**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 USTELECOM ASSOCIATION

Kevin Rupy
B. Lynn Follansbee
Jonathan Banks

USTelecom Association
601 New Jersey Avenue, N.W.
Suite 600
Washington, D.C. 20001
(202) 326-7300

July 3, 2017

## TABLE OF CONTENTS



***  *  ***

## SUMMARY

USTelecom welcomes this proceeding, and appreciates the Commission's approach that would provide carriers with greater flexibility to address the robocall problem. The Commission's decision to respond to the further clarifications sought by the industry-led Strike Force regarding the permissibility of certain provider-initiated call blocking is appreciated by industry, and reflects the significant value to be obtained from cooperation between industry and government stakeholders. USTelecom continues to work cooperatively with a broad range of stakeholders on this issue in order to find practical, workable solutions to the problem of telephony abuse and fraud resulting from unwanted, and sometimes unlawful, robocalls.

Given the rapid and ever-changing nature of the robocall problem, multifaceted holistic approaches are necessary – and indeed, beneficial – in order to mitigate the harms resulting from such illegal calls. Much in the same way that remediation efforts in areas such as spam or cybersecurity must continually evolve through a variety of approaches, the same can be expected with respect to robocalls. USTelecom supports the development of a variety of solutions to the robocall problem by stakeholders throughout the internet ecosystem, including through technological measures, increased industry cooperation, heightened consumer education, and increased enforcement. USTelecom encourages all stakeholders from various sectors to continue to fight the robocall scourge across multiple fronts.

USTelecom supports the Commission's proposal to codify its rules to make clear that voice service providers may block calls from a number if the subscriber to that telephone number requests such blocking in order to prevent its telephone number from being spoofed. As USTelecom demonstrated in its recent briefing to the Commission on DNO efforts, "DNO can be an effective tool for addressing certain types of robocalls, when it is applied in a narrow and targeted manner." However, because of the nature of DNO – outright blocking of calls in the network – it is crucial that a heightened level of due diligence and ongoing maintenance by voice providers is resident throughout the entire process. Thorough vetting measures should be undertaken to identify whether any legitimate out dial service is using the originating telephone number.

USTelecom also supports the Commission's proposal to adopt a rule allowing provider-initiated voluntary blocking of calls purportedly originating from numbers that are not valid under the North American Numbering Plan (NANP). Unlike the DNO approach, blocking in this particular context (*i.e.*, blocking invalid numbers), does not necessarily require the industry coordination referenced above. In other words, whereas DNO involves numbers legitimately assigned to customers, the blocking at issue here involves numbers that have not – and generally cannot – be assigned to any legitimate customer. Nevertheless, as with all manners of blocking in the network, USTelecom maintains that voice providers should still exercise caution in instituting such call blocking.

While USTelecom supports giving service providers the authorization to block numbers that are not allocated or assigned, there is a need for the carrier to do due diligence before blocking. Unlike the preceding instances of provider-initiated blocking discussed above, the Commission's proposal to permit such blocking for unallocated or unassigned numbers raises

greater potential for the inadvertent blocking of legitimate numbers. While USTelecom supports the proposed clarification that such numbers may be blocked at the discretion of carriers, there are substantial risks and hurdles associated with potentially engaging in such blocking on a large scale. The blocking environments envisioned under these two scenarios are much more fluid and potentially dangerous than the call blocking environments associated with either DNO-blocking, or invalid number blocking. Telephone numbers are in a constant state of flux and change, with individual numbers rapidly moving between allocation, assignment and reassignment.

USTelecom notes that while each of the Commission's four proposals for robocall blocking differ in approach, there are varying degrees of complexity and potential consumer harms resident in each. For example, while DNO efforts arguably represent a fairly straightforward approach to blocking calls, even in the tightly controlled manner instituted by the ITB Group, legitimate calls can be blocked. Due to these varying degrees of risk, and the nature of any network blocking, deployment of such services by carriers must be carefully considered and vetted prior to full implementation by industry.

Regarding its Notice of Inquiry, USTelecom supports the development of a variety of objective standards to identify robocalls, since a diversity of approaches would create a more challenging operating environment for illegal robocallers. The Commission, however, should be cautious about cataloguing which methods and approaches are better suited for identifying illegal robocalls, since illegal actors can use this as a roadmap for bypassing such measures.

USTelecom also supports the Commission's proposal to adopt a safe harbor to provide certainty to providers instituting blocking measures consistent with the rules adopted in this proceeding. USTelecom agrees that providers instituting reasonable forms of blocking should not be deemed in violation of the Commission's rules and the Communications Act, nor should such providers have their call completion rates adversely effected due to such reasonable blocking. USTelecom also supports the Commission's proposal to exclude calls blocked in accordance with the rules it adopts in this proceeding from calculation of providers' call completion rates.

USTelecom also supports the Commission's inquiry into the crucial issue of protecting legitimate callers who may have their calls blocked. The importance of protecting legitimate callers is taking on increased importance, particularly as call-blocking services and initiatives continue to increase penetration within the marketplace. The Commission should not, however, adopt an approach that would formally mandate a form of 'white list', given the substantial security concerns such a list would present.

