COMCAST

July 10, 2019

Commissioner Geoffrey Starks
Federal Communications Commission
445 12th Street SW
Washington, DC 20554

Dear Commissioner Starks:

On behalf of Comcast Corporation, thank you for your letter to Brian Roberts, our Chairman and Chief Executive Officer, regarding the company's ongoing efforts to tackle the problem of illegal and fraudulent robocalling. Comcast agrees that it is critically important to maintain the public's trust in voice services and to protect consumers from harmful calling practices in a robust and responsible manner. As Senior Vice President and General Manager, Broadband, Automation and Communications at Comcast Cable, I have played a lead role in ensuring that tools and technology designed to address illegal and fraudulent robocalling are available to Comcast's customers, and have been asked by Mr. Roberts to provide this response to your letter.

Comcast applauds the Commission's continued efforts to promote the development and availability of robocall mitigation solutions, and is proud to be an industry leader in making cutting-edge tools available for the benefit of consumers. As you know, the Commission has issued a series of orders in recent years authorizing voice providers to deploy such tools. The Commission ruled in 2015 that voice providers may make certain kinds of call-blocking technology available to customers who choose to use such technology, and the declaratory ruling issued last month clarified that voice providers may do so on a default, opt-out basis, provided they satisfy certain conditions (including, among other things, that the underlying analytics must avoid blocking emergency calls, must be adequately disclosed, and must otherwise be "reasonable," and that the provider must designate a point of contact for reporting erroneous blocking). Relatedly, the Commission adopted an order in 2017 specifically permitting voice providers to block calls appearing to originate from invalid, unallocated, and unassigned numbers, as well as from numbers on the industry Do-Not-Originate (DNO) list. The Commission also has been active in promoting the development and implementation of the end-to-end call authentication protocol known as SHAKEN (Signature-based Handling of Asserted Information Using toKENs) and STIR (Secure Telephone Identity Revisited).

Comcast is pleased to report that it is currently employing tools at the network level that automatically block tens of millions of illegal and fraudulent robocalls bound for Comcast's customers, without any extra charge to customers or any need for customer opt-in. Specifically, for Comcast's residential Xfinity Voice and other customers, the company has configured edge devices on its voice network to implement blocking of calls appearing to originate from numbers on the industry Do-Not-Originate list and from invalid or unallocated numbers, consistent with FCC precedent expressly authorizing such call blocking.[1] In May 2019 alone, Comcast estimates that these network-level tools blocked approximately 80 million illegal and fraudulent robocall attempts bound for its customers. By implementing such call blocking in a centralized fashion, Comcast not only can block a significantly greater volume of illegal and fraudulent robocalls, but also can move swiftly to add or remove numbers or ranges of numbers to be blocked as the need arises. This automatic blocking technology is already having a major impact in preventing scammers from defrauding our customers.

Additionally, Comcast currently offers a range of free robocall mitigation tools that its customers may opt in to using,[2] and is exploring how to make certain of these tools available on an opt-out basis, in a responsible manner that comports with the Commission's declaratory ruling and avoids blocking desired communications wherever possible. Comcast is developing plans in the short term to convert one of its existing opt-in blocking tools for Xfinity Voice customers—Anonymous Call Rejection—into a default, opt-out feature that remains free of charge. Comcast's Anonymous Call Rejection tool automatically rejects calls where the caller has chosen to block the display of the caller's name and number. Today, a customer can easily activate this feature either by dialing *77 on his or her Xfinity Voice phone line or by accessing his or her user settings in Comcast's online portal. We currently provide clear activation instructions and other information about this feature on our website,[3] and roughly 40 percent of Comcast's residential voice customers have chosen to use this feature.[4] We expect that activating this tool as a default feature on an informed opt-out basis will significantly increase its already substantial impact.

Comcast also makes blocking applications available that subscribers can customize on an individualized basis and that do not require reconfiguring network equipment or otherwise actively managing the voice network. For example, Comcast makes free Nomorobo

[1] With respect to Xfinity Mobile, its status as a mobile virtual network operator (MVNO) offering service over another provider's cellular network means that it is reliant on the underlying provider's own implementation of network-level blocking functionalities (i.e., those that require reconfiguration and management of the underlying network). Comcast continues to work closely with that provider to ensure that Xfinity Mobile customers receive the same network-level robocall protections as the underlying provider's retail customers.

[2] Comcast also makes clear in its terms of service that the company may suspend customers for using Comcast services to engage in potentially illegal activities, thus enabling Comcast to address any illegal robocalling that might be conducted by a user of Comcast services.

[3] *See* Comcast, "Use the Anonymous Call Rejection Feature with Xfinity Voice," https://www.xfinity.com/support/articles/rejecting-anonymous-calls.

