**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 |
| | ) | |
| | ) | |

**PETITION FOR RECONSIDERATION AND REQUEST FOR CLARIFICIATION OF USTELECOM – THE BROADBAND ASSOCIATION**

USTelecom – The Broadband Association ("USTelecom") submits this petition for reconsideration and request for clarification regarding the notification requirement adopted in the Commission's *Fourth Report and Order* in its call blocking proceeding.[1] Specifically, rather than maintain a prescriptive blocking notification requirement – particularly one based on unfinished standards – the Commission should reconsider the *Fourth Report and Order's* notification requirement to afford the industry flexibility to meet the calling community's interest in notification. In addition, the Commission should confirm that the notification and blocked call list requirements are only required for analytics-based blocking, whether opt-in or opt-out, and not for contexts in which there would not be any reasonable expectation for them. Finally, the Commission should confirm that originating voice service providers have the flexibility to work with their enterprise customers to determine the best means and approaches for notifying those customers if their calls are blocked.

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

## I. INTRODUCTION AND EXECUTIVE SUMMARY

In the *Fourth Report and Order*, the Commission required voice service providers that block calls to immediately notify callers of such blocking. The Commission also directed "all voice service providers to perform necessary software upgrades to ensure the codes we require for such notification are appropriately mapped" and required all voice service providers in the call path to transmit the code back to the origination point.[2]

The Commission understandably has decided to heed the request of the calling community in adopting a notification requirement. USTelecom and its members have likewise heard from the calling community and, through a USTelecom working group, have been working to address notification and redress, among other issues. Even though USTelecom opposed a regulatory mandate, USTelecom believes it's important to work with the calling community on solutions that serve all members of the ecosystem – subscribers, providers, and legitimate callers. A balanced policy approach that allows providers to take aggressive action to stop illegal and unwanted calls while ensuring that legitimate callers have means to address inadvertent blocking can serve all stakeholders. After all, subscribers need to believe that the calls they receive are predominantly legitimate in order to be willing to even answer the phone when a legitimate entity calls.

The Commission's approach to the *Fourth Report and Order* did not achieve the right balance, but the problems can be solved with a reconsideration of the specifics of the notification requirement and certain clarifications about its scope and implementation. Specifically, the Commission should:

- **Make clear that service providers have flexibility to select the appropriate code or tool to notify callers that their calls have been blocked.** The Commission should not

[2] *Id.* ¶ 52.

require providers to implement an unfinished standard. Instead, the Commission should favor flexibility and, for providers that choose to send release codes, that should include (but not be limited to) 607 and 608 as those codes work their way through the standards process. Other providers should be able to rely on playing a voice message to callers or providing the option for callers to sign up to receive periodic updates from service providers regarding how their calls have been treated during a particular period of time. The key is helping legitimate callers become aware that their calls are getting blocked so that they can then take action to address any issues.

- **Confirm that voice service providers only are required and expected to provide notification of blocking when calls are blocked based on opt-in or opt-out analytics programs, and not in contexts where those requirements do not make sense.** For example, providers should not be required to provide any form of notification when they block calls from Do-Not-Originate ("DNO") numbers; that are part of a suspected Telephone Denial of Service ("TDoS") attack; pursuant to a customer's Do Not Disturb preference, black or white list, or other customer-initiated mechanism; or as necessary for technical reasons (such as avoiding network congestion or the creation of cascading automatic "re-tries" of calls by originating carriers). Similarly, providers should only be required to include in blocked call lists they provide to subscribers those calls blocked pursuant to opt-in or opt-out analytics programs targeting illegal and unwanted robocalls, and not calls blocked based on other mechanisms initiated by their customers.