Finally, USTelecom encourages the Commission to revisit the important clarifications related to the sharing of CPNI, which is crucial to ongoing industry detection, assessment, traceback and mitigation efforts. The appropriate sharing of such information could positively impact unlawful robocall mitigation by making the identification of the true source of such calls more accurate and timely, and USTelecom encourages the Commission to address this important clarification.

**BEFORE THE**
**FEDERAL COMMUNICATIONS COMMISSION**
**WASHINGTON, D.C. 20554**

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991 | ) | CG Docket No. 02-278 |
| | ) | |
| Establishing Just and Reasonable Rates for Local Exchange Carriers | ) | WC Docket No. 07-135 |
| | ) | |

**COMMENTS OF**
**THE USTELECOM ASSOCIATION**

The USTelecom Association (USTelecom)[1] submits these comments in response to the Notice of Proposed Rulemaking and Notice of Inquiry (Notice) released by the Federal Communications Commission (Commission) in the above-referenced proceedings.[2] Through its Notice, the Commission seeks comment on proposed rules that would allow facilities-based voice providers to – on their customers' behalf – block illegal robocalls based on four categories of calls: 1) blocking at the request of the subscriber to the originating number; 2) calls originating from unassigned numbers; 3) calls originating from numbers not allocated to any provider; and 4) calls originating from numbers that are allocated to a provider, but not assigned to a subscriber.

---

[1] USTelecom is the premier trade association representing service providers and suppliers for the telecommunications industry. USTelecom members provide a full array of services, including broadband, voice, data and video over wireline and wireless networks.

[2] Notice of Proposed Rulemaking and Notice of Inquiry, *Advanced Methods to Target and Eliminate Unlawful Robocalls*, 32 FCC Rcd. 2306, FCC 17-24 (released March 23, 2017) (*Notice*).

## I. Introduction

USTelecom welcomes this proceeding, and appreciates the Commission's approach that would provide carriers with greater flexibility to address the robocall problem. USTelecom has long maintained that cooperative industry and government efforts to address ongoing abuses of the Federal Trade Commission's (FTC) Do-Not-Call framework is the best approach to more effectively address the scourge of robocalls.[3] The Commission's decision to respond to the further clarifications sought by the industry-led Strike Force regarding the permissibility of certain provider-initiated call blocking is appreciated by industry, and reflects the significant value to be obtained from cooperation between industry and government stakeholders.

Because addressing the robocall scourge requires broad cooperation, USTelecom continues to work cooperatively with a broad range of stakeholders on this issue in order to find practical, workable solutions to the problem of telephony abuse and fraud resulting from unwanted, and sometimes unlawful, robocalls. USTelecom has long been involved in addressing the significant consumer and government concerns resulting from violations of the Do-Not-Call framework jointly administered by the Commission and the FTC. USTelecom's member companies understand the annoyance and potential monetary harms inflicted on consumers and businesses resulting from these violations. Our industry has a long and successful history of working with consumer, industry and regulatory stakeholders on ways to mitigate such harms, and has developed strong relationships with law enforcement agencies at the local, state and federal level.

[3] *See e.g.*, Comments of the United States Telecom Association, CG Docket No. 02-278, WC Docket 07-135, pp. 14 – 16 (submitted January 23, 2015). *See also*, Ex Parte Notice, from David Frankel, ZipDX LLC, to Marlene H. Dortch, Secretary, Federal Communications Commission, CG Docket No. 17 – 59, p. 7 (March 30, 2017) (*ZipDX Ex Parte*) (stating that "robocalls are an industry-wide problem and need to be addressed cooperatively.").

## II. Addressing the Robocall Problem Requires a Multi-Stakeholder Holistic Approach, and Blocking Protocols Are Specialized Tools for Addressing the Robocall Problem.

USTelecom and its member companies understand and share the widespread frustration resulting from illegal robocalls that violate the Do Not Call framework. Such calls are not only an annoyance, but criminal elements can exact financial and emotional harms upon unsuspecting or vulnerable consumers. As the Commission acknowledges in its Notice, these calls "bombard [consumers'] phones at all hours of the day, in some cases luring consumers into scams (*e.g.*, when a caller claims to be collecting money owed to the Internal Revenue Service (IRS)) or leading to identity theft."[4] The financial impact of these calls, and the broad variety of associated scams have been well-documented in recent years.[5] Industry and government stakeholders have been advancing a number of comprehensive initiatives to more thoroughly combat and address the robocall scourge.

The rapid and ever-changing nature of the robocall problem, however, makes the potential for a single "silver bullet" solution highly problematic and strongly inadvisable. An open communications network is inherently vulnerable to abuse, and the interdependent, interconnected and global nature of the internet means that areas of vulnerability exist throughout the network, and therefore cannot be realistically addressed by any single stakeholder or mitigation technique. Given the rapid and ever-changing nature of the robocall problem, multifaceted holistic approaches are necessary – and indeed, beneficial – in order to mitigate the harms resulting from such illegal calls. Much in the same way that remediation efforts in areas

[4] *Notice*, ¶ 1.

[5] *See e.g.*, *See*, Emma Fletcher, Rubens Pessanha, Better Business Bureau Institute Report, *2016 BBB Scam Tracker Annual Risk Report: A New Paradigm for Understanding Scam Risk*, (2016) (*BBB Institute Report*).

such as spam or cybersecurity must continually evolve through a variety of approaches, the same can be expected with respect to robocalls.

