERTIFICATION PURSUANT TO 47 C.F.R. § 64.6305(d)(3)(ii)

Pursuant to 47 C.F.R. § 1.16, I declare under penalty of perjury that the statements contained within the foregoing Robocall Mitigation Program are true and accurate to the best of my current information, knowledge and belief.

Executed on October 31, 2024

A handwritten signature in black ink, appearing to read "Alison Minea", is written over a horizontal line.

Alison Minea
Vice President and Associate General Counsel,
Regulatory Affairs
DISH Wireless L.L.C.