

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

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

REPLY COMMENTS OF AT&T

Amanda E. Potter
Gary L. Phillips
David Lawson
AT&T SERVICES, INC.
1120 20th Street, NW
Washington, DC 20036

Its Attorneys

July 31, 2017

TABLE OF CONTENTS

TABLE OF CONTENTS.....	i
DISCUSSION.....	4
I. THE COMMISSION SHOULD ADOPT A BROAD SAFE HARBOR FOR VOICE SERVICE PROVIDERS SEEKING TO COMBAT ILLEGAL AND DECEPTIVE ROBOCALLS	4
A. The Problem of Illegal and Deceptive Robocalls Requires a Shift in the Regulatory Focus of the Commission.	4
B. The Commission Should Establish a “Reasonable Best Efforts” Safe Harbor Standard.	6
C. Microsoft’s Call Blocking Example Demonstrates the Need for a Robust Safe Harbor.	10
II. THE COMMISSION ALSO SHOULD TAKE STEPS TO ENCOURAGE BROADER PARTICIPATION BY STAKEHOLDERS TO COMBAT ILLEGAL AND DECEPTIVE ROBOCALLS	12
CONCLUSION.....	14

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

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

REPLY COMMENTS OF AT&T

AT&T Services, Inc.¹ hereby submits the following reply comments in response to the Notice of Proposed Rulemaking and Notice of Inquiry issued in the above-captioned proceeding and the opening comments filed on July 3, 2017.² AT&T is committed to continuing its work, independently, as well as with the Commission and other stakeholders, to address the scourge of illegal and deceptive robocalls. AT&T therefore welcomes the Commission’s efforts to provide greater flexibility to voice service providers to protect consumers, and appreciates this opportunity to respond to the record developed in the proceeding thus far.

Despite the substantial and sustained efforts of providers, handset manufacturers, and application providers (both individually and collectively), as well as vigorous law enforcement, and consumer education campaigns, illegal and/or deceptive robocalling remains a pervasive problem. Indeed, as statistics cited by the Federal Trade Commission (“FTC”) confirm, consumers continue to be plagued by increasing numbers of illegal and/or deceptive robocalls.³ Specifically, consumer complaints to the FTC regarding “illegal calls”—and illegal robocalls in

¹ AT&T Services, Inc. is filing these reply comments on behalf of AT&T Mobility and its wireline operating affiliates (collectively, “AT&T”).

² *Advanced Methods to Target and Eliminate Unlawful Robocalls*, Notice of Proposed Rulemaking and Notice of Inquiry, 32 FCC Rcd 2306 (2017) (“NPRM”).

³ See Comments of the Federal Trade Commission, CG Docket No. 17-59, at 2-3 (filed July 3, 2017) (“FTC Comments”).

particular—have continued a steady upward climb through 2016,⁴ with a similar trend emerging for 2017.⁵

AT&T takes illegal and deceptive robocalls to its customers very seriously, and is attacking the problem on multiple fronts. For example, Randall Stephenson, AT&T Chairman and Chief Executive Officer, chaired the Robocall Strike Force, an industry-led task force convened for the purpose of identifying ways to address illegal and deceptive robocalls.⁶ In fact, the Commission issued this NPRM in direct response to the Strike Force’s October 2016 report.⁷ AT&T engineering experts also are collaborating with other Strike Force members to conduct tests of advanced Caller ID authentication techniques consistent with the SHAKEN/STIR standards discussed in the 2016 Strike Force Report. In addition, AT&T is pleased to work cooperatively with the Enforcement Bureau to identify robocallers engaged in illegal and/or deceptive activity.

Independently, AT&T offers Call Protect—a free service that automatically blocks calls from fraudsters and provides alerts regarding incoming calls from telemarketers, among others—to AT&T Mobility customers with HD Voice capability.⁸ Additionally AT&T makes it easy for

⁴ See *id.* at 2-3 and Attach. A (documenting substantial increases in the total number of consumer Do-Not-Call complaints and robocall complaints in 2015 and 2016, as well as increases in the average number of monthly Do-Not-Call complaints and robocall complaints).

⁵ See *id.* at 3 (stating that, “in four of the first five months of 2017, the FTC received more than 600,000 Do-Not-Call complaints each month and 61% of the monthly complaints—over 300,000—involve robocalls”).

⁶ AT&T, FCC Hosts First Robocall Strike Force Meeting; AT&T’s Stephenson to Chair Industry-Led Group (Aug. 19, 2016, 9:50 AM), <https://www.attpublicpolicy.com/fcc/fcc-hosts-first-robocall-strike-force-meeting-atts-stephenson-to-chair-industry-led-group/>.

⁷ See Robocall Strike Force, Robocall Strike Force Report (Oct. 26, 2016) (“2016 Strike Force Report”); NPRM ¶¶ 7-8, 16 (describing the 2016 Strike Force Report and the Strike Force’s request for Commission guidance regarding provider-initiated call blocking). Importantly, the work of the Strike Force continues through industry groups such as USTelecom, CTIA, and others. AT&T is a member of USTelecom and CTIA and continues to actively participate in Strike Force initiatives.

