

MEDIACOM WIRELESS DBA MEDIACOM MOBILE - ROBOCALL MITIGATION

MEDIACOM WIRELESS, LLC. STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN (RMP)

Pursuant to 47 C.F.R. § 64.6305, Mediacom Wireless, LLC d/b/a Mediacom Mobile, (“Mediacom”) submits this report on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls, as of February 27, 2026. Mediacom reserves the right to modify, add, delete or otherwise alter any of the policies and procedures described in the plan at any time as it deems appropriate to reflect its business, its capabilities, and its needs.

COMPANY BACKGROUND

Mediacom Wireless, LLC dba Mediacom Mobile is a C-Corporation formed under the laws of Delaware and is a registered carrier with the FCC. The Company holds the FRN/CORES ID Number: 0031055387 and holds 499 Filer ID Number: 836567.

Mediacom Wireless is a Mobile Virtual Network Operator (MVNO) and provides cellular service to individual end user subscribers in the United States. It also provides interconnected VoIP telephone service, internet and cable TV services, to residential and business customers. Mediacom serves customers in 1,500 communities in 22 states.

By nature of Mediacom’s MVNO classification the Company relies on a third-party carrier’s network in order to offer cellular service to end users. As Mediacom is an MVNO and has no real control over the facilities/network infrastructure necessary to implement any form of STIR/SHAKEN framework (since an MNVO does not own its infrastructure). Mediacom has no switches, owns no spectrum licenses, and holds no rental or lease space on any Cellular towers.

Based on the nature of the service which Mediacom offers to individual cellular subscribers, the risk for Robocalling, erroneous telemarketing, and other possible questionable activity is extremely low. Since the service is provisioned on a single cellular device to retail users, which in most cases is not compatible with auto dialers, or other tools that could generate High Volume Short Duration (HVSD) calling thus the risk for any form of robocalling is extremely and inherently low.

In light of the low risk of illegal calls being originated, Mediacom has tailored its Robocall Mitigation Program based on the low risk of illegal robocalls being originated on its networks. The reasonable measures Mediacom takes given the level of risk it faces are described in this plan.

Mediacom Wireless, LLC primary place of business is:

1 Mediacom Way
Mediacom Park, NY
10918
Website: <https://www.mediacommobile.com>

Company Leadership:

CEO: Giuseppe B. Commisso
1 Mediacom Way,
Mediacom Park, NY
10918
Phone: 845-443-2600

MEDIACOM WIRELESS DBA MEDIACOM MOBILE - ROBOCALL MITIGATION

Email Address: jcommisso@mediacomcc.com

COO: John G. Pascarelli

1 Mediacom Way,
Mediacom Park, NY
10918

Phone: 845-443-2600

Email Address: jpascarelli@mediacomcc.com

Designated RMD Contact:

Name: Helen S. Bertona

1 Mediacom Way,
Mediacom Park, NY
10918

Phone: 845-443-2405

Email Address: hbertona@mediacomcc.com

STIR/SHAKEN Implementation

Mediacom Wireless has no defined implementation related to STIR/SHAKEN and the parameters of call authentication framework. As an MVNO Mediacom is not able to implement SIR/SHAKEN in any manner. Since Mediacom lacks control over the facilities and network infrastructure necessary to implement STIR/SHAKEN, and it has no defined infrastructure Mediacom has no ability to assign its own calls.

Therefore, Mediacom Wireless is excluded from the FCC's STIR/SHAKEN implementation obligation pursuant to paragraph 40 of the FCC's First Call Authentication Report and Order. Alternatively, Mediacom relies on its underlying carrier partner(s), which own and maintain the network infrastructure, to implement and utilize STIR/SHAKEN authentication.

In relationship to the initial, and subsequent FCC Orders concerning STIR/SHAKEN and the Robocall Mitigation Database (RMD), the Company clearly serves as a voice service provider in the call chain and is without STIR/SHAKEN obligation.

ROBOCALL Mitigation Plan

As mentioned previously, as an MVNO Mediacom is at minimal risk to have any Robocalling taking place since the Service the Company provides is of individual retail cellular subscriber use.

Customer Due Diligence

Mediacom Wireless offers only Post-Paid plans.

- Mediacom conducts due diligence and credit review before establishing a contractual relationship with customers. For residential customers, Mediacom collects the customer's name, service address, billing address. For business customers, Mediacom collects the business name, service address, billing address, employer identification number, and contacts for billing purposes from business customers. Mediacom also collects the name of the owner, the authorized signer, and a description of the type of business a customer conducts for enterprise and small business customers. Mediacom matches information gathered from all potential customers with publicly available information to verify correlation to its internal maps to verify accuracy and serviceability. Mediacom conducts a credit check for all customers and confirms customers do not have bad debt with Mediacom.

MEDIACOM WIRELESS DBA MEDIACOM MOBILE - ROBOCALL MITIGATION

- Mediacom collects information for customers who are porting numbers. For both residential and business customers, Mediacom collects the number, customer names, and account number associated with the prior carrier and also confirms the number is still active with the current carrier.

PREVENTING ILLEGAL ROBOCALLS

As an MVNO that originates end user calls, Mediacom does not deal with any upstream providers. All calls are routed through its underlying carrier's network upon origination and the Company has no involvement in any kind related to provisioning.

Mediacom has reliance upon its wholesale provider/underlying carrier with which it partners for service delivery and that partner then provides Mediacom notices of intention to block relevant calls either on its own or at the request of Mediacom.

However, Mediacom itself does not have or use any call analytics systems to identify and block illegal traffic since it has no control over the network in any manner, and as mentioned immediately informs its underlying provider of any steps that should be taken to halt or suspend any possible or actual activity unless provided by the underlying carrier who initiates those steps prior to any notification by Mediacom.

TRACEBACK AND INQUIRY & RESPONSE

- Mediacom Wireless has designated an individual as a dedicated point of contact for addressing traceback requests, and a backup person to that individual. It will provide this information to the ITG upon receipt of the first request from the ITG, as requested in ITG's guide for service providers. Mediacom Wireless will endeavor to follow the relevant ITG Best Practices to facilitate its response to traceback requests, including specifically:
 - **Dedicated Point of Contact** – Mediacom Wireless has designated an individual as a dedicated point of contact for addressing traceback requests, and a backup person to that individual.
 - **Ongoing Coordination** – Mediacom Wireless will coordinate with the ITG and our voice service provider in relation to instances of suspicious traffic, including exchanging information related to such traffic and ad hoc follow-up as appropriate.
 - **Prompt Investigation and Response** – Upon receiving a traceback request from the ITG, Mediacom Wireless will endeavor to initiate investigation of the source of suspicious traffic within four (4) business hours after receiving a traceback request and strive to complete the investigation and response to the request through the traceback portal within 24 hours. In the event if Mediacom is unable to respond to a traceback request, it will provide sufficient information in the traceback portal as to why it is unable to respond.
 - **Privacy of Traceback Investigations** – Mediacom Wireless will not share information about traceback investigations with other providers involved in the traceback investigation except with the underlying service provider and the ITG, or when pursuant to a valid legal process.
- Mediacom Wireless maintains current and correct information about its customers so that it can provide accurate responses to traceback requests.

MEDIACOM WIRELESS DBA MEDIACOM MOBILE - ROBOCALL MITIGATION

COMPANY DECLARATION

Mediacom Wireless is not currently subject to a formal Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing.

Mediacom Wireless has the right to update, modify and/or change this plan at any time which such changes made by the Company designated individual; when, and as the Company business model may change. Company shall immediately upload the new plan to the RMD.