- **Confirm that voice service providers serving enterprises and other organizations have the flexibility to work with those customers to determine the best approach to notification on a case-by-case basis.**

## II. THE NOTIFICATION REQUIREMENT INAPPROPRIATELY RELIES ON UNFINISHED STANDARDS AND INSTEAD SHOULD AFFORD PROVIDERS ADDITIONAL FLEXIBILITY

### A. The Commission Should Not Have Relied on an Unfinished Standard to Impose the Notification Requirement

Rather than afford provider flexibility to provide notification to callers about blocking, the *Fourth Report and Order* requires that providers that block calls on an IP network return SIP Code 607 or 608, and where SIP codes are not available, rely on ISUP code 21.[3] The standard the Commission relied on to impose this requirement was not fully vetted and had not been approved by the IP-NNI task force. Further, because many calls transit both IP and TDM networks, the Commission relied on unfinished guidance to require that SIP Codes 607 and 608

[3] *See id.* ¶ 56.

map to ISUP code 21.[4] The IP-NNI is currently working on a standard to address these issues, but the group has not yet finished its work.

Codifying in law standards that have not been fully vetted nor finalized creates several problems. First, and most importantly here, standards that have not yet been accepted broadly by the industry may not be implementable in a practical way. This means that some providers currently blocking scores of illegal and unwanted robocalls (and only very occasionally blocking legitimate ones) may cease doing so if they find themselves unable to comply with the Commission's return code requirement. It also means that providers not currently blocking illegal robocalls are unlikely to start doing so. In the end, subscribers lose. So too does the calling community that needs those subscribers to trust the legitimate phone calls they receive.

Second, codifying a specific, but not yet finalized nor vetted, standard in the Commission's rules threatens to lock in an approach that may not be best for all stakeholders. Both the providers that need to implement it and the enterprise callers that would benefit from it can suffer from a static approach. Indeed, in analogous contexts, the Commission has recognized the importance of not intervening in standards processes, as well as deferring to industry standards. In the Commission's *Call Authentication Second Report and Order*, for instance, the Commission indicated it did "not wish to intervene in the process" as "industry stakeholders, standards bodies, and the Governance Authority are actively working to finalize standards and solutions to complex enterprises cases…."[5] In that same proceeding, the Commission also observed that "industry standards are not static" and indicated that a

[4] *See id.* ¶ 57.

[5] *Call Authentication Trust* Anchor, WC Docket No. 17-97, Second Report and Order, FCC 20-136 ¶ 59 (rel. Oct. 1, 2020).

requirement consistent with industry standards "better aligns with our goal of promoting implementation of the industry-defined caller ID authentication standards rather than interfering with their technical application."[6] Aligning any requirements deemed necessary by the Commission to industry standards best promotes the best solutions. In contrast, Commission intervention in the standards process leads to stagnant approaches that do not advance and adjust to changing landscapes – to the extent that the approach is even implementable by a wide swath of the industry in the first instance.[7]

To that end, the standards referenced in the *Fourth Report and Order* regarding notification have not yet been fully finalized for good reason. Numerous questions remain about how a standardized form of notification can be implemented across different networks and configurations. It will take time to work through those issues in the standards bodies to ensure that the SIP code will be interoperable with TDM. And then, after the industry finalizes a standard it believes can be implemented at scale, providers still will need to make changes to the TDM infrastructure that are dependent on vendors.[8]

In addition, some parties have proposed for the standard a technical requirement to include additional various information in the return code, known as the jCard, which the *Fourth Report and Order* does not reference or otherwise refer to. Implementation of any jCard requirement would be highly complex and pose significant implementation challenges that may not be possible to overcome within the time given. It also is unnecessary, given industry efforts

[6] *Id.* ¶ 142.

[7] Moreover, the *Fourth Report and Order* refers to part but not all of the aspects of the standard, causing further confusion to vender development and future interoperability.

[8] For these reasons, it is highly unlikely that providers will be able to fully complete this work by January 1, 2022, meaning some providers may need to stop blocking illegal and unwanted calls in order to comply with the requirement when it takes effect.

to provide contact information and improve redress through USTelecom's Blocking and Labeling Working Group and other initiatives.[9]

As noted above, if providers cannot meet the notification requirement, they may feel it is necessary to stop blocking the calls they suspect to be illegal and/or unwanted, in direct conflict of the Commission's policy aims to protect consumers from those robocalls. The proposal being worked on through the IP-NNI seeks to address these issues and provide the calling community notification as they have requested, but in a manner that can actually be implemented by providers.