USTelecom supports the development of a variety of solutions to the robocall problem by stakeholders throughout the internet ecosystem, including through technological measures, increased industry cooperation, heightened consumer education, and increased enforcement. The Commission appropriately acknowledges as much in its Notice, when it observed that "stopping illegal robocalls and the problems they cause has been a focus across industry, government, and consumer groups. Few other communications issues have unified disparate interests the way illegal robocalls have."[6]

In light of this reality, USTelecom encourages all stakeholders from these various sectors to continue to fight the robocall scourge across multiple fronts, including consumer education, increased enforcement, and the deployment of a wide variety of tools (including consumer controlled and industry tools). In this ongoing battle against criminal robocallers, there have been several important developments over the last year that are particularly significant.

Most notably, the industry-led, ecosystem-wide Robocall Strike Force issued its report to the Commission on October 26, 2016. In March, 2017, USTelecom submitted to the Strike Force its report regarding the association's Do Not Originate (DNO) efforts, and subsequently briefed Commission staff on its findings. Comprehensive follow-up reports by the industry groups continuing the work started by the Strike Force were delivered to the Commission on April 28, 2017.

These reports hold a significant amount of good news for consumers. For example, the reports note that the crucial SHAKEN/STIR standards development for the next generation of

[6] *Notice*, ¶ 3.

robocall mitigation tools have been accelerated by six months. These standards, which incorporate caller-ID authentication capabilities into the network and consumer devices, have recently entered the industry testing phase. The reports also highlight the increasing number of tools that have been developed and actively deployed to consumers by a growing number of national voice providers and third-party developers.[7] Finally, the reports detail the efforts of USTelecom's Industry Traceback Group, which is comprised of a broad range of network providers including the cable, wireline, wireless and wholesale industries, who are working collaboratively in order to identify the origin of these calls at their source. Industry's strong commitment to this effort can be seen in its significant growth over the last year, from just 3 carriers in July, 2016, to 21 providers as of today.

Consumer groups are also increasingly implementing consumer education components that are equally important to combatting robocalls. As noted in the recent recommendation of the Consumer Advisory Committee, "education is a crucial component to making consumers better aware of existing tools that can protect them from these calls."[8] Similarly, a recent report of the Better Business Bureau Institute (BBB Institute) noted that targeted consumer education efforts "can be a driver for focusing educational and investigative efforts where they are likely to

[7] *See*, Ex Parte Notice, from USTelecom, ACT – The App Association, ATIS and CTIA, to Marlene H. Dortch, Secretary, Federal Communications Commission, CG Docket No. 17 – 59 (April 28, 2017) (*April 2017 Strike Force Report*). For example, AT&T has launched its 'Call Protect' service that allows customers with iPhones and HD Voice enabled Android handsets to automatically block suspected fraudulent calls. Verizon has been trialing on both the wireless and wireline sides services that warn its customers about calls identified as suspicious. And various carriers have worked with NoMorobo to facilitate their customers' ability to use that third-party blocking service, such as Verizon's "one click" solution that simplifies customers' ability to sign up for the service. *April 2017 Strike Force Report*, pp. 17 – 18.

[8] Consumer Advisory Committee Unwanted Calls Recommendation, May 19, 2017 (available at: https://apps.fcc.gov/edocs_public/attachmatch/DOC-344985A1.pdf) (visited, June 27, 2017).

have the greatest effect."[9] Unfortunately, as noted in the October Strike Force Report, a "plurality of experts believe that less than 10% of consumers currently are using available call blocking solutions."[10]

Regarding enforcement efforts, USTelecom applauds the Commission's recent enforcement action targeting a high-volume illegal robocaller. Effective enforcement actions effectively address the robocall problem by addressing the problem at its very root: the source of the calls. As demonstrated by last year's enforcement action targeting illegal robocall call centers in India, the arrest of the criminals originating those calls dramatically reduced consumer impacts. USTelecom maintains that enforcement is ultimately the most effective deterrent to robocalls, since it literally addresses the problem at its source.

USTelecom appreciates the Commission's efforts in this proceeding, which represent one aspect of multi-stakeholder robocall mitigation efforts. The Commission is encouraged to pursue such creative approaches that can potentially create a 'layered defense' for protecting consumers. Independently, no single solution will be a panacea to the robocall problem. However, pursuing multi-pronged approaches to mitigating robocalls – including technological solutions, consumer education, and enforcement – is the best approach for addressing this challenge.

## III. Discussion of the FCC's Blocking Proposal.

USTelecom welcomes and appreciates the approach taken in the Commission's Notice. By examining a variety of approaches to addressing the robocall issue, the Commission appropriately addresses different avenues for addressing and mitigating robocalls. Each of the Commission's four proposals are discussed in greater detail below. In general, while some of the

[9] *See, BBB Institute Report*, p. 7.

[10] Robocall Strike Force Report, October 26, 2016, p. 16 (available at: https://transition.fcc.gov/cgb/Robocall-Strike-Force-Final-Report.pdf) (visited June 28, 2017) (*October 2016 Strike Force Report*).

