

CHARTER COMMUNICATIONS, INC.
ROBOCALL MITIGATION PROGRAM

Pursuant to 47 C.F.R. § 64.6305(a), this document describes the program implemented by Charter Communications, Inc. (“Charter”), on behalf of itself and its affiliated voice service provider operating companies, to avoid originating illegal robocall traffic and to mitigate illegal robocalling.¹

1. Avoiding originating illegal robocall traffic.

1.1. *STIR/SHAKEN*. Charter has fully implemented the STIR/SHAKEN protocol across its network and signs all Internet Protocol (IP) calls that it originates. On or before June 30, 2021, Charter began verifying caller identification information for all SIP calls it receives from other voice service providers and intermediate providers, and for all SIP calls that have been authenticated and terminate on Charter’s network. Charter completed implementation of the STIR/SHAKEN framework throughout its voice core network in December 2019. Specifically, Charter installed proprietary 3rd party STIR/SHAKEN technology within Charter’s voice core network, and integrated the STIR/SHAKEN call flows within the call routing architecture of Charter’s voice core network. These changes enable Charter to sign calls originating from its network, and to verify inbound calls coming into its network.²

1.2. *Knowing our customers*. Charter supports the State Attorneys General in their effort to stop illegal and unwanted robocalls and incorporates the Anti-Robocall Principles into our business practices including Principle #5, Confirm the Identity of Commercial Customers. Charter takes steps to know its commercial customers by implementing various Know Your Customer (“KYC”) protocols which depending on the product may include collecting information such as physical business location, contact person(s), state of incorporation, and the nature of the customer’s business. For retail Voice services

¹ Charter provides two types of voice service: interconnected voice over internet protocol (“VoIP”) service, which it offers under its “Spectrum Voice” mark, and wireless service, which it offers as its “Spectrum Mobile” mark. Charter offers Spectrum Voice through its individual operating entities located in each state where Charter operates and transports its VoIP calls over its own private network.

² Spectrum Mobile, LLC is a mobile virtual network operator (“MVNO”) reselling mobile services of an underlying mobile network operator (“MNO”) to consumers under the “Spectrum Mobile” brand name and to businesses under the “Spectrum Business Mobile” brand name. As an MVNO, Spectrum Mobile operates as a reseller of the voice component of the service and lacks control of any network infrastructure and facilities necessary to implement STIR/SHAKEN. Spectrum Mobile does not own or operate the network associated with the voice service, nor does Spectrum Mobile have access to the underlying network for monitoring, detection, or authentication activities. Additionally, all network-level blocking of harmful traffic is performed by the underlying MNO, except as otherwise described in Section 2.1, Analytics-based Call Blocking, as it pertains to Do-Not-Originate numbers. Retail voice customers of Spectrum Mobile and Spectrum Business Mobile also benefit from the underlying MNO’s call filter tool, which enables customers to screen incoming spam calls, block all known, or suspected fraud and scam calls, and report numbers as spam. Spectrum Mobile works closely with its underlying MNO to ensure that its customers receive the benefits of the robocall mitigation, call authentication, and other activities performed in conjunction with the underlying network.

offered to consumers through Spectrum Mobile³ and Spectrum Voice, prospective customers are required to provide contact details and related information. Additionally, all customers are subject to Charter's terms of service and acceptable use policy ("AUP"), which together prohibit customers from using the service to engage in auto-dialing, non-standard calling patterns, high-volume telemarketing, unusually high traffic volumes, transmission or reception of communications which do not consist of standard residential voice calling, and other practices potentially consistent with illegal robocalling, and which allow for suspension or termination of service upon violation of such prohibitions.

- 1.3. *Active Monitoring.* Charter monitors voice traffic on its network for anomalies, fraud and abuse, and suspicious traffic patterns. Charter may conduct profiling on a per-telephone number basis, to look for patterns or changes in patterns of call volume, duration, and/or call destination that may indicate illegal robocalling activity. If a suspected robocall pattern is identified, we investigate and take action as necessary, including suspending or terminating the suspected customer account, as detailed in Charter's terms of service and acceptable use policy ("AUP").
- 1.4. *Enforcing Contract Terms.* Charter's terms of service incorporate Charter's AUP, which provides additional protections. The AUP restricts the use of auto-dialers and other prohibited robocalling practices, such as illegal number spoofing. Charter investigates all suspected breaches of the AUP and takes actions necessary to correct a breach, up to and including terminating service with the customer.
- 1.5. *Education.* Charter educates its customers about robocall prevention through its website. Charter also provides internal training for our customer service agents so they can educate customers who contact Spectrum Support with robocall concerns.⁴
- 1.6. *Investigations.* Charter investigates all complaints and inquiries relating to potential illegal spoofing or robocalling.
- 1.7. *Robocall Mitigation Database verification.* Charter verifies the registration of potential direct inbound peering partners in the FCC's Robocall Mitigation Database ("RMD"), and those without current registrations are disqualified from doing business with Charter. Charter re-verifies the registrations of current partners every calendar quarter.