### B. Affording Providers Flexibility Regarding Notification Allows Providers to Protect Subscribers While Still Meeting Legitimate Callers' Needs

The Commission concluded that the potential harm from providing notifications to bad actors is more than offset by the significant benefit to legitimate callers.[10] But flexibility regarding how providers notify legitimate callers best ensures that providers can adapt to the landscape and limit potential harm from providing notifications to bad actors. Bad actors have proven highly capable of taking advantage of technology and are likely to do so here. It is reasonable to anticipate that, once a specific release code is ubiquitously used, and once originating carriers begin to pass information to their robocalling customers about release codes received, bad actors will find ways to utilize this new tool in their toolbox to cause harm. Indeed, although the Commission suggested that "[b]ad actors can already rapidly adjust their

[9] *See* Notice of Ex Parte Presentation of USTelecom, CG Docket No. 17-59 (filed Dec. 23, 2020); Notice of Ex Parte Presentation of USTelecom, CG Docket No. 17-59 (filed Dec. 29, 2020); Comments of USTelecom, CG Docket No. 17-59, WC Docket No. 17-97, at 2 (filed Apr. 30, 2021). Notification, combined with clear methods to contact voice service providers and their analytics partners, affords callers what they ultimately have asked for – awareness that their legitimate calls are being blocked and methods to work to address that blocking.

[10] *Fourth Report and Order* ¶ 54.

calling patterns and are likely to change numbers as soon as connection rates drop, regardless of immediate notification,"[11] the Commission cannot reasonably conclude that a notification requirement provides a "significant benefit" to legitimate callers that cannot be achieved by monitoring connection rates but does not provide that same "significant benefit" to unlawful callers. Accordingly, the Commission should proceed with caution and ensure that the industry has the flexibility it needs to adapt as the bad actors do.

In fact, a ubiquitous return code undoubtedly can provide bad actors additional information beyond connection rates. Some robocallers may simply program their equipment to swap in new "calling party" numbers as soon as they receive release codes that tip them off that blocking algorithms have identified a particular number as problematic, but more sophisticated bad actors could leverage the mandated release code for more pernicious activities. For example, some could seek to use the information to reverse engineer and bypass blocking. Others could use information received from release code notifications to gather evidence on valid end points, which could then be resold to others seeking to ensure they are targeting real consumers. In turn, such lists would allow bad actor callers to avoid the honeypots deployed by voice service providers and analytics engines for the precise purpose of detecting and then blocking anomalous traffic. Moreover, in addition to shifting their calling patterns or swapping in new calling party numbers to bypass blocking algorithms, bad actors could choose to escalate their attacks on consumers protected by blocking tools by using intelligent schemes such as "ringless voicemail" to drop voicemails directly into the consumers' voice mailboxes or retaliate with TDoS attacks using response codes to reattempt calls in mass.

[11] *Id.*

Flexibility allows providers to adapt when they have evidence that the bad actors have, and the industry has a long track record in the fight against robocalls of relying on flexibility afforded by the Commission to develop and deploy tools that improve protections for subscribers. By way of example, in response to the call-to-action under then-FCC Chairman Wheeler, the industry-led Robocall Strike Force developed the STIR/SHAKEN authentication framework, which is set to restore trust in Caller ID as it is pervasively deployed.[12] In addition, in response to Commission clarifications authorizing providers to block illegal and unwanted robocalls,[13] industry leaders have deployed powerful blocking tools, blocking collectively more than one million illegal robocalls each day,[14] and labeling additional calls to arm subscribers with more information about the calls they receive. The industry also established the USTelecom-led Industry Traceback Group, which in 2020 initiated greater than 2,500 tracebacks, representing hundreds of millions of calls, and supporting enforcement actions targeting almost 50 entities and individuals.[15] Each of these efforts were initiated in the absence of mandates and were supported by regulatory flexibility.

Notification is no different: Affording flexibility to service providers will allow them to continue to adapt to the robocall threat environment and enhance the protections they offer subscribers, while also allowing them to innovate to meet the needs of legitimate callers who

---

[12] *See* Robocall Strike Force Report, Robocall Strike Force, (Oct. 26, 2016), https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf.