Commission's proposals are fairly straightforward (albeit, presenting certain challenges of their own), others, such as the blocking of unallocated or unassigned numbers, raise more challenging and technologically complex issues.

### A. Blocking at the Request of the Subscriber to the Originating Number.

USTelecom supports the Commission's proposal to codify its rules to make clear that voice service providers may block calls from a number if the subscriber to that telephone number requests such blocking in order to prevent its telephone number from being spoofed.[11] As USTelecom demonstrated in its recent briefing to the Commission on DNO efforts undertaken by the Industry Traceback Group (ITB Group), "DNO can be an effective tool for addressing certain types of robocalls, when it is applied in a narrow and targeted manner."[12]

DNO is a category of call blocking that can have a positive impact on robocall mitigation efforts, and is a process whereby certain telephone numbers identified at VoIP gateways or interconnection points, are prevented from terminating to the end user based. A measured and tightly controlled DNO process can be instituted by some or many carriers. Calls from numbers that have been placed on a DNO list are rejected by the first service provider in the call path that has implemented DNO based on the originating telephone number and thus blocked from entering the phone system.[13]

---

[11] *Notice*, ¶¶ 14 – 15.

[12] *See*, Ex Parte Notice, from Kevin G. Rupy, USTelecom Association, to Marlene H. Dortch, Secretary, Federal Communications Commission, CG Docket No. 17 – 59, p. 13 (June 14, 2017) (*USTelecom DNO Ex Parte Notice*).

[13] DNO is no substitute for authentication, but USTelecom's testing efforts demonstrated that DNO can prevent a certain subset of narrowly defined harmful calls from reaching consumers. It is also important to note that the calls themselves will still route across networks up until the point that the traffic is handed off to a carrier that is instituting a DNO. Because there are potentially multiple paths for any call to take, the effectiveness of any given DNO effort will rely on the participation rate of carriers. In other words, the more carriers that are instituting a DNO on a given number, the more effective that particular DNO undertaking will be.

Given these considerations, USTelecom maintains that DNO is a highly specialized and focused tool that has potential for effective deployment under certain circumstances, and the ITB Group identified DNO candidates based on five criteria.[14] DNO can be an effective tool for addressing certain types of robocalls, when it is applied in a narrow and targeted manner. USTelecom maintains that the efforts of the ITB Group's DNO trials have been effective due to the efforts being narrowly targeted towards the specific set of easily identified, inbound-only telephone numbers. The focus on inbound-only numbers underscores the Commission's observation in its Notice that such calls "are deemed to be presumptively spoofed and likely to violate the Commission's anti-spoofing rules, and have the potential to cause harm both to the called party and to the subscriber who uses the number."[15] However, because of the nature of DNO – outright blocking of calls in the network – it is crucial that a heightened level of due diligence and ongoing maintenance by voice providers is resident throughout the entire process.

Regarding appropriate due diligence, thorough vetting measures should be undertaken to identify whether any legitimate out dial service is using the originating telephone number. The due diligence is the responsibility of both the user of the number (who must ensure that the number for which it is seeking a DNO is inbound-only), as well as the carrier provisioning service to the user of the number (who should scan its network to ensure no outbound calls are identified using the number at issue).[16]

---

[14] *See, USTelecom DNO Ex Parte Notice*, p. 6. Specifically, to be a potential candidate for DNO a candidate number must: 1) be inbound-only; 2) be currently spoofed by a robocaller in order to perpetrate impersonation-focused fraud; 3) be the source of a substantial volume of calls; 4) have authorization for participation in the DNO effort from the party to which the telephone number is assigned; and/or 5) be recognized by consumers as belonging to a legitimate entity, lending credence to the impersonators and influencing successful execution of the scam.

[15] *Notice*, ¶ 14.

[16] Ongoing maintenance of the telephone number prior to and during the DNO must also take place in order to ensure that the disposition of the telephone number at issue does not change

Any such sharing of information among carriers for purposes of implementing DNO should be centrally coordinated for a variety of reasons. To begin with, it would be highly inefficient for entities requesting DNOs to be forced to make individual requests to multiple providers. More importantly, however, it is crucial that DNOs implemented by industry are tracked and coordinated through a central effort. Absent such coordination, the subscriber could end up in a situation where they lose track of which carriers are instituting DNOs. In a scenario where the subscriber wishes to remove the DNO (*e.g.*, the number(s) will start making outbound calls, or is reassigned), it will be imperative for all carriers instituting the DNO to be aware of the need to remove the block(s). Only through a centralized and coordinated effort can such efficiencies and network integrity be obtained. USTelecom's Industry Traceback Group has been facilitating a targeted, centralized, and coordinated DNO trial and stands ready to continue to evolve industry efforts on this front going forward.

**B. Calls Originating from Invalid Numbers.**

USTelecom also supports the Commission's proposal to adopt a rule allowing provider-initiated voluntary blocking of calls purportedly originating from numbers that are not valid under the North American Numbering Plan (NANP).[17] Examples of such numbers could include numbers that use an unassigned area code; that use an N11 code, such as 911 or 411, in place of an area code; that do not contain the requisite number of digits; and that are a single digit repeated, such as 000-000-0000.

