

Lumen Technologies and its domestic affiliates (collectively, “Lumen”) collectively are subject to a continuing extension of the June 30, 2021 STIR/SHAKEN implementation date for those portions of its network that rely on technology that cannot initiate, maintain, and terminate SIP calls (“non-IP calls”) pursuant to Section 64.6304(d) of the Commission’s Rules.¹

As required to meet the criteria for that extension, Lumen is participating in a working group that is developing a non-IP call authentication solution.² Lumen has been a leader within the technical standards community since the beginnings of STIR/SHAKEN development. Specifically, Lumen helped to develop the technical industry standards for STIR/SHAKEN through the partnership of the SIP Forum and the Alliance for Telecommunications Industry Solutions (“ATIS”) (also known as the IP-NNI) and is on the Board of Directors of both the SIP Forum and ATIS. In 2020, Lumen agreed to lead the Non-IP Call Authentication Task Force established by ATIS which will complement the work already being performed by the IP-NNI Task Force to address challenges with call authentication on TDM networks and identify viable alternatives for TDM call authentication functionality.³

Lumen has implemented the robocall mitigation program described in Attachment A as to those portions of its network on which it has not implemented the STIR/SHAKEN authentication framework.⁴

Lumen commits to respond fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls. As a founding member of USTelecom – The Broadband Association’s (“USTelecom”) Industry Traceback Group (“ITG”) and a member of its executive committee, Lumen has demonstrated its commitment to the ITG effort to traceback illegal calls to their source. Lumen continues to be a leader in the responding to traceback requests and has both formal and informal ways for the Commission and enforcement agencies to engage with Lumen. Lumen will continue its cooperation with the Commission, law enforcement and the industry traceback consortium in investigating and stopping any illegal robocallers that use its service to originate calls.

¹ See 47 C.F.R. § 64.6304(d).

² *Id.* at § 64.6303(b).

³ See ATIS, ATIS Launches New Non-IP Call Authentication Task Force (May 13, 2020) <https://www.atis.org/press-releases/atis-launches-new-non-ip-call-authentication-task-force/>.

⁴ See 47 C.F.R. § 64.6305(a), (b)(2).

ATTACHMENT A
LUMEN ROBOCALL MITIGATION PROGRAM

Lumen has taken the specific reasonable steps set forth in this attachment to avoid originating illegal robocall traffic as part of its robocall mitigation program. Lumen is continuously analyzing the effectiveness of this program and reviewing best practices in this space. Lumen reserves the right to modify and/or supplement the robocall mitigation measures included here to adapt to risks from bad actors and to improve the overall effectiveness of its program for the benefit of its customers.

- **Network Monitoring Practices.** Lumen continuously monitors its networks for mass calling events and coordinates with other major providers, the ITG, trusted third parties, and key federal agencies to address and mitigate obviously fraudulent calls. In coordination with the ITG, Lumen performs *Do Not Originate* (“DNO”) blocking of government impersonation calls. Lumen also blocks “call back” *Direct Inward Dial* (“DID”) numbers used by such scams, including one-ring scams, and may block calls from numbers associated with mass robocalling scam campaigns as identified by a trusted third party. Lumen stands ready to conduct additional network-level blocking in response to “cease-and-desist” letters issued by the Commission to the extent the recipients of those letters fail to undertake the directed remedial measures.
- **Know-Your-Customer Initiatives.** Lumen employs a variety of “know-your-customer” initiatives to help mitigate the risk that its customers would attempt to use Lumen’s network to initiate an illegal robocalling campaign. Lumen makes reasonable, good faith efforts to validate the identity of its customers, particularly smaller customers that may be more susceptible to identity theft. These measures include, but are not limited to, performing a credit check; requiring customers to demonstrate that they are a legitimate business entity if they are not among the following: a Fortune 500 company, a public company, a state or federal government agency, or a major state university; and monitoring of financial position and payment performance. To comply with the Know Your Customer regulations set forth in the Patriot Act, all customers must be checked against the U.S. Treasury Department’s Office of Foreign Assets Control (“OFAC”) list of Specially Designated Nationals (“SDN”).
- **Contractual Terms and Other Conditions.** Lumen’s service agreements contain acceptable use and traffic integrity terms that prohibit using Lumen’s services for illegal purposes. Network capacity limitations also serve as a check against customers originating large volumes of calls, which are often hallmarks of illegal robocalling campaigns. Large and wholesale customers may also be subject to a review of their call counts, minutes, and target rates on a destination-by-destination basis. New and existing customers are also provided calling party hygiene standards that assist with preventing originating calls with invalid or malformed calling party information as applicable. Customers are also re-evaluated when they order new products or services.

- **NANC Call Authentication Trust Anchor Working Group Best Practices.** Lumen supports the best practices developed by the North American Numbering Council Call Authentication Trust Anchor Working Group: <https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>. While many of those best practices relate to STIR/SHAKEN implementation, Lumen notes that some of the principles identified by that group apply to robocall mitigation, particularly in the areas of customer vetting and network monitoring for suspicious calling patterns. Lumen's robocall mitigation program takes these best practices into account to minimize the risk that Lumen's network could be used for illegal robocalling campaigns.
- **State Attorneys General Anti-Robocall Principles.** Lumen (then CenturyLink) was directly engaged with State Attorneys General in developing a slate of anti-robocall principles designed to help curtail this pervasive and complex problem. Lumen signed onto these principles which generally call for voice service providers to implement call blocking technology on residential VoIP and mobile networks, to know their customers, to actively monitor their networks for robocall traffic, and to cooperate in investigations that trace the origins of illegal robocalls. The full list of principles can be found here: <https://oag.ca.gov/system/files/attachments/press-docs/State%20AGs%20Providers%20AntiRobocall%20Principles-With%20Signatories.pdf>. Through these steps, Lumen and the other voice service provider signatories are mitigating illegal robocalls and aiding state Attorneys General in identifying and prosecuting the bad actors that initiate these illegal calls.

Lumen is committed to doing its part to combat illegal robocalls. As STIR/SHAKEN and other call authentication technology continues to be deployed across all networks, robocall mitigation programs play an important role to curtailing these annoying and harmful calls. Lumen will continue to evaluate the effectiveness of its robocall mitigation program and, if warranted, may modify or supplement the measures identified here for the benefit of its customers.

* * * * *