2. Protecting Customers from Receiving Robocalls

- 2.1. *Analytics-based Call Blocking.* Charter employs a free, network-level robocall-blocking tool, "Call Guard," enabled by default (with the option for customers to opt out), for

³ Spectrum Business Mobile customers are required to have internet service or sign up for internet service before ordering Spectrum Business Mobile service. Charter knows the physical business location of the internet service and contact person(s).

⁴ See [How to Use Call Guard to Block Robocalls](#) and [Mobile Call Blocking and Spam Call Prevention](#).

Spectrum Voice and Mobile service. Call Guard⁵ uses industry-leading data and predictive analytics to assess incoming calls, applying a score based on the measured risk level, and categorizing malicious or likely fraudulent calls. Call Guard automatically blocks all known or suspected fraud and spam calls for our Spectrum Mobile and Spectrum Voice residential customers. For Business Voice customers, Call Guard blocks all known spam callers and applies a caller ID alert to other suspicious telemarketing or potential spam calls to ensure our customers continue to receive the legitimate calls they need from, e.g., schools or healthcare providers.⁶ For Spectrum Voice Charter also blocks numbers on the Industry Traceback Group's Do-Not-Originate list and offers customers additional free tools through Spectrum.net and the My Spectrum App, including customizing numbers on an "allowed calls" list, accepting only select calls, blocking specific unwanted callers, and blocking anonymous calls. Furthermore, Spectrum Voice includes features to adjust the customer's blocking level.⁷

3. Responding to traceback requests and cooperating with investigations.

- 3.1. Charter actively participates on the Industry Traceback Group, and is a member of the Industry Traceback Consortium Executive and Steering Committees. Through this participation, Charter is committed to responding fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the Industry Traceback Group, and cooperating with such entities to investigate and stop illegal robocallers that may use Charter's service to originate illegal calls.⁸
- 3.2. Charter is committed to responding fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the ITG.

⁵ Call Guard is a service provided by Charter. Charter contracts with Transaction Network Service ("TNS") to perform the analytics. Call Guard is automatically enabled for Spectrum Voice customers. Spectrum Voice customers can adjust their Call Guard sensitivity levels, as desired. Spectrum Mobile customers also have Call Guard automatically enabled. Call Guard for Spectrum Mobile provides SPAM identification and SPAM blocking. Enabling Call Guard for Spectrum Mobile customers instructs Spectrum Mobile's third-party mobile network operator ("MNO") to implement a network-level robocall-blocking tool.

⁶ See [Charter Takes New Steps to Block Robocalls](#).

⁷ See [How to Use Call Guard to Block Robocalls](#).

⁸ Spectrum Mobile cannot perform tracebacks since its an MVNO.

Appendix A

Charter Communications, Inc. Principals

Christopher L. Winfrey	President and CEO
Richard J. DiGeronimo	President, Product and Technology
Jessica M. Fischer	Chief Financial Officer
Jamal H. Haughton	Executive Vice President, General Counsel and Corporate Secretary
Magesh Srinivasan	Executive Vice President, Network Technology Services
Kevin D. Howard	Executive Vice President, Chief Accounting Officer and Controller
R. Adam Ray	Executive Vice President, Chief Commercial Officer

Appendix B

Operating Company Numbers (OCNs)

3839	577C
5606	578C
5607	579C
008E	580C
009E	582C
011F	583C
028G	595J
029G	601D
030G	621D
031G	623D
032G	692F
034G	694F
089J	696F
219G	698F
228H	704C
293C	720G
336E	753E
337E	775C
338E	776C
339E	777C
349D	778C
350D	781C
351D	813D
352D	814D
353D	851F
383E	853C
446G	871D
447D	872D
462C	874D
497G	927D
532D	948F
547D	792K
551D	793K
572H	045L
575C	151M
576C	