Unlike the DNO approach, blocking in this particular context (*i.e.*, blocking invalid numbers), does not necessarily require the industry coordination referenced above. In other

---

over time. Among other things, such scenarios can arise if the DNO telephone number is changed to permit outbound calls, or if it is reassigned to another entity. Any such change may trigger a requirement that the number is removed from its DNO status.

[17] *Notice*, ¶¶ 17 – 18.

words, whereas DNO involves numbers legitimately assigned to customers, the blocking at issue here involves numbers that have not – and generally cannot – be assigned to any legitimate customer. As the Commission acknowledges in its Notice, it does not "foresee any reasonable possibility that a caller would spoof such a number for any legitimate, lawful purpose," since "unlike a business spoofing Caller ID on outgoing calls to show its main call-back number, invalid numbers cannot be called back."[18]

Nevertheless, as with all manners of blocking in the network, USTelecom maintains that voice providers should still exercise caution in instituting such call blocking. For example, while numbers that do not reflect the traditional 10-digit structure of those assigned by the NANP could presumably be targeted for such blocking, legitimate calls from foreign numbers can potentially be blocked since many do not follow the NANP format. As noted by at least one commenter in this proceeding, there can be instances of legitimate domestic calls reflecting seemingly 'invalid' numbers.[19]

While USTelecom maintains that instances such as these are not necessarily a barrier to instituting such blocking, they do illustrate the importance of exercising caution when instituting blocking in the network. Moreover, it further underscores USTelecom's view that any manner of blocking – whether through a targeted DNO, or directed at invalid telephone numbers – is accompanied by a legitimate risk that legitimate calls will sometimes be blocked. It is therefore imperative that the Commission make the initiation of any such blocking by a voice provider a voluntary measure, so that individual carriers can measure the potential risk and implement the necessary safeguards as they deem appropriate.

---

[18] *Id.*, ¶ 17.

[19] *See*, *ZipDX Ex Parte*, p. 7 (noting for example that "33120298989 is a fixed line in Paris, France (11 digits not valid for NANP); 4329821234 – invalid NXX in Texas, or valid number in Austria?; 8252403456 –invalid NXX in Alberta, or valid number in South Korea?").

### C. Calls Originating From Numbers Not Allocated to Any Provider, or Assigned to a Subscriber.

While USTelecom supports giving service providers the authorization to block numbers that are not allocated or assigned, there is a need for the carrier to do due diligence before blocking. Unlike the preceding instances of provider-initiated blocking discussed above, the Commission's proposal to permit such blocking for unallocated or unassigned numbers raises greater potential for the inadvertent blocking of legitimate numbers. While USTelecom supports the proposed clarification that such numbers may be blocked at the discretion of carriers, there are substantial risks and hurdles associated with potentially engaging in such blocking on a large scale.

Whereas DNO and invalid numbers are narrow targets of opportunity for voluntary blocking, the scale of numbers at issue in the Commission's latter two proposals are potentially enormous – encompassing 3 billion telephone numbers.[20] While the Commission focuses on numbers that are not yet allocated or assigned, because of the prominence of illegal spoofing of phone numbers, protecting subscribers' legitimately assigned numbers from spoofing is a prominent factor in any consideration of blocking in this context.

The blocking environments envisioned under these two scenarios are much more fluid and potentially dangerous than the call blocking environments associated with either DNO-blocking, or invalid number blocking. Telephone numbers are in a constant state of flux and change, with individual numbers rapidly moving between allocation, assignment and reassignment. By some estimates, 100,000 mobile phone numbers are reassigned to new users

[20] As of December 31, 2016, the NANPA reported that there were 313 geographic NPA codes in service for the United States alone, equating to a universe of approximately 3 billion telephone numbers. *See*, Neustar Report, *2016 NANPA Annual Report*, p. 7 (available at: https://www.nationalnanpa.com/reports/2016-nanpa-annual-report.pdf) (visited June 28, 2017).

each day, and this does not address wireline and VoIP numbers that are also reassigned on a daily basis.[21]

Because the status of such numbers are rapidly changing, there is an ongoing risk that to the extent such numbers get allocated to a provider and subsequently assigned to a subscriber, the potential for blocking legitimate calls increases substantially. In essence, the Commission is proposing a de facto white list/black list blocking for these category of numbers. Such an approach is extremely risky, given the nature of spoofing, the fluidity of the list, and the volume of call traffic at issue. USTelecom has previously addressed the substantial challenges and risks associated with deployment of such black list/white list technologies.[22]

In its Notice, the Commission asks whether providers "can readily identify numbers that have yet to be allocated to any provider,"[23] and also about the "ability of providers to accurately and timely identify numbers" that have not yet been assigned to any subscriber. There is currently no commercially available means whereby voice providers can accurately determine whether a NANP number has been either allocated to a provider or assigned to a subscriber, and creating a new means to ascertain this information, such as a new industry database, would involve substantial security and technical complexities because of the call volumes associated with such a mechanism. A 2012 USTelecom analysis showed that in 2011, American consumers and businesses originated a total of 660 billion phone calls across wireline and wireless voice

[21] Declaratory Ruling and Order, *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Dissenting Statement of Commissioner Ajit Pai, 30 FCC Rcd. 7691, 80 FR 61129, FCC 15-72 (released July 10, 2015).