[13] *See, e.g.*, *Advanced Methods to Target and Eliminate Unlawful Robocalls*, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 9706 (2017) ("*2017 Call Blocking Order*"); *Advanced Methods to Target and Eliminate Unlawful Robocalls*, 34 FCC Rcd 4876 (2019) (*"2019 Call Blocking Ruling*").

[14] *See, e.g.*, FCC Consumer and Government Affairs Bureau, *Call Blocking Tools Now Substantially Available to Consumers: Report on Call Blocking*, CG Docket No. 17-59 ¶ 13 (June 2020).

[15] *See* Industry Traceback Group, *Combatting Illegal Robocalls Report* (2020), https://www.ustelecom.org/the-industry-traceback-group-itg/.

want to know their calls are being blocked. In contrast, hardcoding a specific mechanism threatens to lock in an approach that does not serve subscribers or callers.[16]

The caller community's request for notification and the Commission's policy preference for it are understandable. As the callers have explained, without awareness that their calls are being blocked, they are unable to take action to try to address the blocking.[17] But for the reasons above, a specific, incomplete standard is not the answer. Instead, the Commission should require that providers give effective notice – whether through an industry standardized return code, an intercept announcement, or other notification mechanism later deemed sufficient.[18] That approach will allow the industry to continue its work on the return code standard through the IP-NNI and continue to enhance and improve other mechanisms, while still satisfying the calling community's demand underlying the requirement.[19]

---

[16] In fact, callers identified and advocated for several different approaches to notification. *See, e.g.*, *Fourth Report and Order* ¶ 60 (noting that some commenters propose use of an intercept message); *see also id.* ¶ 59 (noting that some commenters requested the inclusion of additional information in an immediate notification, including the reason the call was blocked or a website or phone number for resolution). Separately, standards contemplate, in a complete IP end-to-end path, sending authenticated name information and more, commonly called "branded calling" in the industry, as a benefit to the calling community. Once deployed, the technology could reduce any need for notification to legitimate callers in the first instance.

[17] *See, e.g., Fourth Report and Order* ¶ 53 ("Many commenters support immediate notification, arguing that a caller cannot readily access redress if it is uncertain whether calls are being blocked.").

[18] To effectuate this new approach, the Commission could explore creating safe harbors that allow providers to choose not to use release codes if they have other acceptable means to inform callers about how their calls are being treated and could task, for instance, the CATA Working Group on evaluating and making recommendations regarding such alternative means.

[19] Regardless of any specific notification requirement or return code, the Commission should ensure that upstream providers and originating voice service providers react to any blocking notification in accordance with industry standards. In particular, the Commission should make sure that providers do not retry sending calls that have been intentionally blocked as indicated by the notification, which can disrupt network service and drain resources.

## III. THE COMMISSION SHOULD CONFIRM THAT THE NOTIFICATION AND BLOCKED CALLS LIST REQUIREMENTS ONLY APPLY TO ANALYTICS-BASED BLOCKING TARGETING ILLEGAL OR UNWANTED ROBOCALLS

### A. Notification Should Only Be Required Where Legitimate Callers Have a Reasonable Expectation of Notification

The Commission should confirm that notification is only necessary for blocking where a legitimate caller might have a reasonable expectation its call is completed and not blocked. More specifically, the Commission should confirm that notification is only required for analytics-based blocking that targets illegal or unwanted robocalls, regardless of whether such blocking is offered on an opt-in or opt-out basis.

As the Commission recognized when it first allowed voice service providers to block certain categories of calls by default, some calls are highly likely to be illegitimate simply due to their nature.[20] These include calls from, for example, phone numbers on a DNO list, such as the DNO list that USTelecom's Industry Traceback Group maintains on behalf of the industry.[21] Because DNO numbers are put on the DNO list at the subscriber's request,[22] no legitimate caller should be using those numbers and therefore no caller should expect a return code if their calls from those numbers are blocked.[23] In turn, terminating voice service providers should not be expected to provide notification when they block DNO numbers.

---

[20] *See 2017 Call Blocking Order* ¶ 9 (establishing certain "well-defined circumstances in which voice service providers may block calls that are highly likely to be illegitimate because there is no lawful reason to spoof certain kinds of numbers").

