May 6, 2022

Marlene Dortch, Secretary
Federal Communications Commission
45 L Street NE
Washington, D.C. 20554

Re: Notice of Ex Parte Presentation
***Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59; *Call Authentication Trust Anchor*, WC Docket No. 17-97**

Dear Ms. Dortch:

On May 5, 2022, on behalf of INCOMPAS, VON Coalition, and USTelecom – The Broadband Association (the "Associations"), Chris Shipley, Glenn Richards, Patrick Halley, and the undersigned met virtually with Michele Berlove, Megan Danner, Elizabeth Drogula, Jesse Goodwin, Jonathan Lechter, and John Visclosky of the Wireline Competition Bureau and Mark Stone, Jerusha Burnett, Aaron Garza, Kristi Thornton, and Karen Schroeder of the Consumer and Governmental Affairs Bureau to discuss the Commission's Draft Sixth Report and Order in CG Docket No. 17-59 & Fifth Report and Order in WC Docket No. 17-97 ("Draft Order").[1]

We explained that the Associations view the Draft Order overall as a positive step to addressing foreign-originated illegal robocalls but that there are several aspects of the Draft Order that could be clarified.

1. **Do Not Originate ("DNO") Blocking Requirement.** The Draft Order mandates that gateway providers must block calls based on a "reasonable DNO list."[2] It then suggests that "a reasonable list would need to include, at a minimum, any inbound-only government numbers where the government entity has requested the number be included."[3] Some equipment and switches have limits on the total amount of numbers that can be blocked based on a DNO. To address this limitation, the Industry Traceback Group's Do Not Originate Policy mandates that DNOs on behalf of a government agency "should be *currently* spoofed by a robocaller to perpetrate impersonation-focused fraud" and "the source of a *substantial volume* of illegal calls."[4] The Commission should ensure that providers can rely on the existing ITG DNO list and

---

[1] *Advanced Methods to Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Draft Sixth Report and Order, Seven Further Notice of Proposed Rulemaking in CG Docket No. 17-59 & Fifth Report and Order, Order on Reconsideration, and Fifth Further Notice of Proposed Rulemaking in WC Docket No. 17-97, FCC-CIRC2205-01 (rel. Apr. 28, 2022) ("Draft Order").

[2] *Id.* ¶ 87.

[3] *Id.* ¶ 89.

[4] Industry Traceback Group, Policies and Procedures, Appendix B: Do Not Originate Policy, https://tracebacks.org/wp-content/uploads/2022/04/ITG-Policies-and-Procedures-Updated-Apr-2022.pdf (emphasis added).

otherwise include these reasonable conditions for all DNO requests, whether for government or private organization numbers, to best protect consumers while also accounting for practical technical challenges. Enabling providers to impose reasonable requirements on DNO requests also allows for processes confirming the phone numbers in fact are only used for inbound calling. The Commission can achieve this with the following change to the text in paragraph 89:

> Therefore, we find that a reasonable list would need to include, at a minimum, any inbound-only government numbers where the government entity has requested the number be included. It must additionally include private inbound-only numbers that have been used in imposter scams, when a request is made by the private entity assigned such a number ~~but may impose additional requirements on including those numbers~~. In either scenario, the provider, or the third party that manages the DNO list, may impose reasonable requirements on including the numbers, such as requiring that the number is currently being spoofed at substantial volume.

In addition, the Commission should deem providers that play multiple roles in the ecosystem, including as gateway providers, in compliance with the requirement if they have implemented DNO in some part of their network, even if not in the gateway. This would avoid forcing providers to make inefficient and redundant network investments to certain switches when the providers already have implemented, or could implement, DNO mechanisms elsewhere in their networks that afford robust consumer protection. The Commission can do so through the following text changes in paragraph 91:

> We recognize that providers have used DNO lists to reduce the number of illegal calls that reach consumers. We applaud these industry efforts and find providers that already offer consumer protections through the implementation of DNO in other portions of their network, even if not the gateway, in compliance with this requirement. We find that enlisting all gateway providers in this effort will further reduce the risk of illegal calls reaching consumers.

2. **Know Your Upstream – Effective Steps.** Paragraph 98 of the Draft Order suggests that "[i]f a gateway provider repeatedly allows a high volume of illegal traffic onto the U.S. network, the steps that provider has taken are not effective and must be modified for that provider to be in compliance with our rules."[5] The following paragraph then "recognize[s] that gateway providers cannot prevent all instances of illegal calls from entering the U.S. network," suggesting that "a gateway provider's previously effective steps may become unexpectedly ineffective due to changes in factors outside of the gateway provider's control…"[6]

In some circumstances, provider's mitigation steps may continue to be effective even if illegal calls occasionally enter the U.S. through that provider's network, precisely because "*gateway providers cannot prevent all instances of illegal calls from entering the U.S. network*." This is particularly true where providers serve as the gateway for substantial amounts of foreign-originated traffic that only occasionally yields illegal robocalls. The Commission thus should

[5] Draft Order ¶ 98.

[6] *Id.* ¶ 99.

make clear that occasionally serving as a gateway provider for illegal robocalls, particularly where those illegal calls are an insignificant fraction of that provider's traffic, does not inherently make the provider's practices ineffective. Accordingly, the Commission should make the following changes to the text in paragraph 98:

> If a gateway provider repeatedly allows a high volume of illegal traffic onto the U.S. network, the steps that provider has taken ~~are~~ might not be effective and ~~must~~ may need to be modified for that provider to be in compliance with our rules.

3. **24 Hour Traceback Requirement.** The Draft Order requires that gateway providers respond to tracebacks within 24 hours.[7] The Commission should clarify that the requirement contemplates business hours so that providers are not out of compliance if they fail to respond to tracebacks they receive on Fridays or non-workdays, such as weekends and holidays.

4. **Protection of 911 Calls**. The Draft Order indicates that "[c]onsistent with our existing blocking rules, gateway providers must never block calls to 911 and must make all reasonable efforts to ensure that calls from public safety answering points (PSAPs) and government emergency numbers are not blocked."[8] The draft rule and the Commission's existing requirement, however, suggest that the restriction only applies when "the call is an emergency call placed to 911."[9] Accordingly, consistent with the text of the rule and to avoid any doubt, the Commission should clarify in the text of the Draft Order that the restriction applies only to "emergency call[s] placed to 911" and therefore gateway providers can block calls to 911 that are intended to cause harm to public safety, such as through a telephone denial of service attack, or at the request of the public safety answer point.

Please contact the undersigned if you have any questions.

Sincerely,

/s Joshua M. Bercu/
Joshua M. Bercu
Vice President, Policy & Advocacy, USTelecom

[7] *Id.* ¶ 65.

[8] *Id.* ¶ 94.

[9] Draft 47 C.F.R. 64.1200(k)(5); 47 C.F.R. 64.1200(k)(5).