[22] *See e.g.*, USTelecom Response to Subcommittee on Consumer Protection, Product Safety and Insurance, pp. 6 – 9 (October 15, 2013) (available at: https://www.mccaskill.senate.gov/imo/media/doc/RobocallDetailedResponsetoSen%20McCaskill.pdf) (visited July 3, 2017) (*USTelecom Response*); *see also, USTelecom Comments*, pp. 14 – 16.

[23] *Notice*, ¶ 20.

platforms.[24] While the ability of any entity to maintain an accurate database of allocated and assigned numbers in near real-time is challenging in and of itself, the feasibility of providers to integrate such a database into the network to track – and potentially block – this volume of calls could be technologically infeasible.

And because robocallers are extremely adaptive, it is likely they could easily circumvent such an approach by spoofing legitimate (*i.e.*, assigned) numbers. While robocallers currently utilize only a small universe of phone numbers to conduct their operations, they are increasingly randomizing the phone numbers that they employ in their calling schemes. Once a database relying on unallocated or unassigned numbers is extensively deployed, robocallers could very easily and rapidly transition to utilizing assigned numbers in order to circumvent such protections. In fact, the widespread deployment of a database technology such as that proposed by the Commission could have the perverse effect of quickly nullifying any protections, while also making robocallers more difficult to identify, as they 'mask' their calling campaigns with legitimate numbers.

Accordingly, while USTelecom supports all of the proposed rules, it maintains that ongoing efforts within industry – particularly with respect to implementation of the SHAKEN/STIR standards – will be more beneficial and effective in identifying illegal robocalls than to focus on reassigned/unallocated numbers.

---

[24] *See*, Patrick Brogan, USTelecom Industry Analysis Report, *The Broadband and Mobile Transformation of Personal Communications*, November, 2012, pp. 17 – 18 (available at: http://www.ustelecom.org/sites/default/files/documents/Voice%20Competition%20Slides%202012-11-15.pdf) (visited June 27, 2017).

## IV. There are Varying Degrees of Risk Associated with Each of the FCC's Proposed Call Blocking Proposals.

USTelecom notes that while each of the Commission's four proposals for robocall blocking differ in approach, there are varying degrees of complexity and potential consumer harms resident in each. For example, while DNO efforts arguably represent a fairly straightforward approach to blocking calls, even in the tightly controlled manner instituted by the ITB Group, legitimate calls can be blocked. Potential subscribers to a DNO implementation who attests that they never initiate calls with a particular number, may find other parts of their business, or third parties' contracted services, that do. Indeed, as noted in the most recent Strike Force Report, "as happened during one of the [DNO] trials, legitimate calls will be blocked if any carrier attempts to implement blocks of purported inbound-only numbers without fully vetting the subscriber's understanding that the number is inbound-only."[25]

Moreover, the Commission's proposals regarding the blocking of unassigned and unallocated numbers is particularly risky, given the extreme fluidity of the numbering environment. Given the constant state of churn within this universe of numbers, the potential for a legitimate consumer to have their calls inadvertently blocked presents a very real risk. While the Commission appropriately raises protections for such consumers in its Notice of Inquiry, given the increasing prevalence of a variety of blocking tools available to consumers, this potential harm is increasing. As USTelecom has previously addressed,[26] as blocking technologies become more widely deployed by numerous third-party and/or network providers, consumers who are unable to complete phone calls through no fault of their own will be faced with a near-impossible task of figuring out how to fix the problem, or who to even contact.

[25] *April 2017 Strike Force Report*, p. 26.

[26] *See, USTelecom Response*, pp. 6 – 9.

Finally, until the implementation of the SHAKEN/STIR standards, the fundamental challenge carriers and consumers face is that the telephone number delivered with each call – whether initiated by a human or a machine – is the only way for a carrier or an end user to identify the purported calling party. These telephone numbers are easily hidden, disguised, or deliberately spoofed at origination and through call delivery, even though federal law prohibits such activity. Due to these varying degrees of risk, and the nature of any network blocking, deployment of such services by carriers must be carefully considered and vetted prior to full implementation by industry.

## V. Comments Regarding the FCC's Notice of Inquiry.

USTelecom also submits the following comments regarding issues raised in the Commission's Notice of Inquiry. The comments address issues regarding objective standards for identifying illegal robocalls; establishing safe harbors for providers engaging in voluntary blocking efforts; and protecting legitimate callers. USTelecom also recommends that the Commission provide necessary clarity relating to the sharing of Customer Proprietary Network Information (CPNI) between providers engaged in robocall mitigation efforts.

### A. Objective Standards to Identify Illegal Calls.

The Commission appropriately focuses a portion of its Notice on methods providers and third-party call blocking service providers employ in order to determine that a certain call is illegal.[27] Carriers and third-party providers should have sufficient flexibility in establishing such objective standards. USTelecom maintains that the development of a variety of such standards are beneficial to broader mitigation efforts against robocalls, since a diversity of approaches would create a more challenging operating environment for illegal robocallers.

[27] *Notice*, ¶¶ 29 – 33.