[21] *See* Industry Traceback Group, *Policies and Procedures*, 14 (Jan. 2020), https://docs.fcc.gov/public/attachments/DOC-368957A3.pdf.

[22] Somos, the Toll Free Numbering Administrator, also maintains and makes available a DNO list with all non-dialable, non-allocated, and non-assigned toll free numbers.

[23] Indeed, calls from DNO numbers often are blocked in the call path before they ever reach the terminating provider, let alone that provider's subscriber. In those cases, because the notification requirement only applies to terminating providers, *see* 47 C.F.R. § 64.1200(k)(9), notification is not required.

Notification of blocking for several other categories of calls also would not serve subscribers or legitimate callers. In these instances, notification is unnecessary at best and counterproductive and damaging at worst. TDoS attacks are one example. There should be no expectation or requirement that voice service providers provide callers notification when blocking a suspected TDoS attack from those callers, as doing so could permit malicious actors to game the system and impose substantial harm on the victims. Such blocking is only temporary, and the Commission must ensure that voice service providers have complete flexibility as they work to mitigate TDoS attacks in real time, protecting the victims of the attack.

Notification also should not be required where blocking is done based on the customer's own analysis of what calls they want or do not want, such as when the customer relies on Do Not Disturb, white or black list, call rejection, or line-level blocking features. Such blocking is done exclusively at the customer's own initiative and based on their own decision about how to handle incoming calls, and it would not be appropriate, nor consistent with customer proprietary network information privacy protections, for a voice service provider to reveal such information about individual subscribers. Indeed, that information can reveal details about the subscriber's individual preferences, including whether or not the subscriber wants to receive calls from a particular caller, or when he or she wants to receive calls in the first instance. Additionally, the service provider could not do anything to reverse that type of blocking if contacted by the caller, as such blocking is being carried out at the subscriber's specific direction.

Voice service providers also should not be required to provide notification if they are temporarily unable to for technical reasons. There are instances in which providers may not be able to provide notification, such as in network congestion events or to prevent cascading

automatic "re-tries" of calls by upstream providers that ignore any provided release code.[24] Continuing to send a release code in such contexts could cause spikes in the service providers' network usage that impair legitimate calling to end users.

For the reasons above, the Commission should make clear that notification is only required when the call is blocked by the service provider based on analytics, and not due to, for example, blocking of calls using DNO numbers, TDoS attacks, or pursuant to a customer-initiated features. Legitimate callers do not (or should not) have an expectation of notification in such contexts.

### B. Only Calls Blocked Based on Opt-in or Opt-Out Analytics Programs Should Be Included in the Blocked Call List

Similarly, providers should only be required to include in the blocked call list provided to subscribers under section 64.1200(k)(1) of the Commission's rules those calls blocked pursuant to opt-in or opt-out analytics programs targeting illegal and unwanted robocalls.[25] In particular, providers should not be expected to include calls that are not completed pursuant to subscriber-initiated features such as Do Not Disturb, white and black lists, call rejection, and line-level blocking.

There is no evidence that the Commission intended that the blocked call list capture calls blocked specifically at the subscriber's direction through such features. Rather, the *Fourth Report and Order* appears to suggest the requirement applies only to analytics-based blocking,

[24] As noted above, it is critical for the Commission to ensure that upstream providers respond and react appropriately to any industry standard for blocking notification to avoid re-tries of blocked calls that, in effect, can create unintentional TDoS attacks. *See supra* note 19.

[25] 47 C.F.R. 64.1200(k)(1).

performed on either an opt-in or opt-out basis.[26] That approach makes sense. Subscribers choose to use these features and customize them to their preferences. They therefore know, or should know, that they will not receive calls when they have such features activated, and therefore there is no reason for notice. Just as importantly, such features typically are separate and apart from the analytics-based blocking programs providers offer their subscribers. Therefore, it may not be practical from a technical perspective to include those calls in a blocked class list, particularly in the case of features offered through legacy TDM networks like line-level blocking.[27]

For these reasons, as the Commission did with labeling,[28] the Commission should confirm that such list need only include calls blocked based on a provider's opt-in and opt-out analytics-based robocall blocking services, and not based on other features selected by the customer.

