

# United States Senate

WASHINGTON, DC 20510-1904

February 21, 2020

143

The Honorable Ajit Pai  
Chairman  
Federal Communications Commission  
445 12th Street SW  
Washington, DC 20554

Dear Chairman Pai:

We are writing to ask what further statutory authority the Commission may need to shut down U.S.-based Voice over Internet Protocol (“VoIP”) providers that knowingly serve as gateways for illegal robocall traffic originating overseas.

As the Commission is aware, criminal networks operating offshore are flooding our nation’s telephones with billions of illegal robocalls, in search of victims for their incessant scams. Since 2013, the Senate Aging Committee, on which we serve, has held 25 hearings to highlight a never-ending parade of scams targeting our nation’s seniors. Nearly all of these scams are initiated by offshore con artists who use VoIP and caller-ID “spoofing” to hide their true identity from their intended victims. According to the latest estimates we have seen, scammers now generate four billion unwanted, illegal robocalls targeting Americans every month.

These calls would never reach American consumers without the assistance of so-called “gateway carriers” located in the United States that facilitate the delivery of international traffic onto the U.S. telecommunications system. “Gateway carriers” often transmit massive volumes of highly suspicious robocall traffic with characteristics that should be obvious “red flags.” One is their short duration: 12 seconds, versus five minutes and nine seconds for calls to parties on the caller’s contact list. Other suspicious signs include the number of calls placed per minute, the number of unique caller-IDs used, and suspicious patterns in call destinations (such as sequential calling or geographic concentration).

It may be possible that these and other common markers of illegal robocall traffic could serve as part of a “know your customer” obligation that gateway carriers should be required to follow before placing foreign commercial call traffic on the U.S. telecommunications system. For example, if the gateway provider becomes aware that it is receiving illegal robocall traffic, the gateway provider should be obligated to refuse that traffic or take other measures to eliminate illegal calls. Second, if the gateway provider fails to mitigate illegal calls, carriers at the next level should be allowed to refuse the traffic. It may also be possible to impose these traffic restrictions by contract between telecommunications providers.

We note that the Attorneys General for all fifty states and the District of Columbia have endorsed Anti-Robocall Principles that would require telecommunications carriers to confirm the identities of their commercial customers (Principle Five). With commercial traffic in mind, we would welcome your thoughts with regard to the following questions:

1. Does the Commission have the authority to impose “know your customer” obligations consistent with Principle Five on gateway carriers under existing law?
  - a. If not, what changes to federal law would be required to provide the Commission with this authority?
2. Could U.S. telecommunications carriers impose such “know your customer” obligations by contract?
  - a. If not, what changes to federal law would be required to provide U.S. telecommunications carriers with this authority?
3. What further statutory authority does the Commission need to shut down U.S.-based Voice over Internet Protocol (“VoIP”) providers that knowingly serve as gateways for illegal robocall traffic originating overseas?

We welcome the Commission’s continued attention to the problem of illegal robocalls and spoofing, and look forward to working together with you to bring it to an end.

Sincerely,

  
Susan M. Collins  
United States Senator

  
Kyrsten Sinema  
United States Senator

  
Martha McSally  
United States Senator

cc: Commissioner Michael O’Rielly  
Commissioner Brendan Carr  
Commissioner Jessica Rosenworcel  
Commissioner Geoffrey Starks