In addition, the Commission should be cautious about cataloguing which methods and approaches are better suited for identifying illegal robocalls. While many industry stakeholders have developed such methods and standards, an acknowledged industry best practice is to retain confidentiality of such practices. By publishing the manner in which robocalls can be blocked, illegal actors can use this as a roadmap for bypassing such measures. Ultimately, illegal robocallers will eventually adapt their practices to bypass evolving industry efforts, and such methods and practices will also need to evolve and change accordingly. The Commission should note, however, that a growing number of providers and third-party developers already deploy a broad assortment of approaches to identifying illegal robocalls.

### B. The FCC Should Implement a Safe Harbor for the Blocking of Calls Identified Using Objective Standards.

USTelecom supports the Commission's proposal to adopt a safe harbor to provide certainty to providers instituting blocking measures consistent with the rules adopted in this proceeding.[28] USTelecom agrees that providers instituting reasonable forms of blocking should not be deemed in violation of the Commission's rules and the Communications Act, nor should such providers have their call completion rates adversely effected due to such reasonable blocking.

In its Notice, the Commission appropriately notes that it must be cautious in providing too much specificity regarding safe harbors. USTelecom agrees with the Commission that such specificity would provide a "roadmap enabling makers of robocalls to circumvent call blocking by providers."[29] For example, USTelecom cautions the Commission regarding the use of established thresholds for volumes of calls, since that would essentially provide robocallers with

[28] *Id.*, ¶¶ 34 – 36.

[29] *Id.*, ¶ 34.

a publicly available ceiling under which they could operate. Given the highly fluid and evolving nature of the robocall environment, USTelecom believes it is best to afford providers with the necessary flexibility to adapt accordingly and work collaboratively in such an environment.

The Commission should also focus particular attention on the potential impacts that collective call blocking efforts may have with respect to the agency's call completion rules. In particular, USTelecom supports the Commission's proposal to exclude calls blocked in accordance with the rules it adopts in this proceeding from calculation of providers' call completion rates.[30] In particular, the Commission should address concerns regarding carriers' filing of the FCC Form 480 pursuant to the Rural Call Completion Order.[31] Although the Commission's Rural Call Completion Order accounts for the reporting of alleged autodialer traffic,[32] the proposals contained in its Notice adds additional layers of complexity and ambiguity. For example, a carrier instituting a DNO could potentially block millions of calls in the network, a portion of which would have terminated in rural areas. However, since the carrier is blocking calls at the request of the telephone number's subscriber, the carrier cannot provide "an explanation of the method the provider used to identify the autodialer traffic," as required under the Rural Call Completion Order. Indeed, the four proposals set forth in the Commission's Notice are based on analysis of a given *telephone number*, and not on any analysis of the *traffic* itself as required under the Rural Call Completion Order.

[30] *Id.*, ¶ 26.

[31] Report and Order and Further Notice of Proposed Rulemaking, *Rural Call Completion*, 28 FCC Rcd 16154, 78 FR 76218, 78 FR 76257, FCC 13-135, ¶¶ 65 – 68 (released November 8, 2013).

[32] *Id.*, ¶ 66.

### C. Protecting Legitimate Callers.

USTelecom appreciates and supports the Commission's inquiry into the crucial issue of protecting legitimate callers who may have their calls blocked. The importance of protecting legitimate callers is taking on increased importance, particularly as call-blocking services and initiatives continue to increase penetration within the marketplace. Such scenarios could arise in instances where voice providers block numbers directly, and for blocking services that consumers may opt into in order to block or filter potentially unwanted calls. It is an issue USTelecom and its members have been wrestling with for years, and this summer USTelecom is planning to host a workshop aimed at helping develop "best practices" for creating and maintaining blacklists.

USTelecom, however, discourages the Commission from adopting an approach that would formally mandate some form of 'white list.' To begin with, any such centralized white list would create a substantial security risk should it fall into the hands of even a single robocaller. Such a white list would effectively create a de facto master key that would provide robocallers with the unimpeded ability to generate high volumes of calls to unsuspecting consumers.

Moreover, in the event that such a list were to be breached, it would create three significant problems. First, it would immediately render as moot the protections for subscribers to such a list. Although the Commission's Notice keeps the scope of such a list fairly broad, it would likely include the tens of thousands of local police, fire, education, and public health agencies or districts across the country that would have their numbers on the list. Second, because robocallers would know that these numbers are white listed, they would immediately start spoofing these numbers to complete their calls. This in turn would significantly undermine

the reputational integrity of these organizations by associating their legitimate numbers with illegitimate criminal activities.

Finally, in order to remediate such a breach, white list subscribers, white list database managers and voice providers would face a series of abysmal options. Should the white listed numbers now be blacklisted in order to stop the robocalls? Should the potentially tens of thousands of white list subscribers have new numbers assigned to them? Should those numbers now be added to an updated white list?

USTelecom raises this issue not to cast aspersions on the importance of protecting legitimate callers, but rather to address the serious concerns that could arise in the event that such white lists fall into the wrong hands. The unfortunate reality is that while the majority of providers that constitute the nation's communications networks are working aggressively to combat illegal robocalls, instances in which one rogue provider breaches the integrity of a white list could have profound consequences.

### D. Telecommunications Carriers Can Share CPNI Under Section 222(d)(2)

Earlier this year, Congress passed a Congressional Review Act that was signed into law by the President that removed rules adopted by the Commission in its 2016 Privacy Order.[33] As a result of this Congressional action, the Commission's clarification provided to carriers in its 2016 Privacy Order regarding the sharing of CPNI was also removed. With the removal of these important clarifications related to the sharing of CPNI, USTelecom encourages the Commission to revisit this important issue, which is crucial to ongoing industry detection, assessment, traceback and mitigation efforts.