[26] *See Fourth Report and Order* ¶ 65 ("We require that the blocked calls list include calls *blocked on an opt-out or opt-in basis*….") (emphasis added); *id.* ("This is also consistent with the scope of transparency and effective redress requirement in section 10(b) of the TRACED Act, which applies to '*robocall blocking services provided on an opt-out or opt-in basis*") (emphasis added); *see also 2019 Call Blocking Ruling* ¶ 34 (clarifying that voice service providers may offer "opt-out call blocking programs based on any reasonable analytics designed to identify unwanted calls" in addition to offering such programs on an opt-in basis).

[27] Further, the Commission should ensure that the blocked call list requirement cannot be read in a manner that conflicts with other Commission rules, such as the *67 requirements that protect the originating caller's information.

[28] *See Fourth Report and Order* ¶ 66.

## IV. ORIGINATING VOICE SERVICE PROVIDERS SHOULD HAVE FLEXIBILITY REGARDING HOW THEY NOTIFY THEIR CALLING CUSTOMERS ABOUT BLOCKED CALLS

The Commission should confirm that originating voice service providers can determine with their enterprise customers how to best serve such customers, including how those customers wish to address and be notified about blocking of their calls by downstream providers.

The rule itself is not clear whether or not an originating voice service provider must provide a response code to its calling customer,[29] but language in the *Fourth Report and Order* could be read to suggest that the requirement extends to notifying callers through the return codes established.[30] There are, however, a variety of solutions in the dynamic communications marketplace for enterprise callers. To compete and offer value-added services, some originating voice service providers offer their customers complete voice service solutions, where providers troubleshoot any telecommunications issues on their customers' behalf – including any blocking issues that the customers experience. Other originating voice service providers offer more traditional setups, where the enterprise may have a team specialized in telecommunications that handles any outbound calling issues. Those enterprises may be able to, and wish to, receive a return code, audio intercept, or similar mechanism from their service provider**.** And some providers may have both offerings for their customers, depending on each customer's preference.[31]

---

[29] 47 C.F.R. § 64.1200(k)(9) (all voice service providers must transmit an appropriate response code "to the origination point of the call")

[30] *Fourth Report and Order* ¶ 56 ("Callers with properly configured equipment will thereby receive sufficient information…."); *id.* ¶ 131 ("We note that callers may need to make upgrades to their systems to ensure that they receive these codes.… We further encourage originating voice service providers to work with their enterprise customers to ensure that these codes are properly passed.").

[31] Importantly, as the Commission recognizes, the notification requirement adopted in the *Fourth Report and Order* will be incompatible with many enterprise customer networks. *See, e.g., Fourth Report and*

The Commission need not, and should not, dictate the terms of the relationship between an originating provider and its customer. The Commission therefore should confirm that notification by an originating voice service provider to its customer can be determined by their relationship and contract and is not covered by the Commission's notification requirement.

## V. CONCLUSION

The Commission should rescind the *Fourth Report and Order*'s prescriptive notification requirement as it was based on incomplete standards. Instead, the Commission should require that terminating voice service providers give effective notice to callers, affording providers the flexibility to provide such through an industry standardized return code, an intercept announcement, or other notification mechanism later deemed sufficient. In addition, the Commission should confirm that the scope of the notification and blocked call list requirements apply only to opt-in or opt-out analytics-based blocking programs, and not to contexts where such information should not be reasonably expected. Finally, the Commission should confirm that originating voice service providers and the enterprises they serve can determine the best methods for the provider to notify an enterprise customer that its calls are being blocked.

*Order* ¶ 56 n. 131. Therefore, any specific mandate for originating voice service providers to send notice to their enterprise customers could cause unintended consequences and harm to those customers' networks.

Respectfully submitted,

By: */s Joshua M. Bercu /*

Joshua M. Bercu
Vice President, Policy & Advocacy

USTelecom – The Broadband Association
601 New Jersey Avenue, N.W.
Suite 600
Washington, D.C. 20001
(202) 551-0761

May 6, 2021