[4] Additionally, Comcast offers its residential Xfinity Voice customers a more tailored robocall mitigation tool called Call Screening (also known as Selective Call Rejection), which enables a customer to create a list of up to 25 callers who, instead of getting through to the customer's phone, will receive an announcement stating that the individual is not available. This tool is similarly easy to activate—either by dialing *60 on an Xfinity Voice phone line and following the prompts to add calling numbers to the list, or by adjusting user settings in Comcast's online portal. Comcast's website also provides activation instructions and other information about this tool. *See* Comcast, "Use the Call Screening Feature with Xfinity Voice," https://www.xfinity.com/support/articles/call-screening.

compatibility available to the vast majority of its residential voice customers nationwide on an opt-in basis.[5] Nomorobo is a third-party cloud-based service that can be configured by consumers to block various types of robocalls, and was featured at the FCC's expo on robocall mitigation technologies in April 2018. We provide an easily accessible webpage instructing customers on how to activate the service,[6] and estimate that Nomorobo successfully blocks roughly 10 million robocalls bound for Comcast residential customers every month. For Xfinity Mobile customers, Comcast recently announced a collaboration with Hiya, another leading call-blocking platform.[7] Under this partnership, Xfinity Mobile customers may now download the Hiya app for free and begin not only receiving alerts about potential spam calls but also blocking them. Hiya also can "identify calls from common businesses to provide clarity on who is calling, and includes a 'neighbor spoofing' blocker, which allows customers to block specific area codes if they notice a lot of unwanted calls coming from them."[8] Comcast provides clear instructions to Xfinity Mobile subscribers for downloading and using the free Hiya app on its website.[9] Comcast is committed to promoting the availability of these services and ensuring that the signup process is as streamlined as possible for our customers.

Moreover, Comcast is pursuing an aggressive timeline for implementing an end-to-end call authentication capability based on the STIR/SHAKEN protocol for our residential Xfinity Voice subscribers—another robocall mitigation tool that will come at no additional cost to our customers. In addition to being at the forefront of developing the STIR/SHAKEN protocol,[10] we are leading the way in deploying this technology. Earlier this year, Comcast implemented the capability to verify calls that contain a STIR/SHAKEN-compliant signature for the company's entire residential subscriber base—enabling Comcast to sign originating and verify terminating calls between its subscribers, and paving the way for the company to begin interoperating with other voice providers that have implemented such capabilities. In March 2019, Comcast and AT&T successfully accomplished an exchange of authenticated calls in a real-world (non-laboratory) setting using phones on the companies' consumer networks—a feat "believed to be an industry first for calls between separate providers."[11] In April 2019, Comcast began

[5] Less than 10 percent of Comcast's residential voice customers choose a plan that does not include the simultaneous ring feature required for Nomorobo.

[6] *See* Comcast, "How to Stop Unsolicited Robocalls to Your Home," https://www.xfinity.com/support/articles/nomorobo.

[7] *See* Comcast, "Xfinity Mobile Collaborates with Hiya to Thwart Mobile Robocalls," Jun 24, 2019, https://corporate.comcast.com/stories/xfinity-mobile-hiya-thwart-mobile-robocalls. As noted above, an application like Hiya does not require any reconfiguration or management of the underlying voice network. Accordingly, unlike the network-level blocking tools described elsewhere, Comcast is able to make this application available to Xfinity Mobile subscribers without relying on the underlying network operator for implementation.

[8] *Id.*

[9] *See* Comcast, "How Do I Block Robocalls," https://www.xfinity.com/mobile/support/article/how-to-block-robocalls.

[10] *See* Comments of Comcast Corp., CG Docket No. 17-59, at 3-4 (filed July 20, 2018) (describing leadership roles of specific Comcast personnel in developing and implementing the STIR/SHAKEN protocol).

[11] Comcast Corp., Press Release, "AT&T, Comcast Announce Anti-Robocalling Fraud Milestone Believed To Be Nation's First," Mar. 20, 2019, *available at* https://corporate.comcast.com/press/releases/att-comcast-announce-anti-robocalling-fraud-milestone-believed-to-be-nations-first; *see also* Eli Blumenthal, *Fight Against Robocalls Continues as AT&T, Comcast Complete Test of Verified Call*, USA Today, Mar. 20, 2019, *available at*

exchanging authenticated calls with T-Mobile as well,[12] and in the coming months Comcast expects to exchange authenticated calls with more providers across the industry.[13]

As these efforts demonstrate, Comcast is dedicated to combatting the scourge of illegal and fraudulent robocalls and empowering its customers with free robocall mitigation tools and technologies. We appreciate your inquiry into these issues and look forward to continuing our close work with the Commission in stopping these abusive practices.

Respectfully submitted,

Eric Schaefer
Senior Vice President and General Manager,
Broadband, Automation and Communications,
Comcast Cable

cc: Brian Roberts, Chairman and CEO, Comcast Corporation

https://www.usatoday.com/story/tech/2019/03/20/at-t-comcast-say-they-making-progress-fight-against-robocalls/3215621002/.

[12] *See* Eli Blumenthal, *T-Mobile, Comcast Turn on Call Verification Between Networks in Latest Robocall Fight*, USA Today, Apr. 17, 2019, *available at* https://www.usatoday.com/story/tech/talkingtech/2019/04/17/t-mobile-comcast-turn-call-verification-fight-robocall-epidemic/3490265002/.

[13] Because STIR/SHAKEN is a network-level functionality that requires reconfiguration and management of the voice network, Xfinity Mobile's status as an MVNO means that it is reliant on the underlying provider's own implementation of such functionalities. Comcast will continue to work with that provider on encouraging implementation of this call authentication protocol for mobile customers.