---

[33] *See*, Report and Order, *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, 31 FCC Rcd 13911, 81 FR 87274, FCC 16-148 (released November 2, 2016). *See also*, Public Law No: 115-22 (April, 2017) (available at: https://www.congress.gov/bill/115th-congress/senate-joint-resolution/34) (visited July 3, 2017).

As in its original proceeding, the Commission was correct to interpret Section 222(d)(2) to allow telecommunications carriers to use or disclose calling party phone numbers, including phone numbers being spoofed by callers, without additional customer consent when doing so will help protect customers from abusive, fraudulent or unlawful activities, including unlawful robocalls.[34] USTelecom maintains that a plain reading of the statute explicitly permits such sharing, and extends beyond just unlawful robocalls to include activities that involve "fraudulent, abusive, or unlawful use" of such services.[35]

Section 222(d) of the Act stipulates that "nothing" in the section "prohibits a telecommunications carrier" from "disclosing, or permitting access to" CPNI, so long as it falls within one of three defined categories.[36] One of those categories – Section 222(d)(2) – permits sharing CPNI so long as it is done "to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services."[37]

[34] *See*, *Notice*, at ¶ 118. This section of USTelecom's comments do not address the application of Section 222(d)(2) to BIAS providers.

[35] In previous instances, the Commission has defined robocalls to include calls made either with an automatic telephone dialing system (*i.e.*, an autodialer) or those with a prerecorded or artificial voice. *See e.g.*, Notice of Proposed Rulemaking, *Rules and Regulations Implementing the Telephone Consumer Protection act of 1991*, 31 FCC Rcd. FCC 15-71, n. 3 (released May 6, 2016). However, other fraudulent activities that occur over a telecommunications network may not fall into that category, but nevertheless may constitute a "fraudulent, abusive, or unlawful use" of the network. Such activities could include targeted fraud calls such as the Grandparent Scam and Jamaican Lottery Scam, or other activities that do not utilize an autodialer or a prerecorded voice.

[36] 47 U.S.C. §222(d).

[37] 47 U.S.C. §222(d)(2).

In instances where telecommunications carriers share some limited CPNI during robocall investigations,[38] it is clearly being done in order to both protect the rights and property of the carrier, as well as to protect users of those services (including their own customers) from the inherent fraud and abuse associated with such calls. As such, the Commission is correct to interpret the Section 222(d)(2) exclusion to allow such sharing.

Despite federal prohibitions against illegal spoofing, telephone numbers can be easily disguised, or deliberately spoofed at origination and through call delivery in a way that is malicious or fraudulent. Because calls can be processed over multiple providers' networks, the ability of carriers to share CPNI greatly facilitates their ability to collaboratively investigate instances of robocalls, ideally leading to their true origin. As a result, the sharing of CPNI by telecommunications providers is essential to ensuring accurate and thorough call traceback efforts in multiple providers' networks related to suspicious calling events.

The sharing of such information by telecommunications providers can benefit consumers by enabling providers to quickly, efficiently and cooperatively identify the true source of fraudulent, abusive or unlawful calls, including robocalls. In instances where calls are traced to their point of origin, this often enables investigating providers to work with the originating carrier to cease such calls initiated by its customer. Such efforts are also extremely valuable to law enforcement, since carriers' ability to trace calls through several networks can substantially assist law enforcement personnel in subsequent investigations.

In addition to interpreting Section 222(d)(2) to permit the sharing of CPNI, the Commission should also encourage such sharing between providers. The appropriate sharing of

[38] Carriers' use of CPNI in such instances is generally limited to the information necessary to conduct an appropriate investigation. This information generally includes the calling telephone number, the called telephone number, and the date and time of the call.

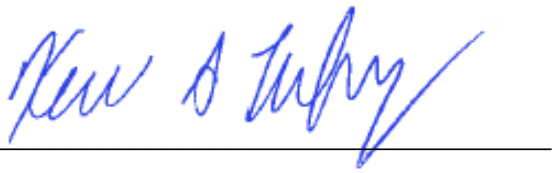
such information between larger numbers of telecommunications providers could positively impact unlawful robocall mitigation by making the identification of the true source of such calls more accurate and timely. The Commission's clarification on Section 222(d)(2) could also prove useful in encouraging reticent telecommunications providers to more willingly participate in the sharing of CPNI information during investigations into the source of unlawful robocall campaigns.

## VI. Conclusion.

USTelecom appreciates the Commission's proposals in this proceeding that would provide carriers with greater flexibility to address the robocall problem. USTelecom encourages the Commission to continue to work in a collaborative manner with all stakeholders engaged on this issue, and to adopt its proposed rules consistent with the issues and concerns discussed above.

Respectfully submitted,

USTELECOM ASSOCIATION

By: 

Kevin Rupy
B. Lynn Follansbee
Jonathan Banks

Its Attorneys
USTelecom Association
601 New Jersey Avenue, N.W.
Suite 600
Washington, D.C. 20001
(202) 326-7300

July 3, 2017