Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

	)	
In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
	)	
	)	

COMMENTS OF THE VOICE ON THE NET COALITION

The Voice on the Net Coalition ("VON")[1] respectfully files these comments in response to the Petition for Reconsideration and Request for Clarification of USTelecom – The Broadband Association (the "Petition") of the Fourth Report and Order[2] filed May 6, 2021 in the above-referenced proceeding.[3] Throughout these proceedings, VON has supported Commission and industry efforts to substantially reduce the volume of illegal robocalls. Nevertheless, concerns remain that providing unrestricted authority for carriers and analytics engines to block suspect calls could result in many uncompleted, legitimate calls.[4] To address that balance, the Commission adopted specific requirements that callers be notified using SIP codes 607 and 608 when calls are blocked. The Petition questions whether those specific SIP codes should be the only option for providing blocking notification, seeks clarification regarding the types of blocked calls for which notification is required and seeks confirmation that originating carriers have flexibility on how to notify enterprise customers that their calls have been blocked by downstream providers.

[1] The VON Coalition works to advance regulatory policies that enable Americans to take advantage of the promise and potential of IP-enabled communications, including interconnected Voice over Internet Protocol ("VoIP"). For more information, see www.von.org.

[2] *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, Fourth Report and Order, 35 FCC Rcd 15221 (2020) ("*Fourth Report and Order*").

[3] Notice of the Petition was published in the Federal Register, establishing June 4, 2021 as the deadline for filing oppositions. 86 Fed. Reg. 27354 (May 20, 2021).

[4] Comments of the Voice on the Net Coalition, CG Docket No. 17-59 (August 31, 2020).

VON provides the following comments in response to those proposed changes/clarifications, in particular 1) recommending that if the requirement to provide blocking notifications are delayed; analytics-based blocking should be delayed as well; 2) agreeing that voice service providers are required to send notification of blocking only when calls are blocked based on analytics programs; and 3) agreeing that the communication of the SIP response code to the originating voice service provider is the critical requirement for identifying and correcting erroneous analytics-based call blocking.

The Fourth Report and Order, as mandated by the TRACED Act, required voice service providers that block calls to disclose such blocking, establish a process to correct erroneous blocking and promptly resolved disputes.[5] These transparency and redress requirements are evidence the FCC is concerned that service providers might block wanted calls, harming calling parties seeking to transact legitimate business or called parties who might not receive critical information such as fraud alerts or notices of school closings.[6] Most significantly, the Commission (supported by many commenters including VON) required terminating voice service providers that block calls to immediately notify the caller that the call has been blocked by sending either a Session Initiation Protocol (SIP) Code 607 or 608 or ISDN User Part (ISUP) response code 21 (for calls on TDM networks), as appropriate.[7]

The FCC correctly paired SIP Response Code requirements with its decision to expand reliance on data analytics for call blocking.[8] Data analytics are not perfect and will block legitimate phone calls; a practice that would have been unheard of (and in most cases unlawful) on the U.S. telephone network just a few short years ago before the FCC authorized call blocking as a tool to mitigate illegal robocalls.

The use of data analytics to support network level call blocking takes control away from the called party, who has no specific understanding of precisely which calls are prevented from

[5] The Fourth Report and Order also permitted voice service providers to implement network-based blocking of calls highly likely to be illegal, based on reasonable analytics, with no requirement that the consumer be given the option to opt out, if the provider takes certain measures to ensure that the calls are highly likely to be illegal. *See Fourth Report and Order* at paras. 39-46.

[6] Id. at para. 48.

[7] Id. at paras. 56-58.

[8] Id. at para. 49.

reaching them nor the criteria used to determine which calls are blocked. Moreover, without SIP response codes, expanded call blocking based on analytics would be invisible to the called party, the calling party and the originating voice service provider. Thus, without the response codes, there is no other way to measure the level of erroneous blocking or to know whether to activate redress channels to remediate such errors.

US Telecom claims that more than one million illegal calls are blocked each day.[9] The likelihood is that some of these blocked calls are legitimate and wanted. VON members have already been negatively impacted by this type of blocking.[10] US Telecom is measuring success by ignoring failures (blocked legitimate calls). SIP response codes help identify overzealous or flawed blocking efforts, ultimately to the benefit of data analytics engines and a better functioning telephone system, while still allowing for blocking illegal calls.

The FCC recognized the harm that blocked legitimate calls can create. As required by section 10(b) of the TRACED Act,[11] the FCC established a requirement for redress mechanisms but recognized that redress mechanisms are not useful without awareness of the need for redress – that is, if the originating carrier or calling party is unaware of a call having been blocked.[12] Thus, when it authorized greater use of data analytics for call blocking, it recognized the potential for greater harm and more erroneous blocking of legitimate calls, and therefore required the use of SIP response codes 607 and 608. That was entirely appropriate, and the US Telecom Petition does not dispute that.

It is, however, misleading and erroneous for US Telecom to suggest that IP-NNI referencing a standard is necessary before any finalized Request for Comments ("RFC") can be implemented in a usable way.[13] By way of comparison, the core Session Initiated Protocol standard, RFC 3261, released in June 2002, was widely used and implemented

[9] Petition at 8.

[10] See Comments of Twilio, Inc., CG Docket No. 17-59 at 3 (August 31, 2020).

[11] Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105, 133 Stat. 3274 (2019).

[12] *Fourth Report and Order* at para. 41.

[13] Petition at 3-4.

globally without requiring an ATIS IP-NNI standard referencing it and before ATIS 1000063 was approved in 2015.[14]

Although it overstates the necessity of an IP-NNI reference, US Telecom's primary point seems to be that RFCs 8197 (Response Code 607) and 8688 (Response Code 608) would benefit from IP-NNI creating a framework for more uniform implementation.[15] VON does not disagree with that approach, but the Commission should establish a deadline by which an IP-NNI reference must be completed in order to avoid undue delay.[16] More importantly, if the Commission is inclined to defer implementation of SIP response codes, it also should delay the commencement of the additional analytics-based blocking; otherwise, the Commission would introduce the harm of increased but undetected blocking of legitimate calls by users of the U.S. voice network without any potential cure.[17]

US Telecom rehashes the flawed and defeated notion that "some could seek to use the information to reverse engineer and bypass blocking."[18] This is specious for numerous reasons.

First, knowing that a call is blocked does not reveal the complexity of the algorithm that caused the block. Second, there are alternatives other than SIP response codes that enable this type of "reverse engineering." Whether a particular number or range of numbers has been "blacklisted" by a terminating provider's network can just as easily be discovered by opening an account with that terminating provider and making calls to that account to see whether they're passed to the dialed number. Finally, the Commission has heard and rejected this argument before.[19] There's no new evidence to suggest that the theoretical harms that US Telecom raises are likely to happen. On the other hand, the harms caused by blocked legitimate calls are real –

[14] See. RFC 3261, SIP: Session Initiation Protocol, found at RFC 3261: SIP: Session Initiation Protocol (2rfc.net).

[15] Id. at 6.

[16] The Commission did recognize that "because SIP and ISUP codes are in standard use throughout the network, they are the best solution for immediate notification at this time." Fourth Report and Order at para. 60.

[17] US Telecom overstates the impact that that SIP Response Code requirements may have. It claims in footnote 8 that carriers may stop call blocking if they can't implement SIP response codes. Petition at 5. SIP response codes were a condition of permission to engage in the very specific type of call blocking adopted in the Fourth Report & Order. Previous authorizations for call blocking – such as for invalid phone numbers, Do Not Originate numbers or user-initiated blocks, for example – are unaffected by the SIP response code requirement.

[18] Id. at 7.

[19] *Fourth Report and Order* at para. 54.

and potentially dangerous – and it is irresponsible for US Telecom to encourage the FCC to ignore those real dangers to avoid phantom harms.

VON agrees with the request for clarification that voice service providers are only required to send notification of blocking when calls are blocked based on analytics programs.[20] The problem is that analytics programs are imperfect at identifying illegitimate calls, and the called party lacks the real-time knowledge what calls are blocked. Thus, the notification requirement would not be necessary for blocking or diversion of calls in which the user is in control and maintains knowledge of the scope of blocking or diversion. Examples include:

- anonymous call rejection (subscriber configures their line not to accept calls with caller ID withheld, or to send those calls to voice mail);
- selective call rejection (subscriber configures a list of telephone numbers from which they will not accept calls);
- selective call acceptance (subscriber configures a list of telephone numbers which are the only ones from which they will accept calls);
- Do Not Disturb (subscriber disables all incoming calls); and,
- Call Manager Services (subscriber rejects incoming calls during certain periods of time, *e.g.*, the middle of the night).

In each of these examples, the called party/subscriber is in control and has a firm understanding of the scope of calls that are being blocked. VON agrees that the Commission should confirm that these scenarios fall outside of the scope of the Commission's SIP response code requirements.

VON also agrees that the communication of the SIP response code to the originating voice service provider is the critical requirement for identifying and correcting erroneous analytics-based call blocking.[21] Whether that information is passed along to the originating caller should be discussed at IP-NNI, and, indeed, it might warrant different approaches depending on the type

[20] Petition at 10-12.

[21] Id. at 14-15.

of customer; suggesting there may be good reasons for the decision to remain within the discretion of the originating voice service provider.

<u>**CONCLUSION**</u>

The Commission should act in accordance with the recommendations herein.

Respectfully submitted,

VOICE ON THE NET COALITION

/s/ *Glenn S. Richards*
Glenn S. Richards
Pillsbury Winthrop Shaw Pittman LLP
1200 Seventeenth Street, NW
Washington, DC 20036
(202) 663-8000

Its Attorney

June 4, 2021