⁸ AT&T, AT&T Unveils AT&T Call Protect to Help Customers Manage Unwanted Calls (Dec. 20, 2016), http://about.att.com/story/att_call_protect.html.

customers to use other third-party apps like Nomorobo.⁹ AT&T also has taken (and continues to take) steps to address the problem of robocalls on its wholesale network. In particular, AT&T fraud management and network analytics teams established a program whereby AT&T blocks unwanted robocalls originating from AT&T's wholesale customers that traverse AT&T's network.¹⁰ As previously announced, AT&T blocked its one billionth unwanted robocall earlier this year using this new program.¹¹ AT&T recently surpassed the milestone of two billion blocked calls. Significantly, AT&T's work on these and other robocall-related initiatives continues full-throttle, as AT&T's experts in engineering, fraud management, and analytics, among others, continue to develop new tools and methods (and improve existing ones) to address the problem of robocalls.

Commission efforts to empower providers to continue to innovate in this space, including through the adoption of an order in the instant proceeding, are *precisely* what is needed for AT&T and others to continue to make headway to address the problem of illegal and deceptive robocalls more effectively. Adoption of the rule proposals set forth in the NPRM are an important step toward that goal, but as the 2016 Strike Force Report emphasized, “[t]here is no silver bullet to solve the robocalling problem.”¹² On the contrary, as USTelecom explained in its comments, mitigating the impact of illegal and deceptive robocalls will require a multi-pronged approach involving active participation by *all* stakeholders, including the Commission, other law

⁹ Nomorobo currently is available for free download for VoIP landlines. For smartphones, Nomorobo charges a small per device, per month fee. Nomorobo is not available for traditional wired landlines at this time. *See* www.nomorobo.com.

¹⁰ AT&T, More Than 1 Billion Robocalls Blocked (Apr. 13, 2017), http://about.att.com/story/more_than_one_billion_robotcalls_blocked.html.

¹¹ *See id.*

¹² 2016 Strike Force Report at 2. *See also* Comments of the Alliance for Telecommunications Industry Solutions, CG Docket No. 17-59, at 11 n.22 (filed July 3, 2017); Comments of CTIA, CG Docket No. 17-59, at 16 (filed July 3, 2017); Comments of Comcast Corporation, CG Docket No. 17-59, at 4 (filed July 3, 2017) (“Comcast Comments”).

enforcement agencies, industry, and consumers themselves.¹³ To that end, AT&T supports the adoption of a safe harbor for providers that, notwithstanding adherence to the Communications Act of 1934, as amended (the “Act”), and the Commission’s rules, inadvertently block a legitimate call. AT&T also is concerned by the comments of Microsoft, which take a myopic view of the robocalling problem, and ignore the role of outbound-only voice services, such as SkypeOut, in perpetuating illegal calls, including robocalls. AT&T urges the Commission to affirm the ability—indeed, responsibility—of these stakeholders to continue to innovate to combat illegal and deceptive robocalls.

DISCUSSION

I. THE COMMISSION SHOULD ADOPT A BROAD SAFE HARBOR FOR VOICE SERVICE PROVIDERS SEEKING TO COMBAT ILLEGAL AND DECEPTIVE ROBOCALLS

A. The Problem of Illegal and Deceptive Robocalls Requires a Shift in the Regulatory Focus of the Commission.

Voice service providers such as AT&T generally do not want to block calls placed to their customers, and, indeed, the Commission’s rules, absent the call recipient’s consent, generally prohibit them from doing so.¹⁴ The NPRM acknowledges the tension between the Commission’s call blocking rules and precedent and the desire to address the pervasive problem of robocalls.¹⁵ AT&T agrees that the Commission must balance the important policy considerations of consumer protection and network reliability in this context.

¹³ See Comments of the USTelecom Association, CG Docket No. 17-59, at 4 (filed July 3, 2017).

¹⁴ See *Developing a Unified Intercarrier Compensation Regime; Establishing Just and Reasonable Rates for Local Exchange Carriers*, Declaratory Ruling, 27 FCC Rcd 1351 ¶ 11 (WCB 2012); see also *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991 et seq.*, Declaratory Ruling and Order, 30 FCC Rcd 7961 ¶ 158 (2015) (“2015 Omnibus TCPA Order”); NPRM ¶ 9 n.31 (citing Section 201(b) of the Act and the Commission’s call blocking precedent).

¹⁵ NPRM ¶ 10. See also 2015 Omnibus TCPA Order ¶¶ 154, 158.

Unfortunately, current rules are discouraging, if not thwarting outright, providers' efforts to tackle the issue of illegal and deceptive robocalls. Indeed, as the statistics cited above reflect, and numerous commenters confirm, the robocalling problem continues to grow. AT&T thus strongly disagrees with commenters who advocate the adoption of rigid customer opt-in/consent requirements to enable providers to block illegal or deceptive robocalls and, instead, supports the FTC, which recognizes that "provider-based call blocking is integral to solving the problem of illegal robocalls."¹⁶ Simply put, voice service providers need more arrows in their quiver before industry can more effectively combat illegal and deceptive robocalls.

As AT&T previously explained, one key reason for the rapid proliferation of robocalls is the technological advances that allow illegal dialers to "spoof" numbers—that is, to use fake caller IDs.¹⁷ And as AT&T has witnessed, robocallers' spoofing activities have only grown in sophistication. For example, AT&T has seen a marked increase in the incidence of incoming robocalls that engage in "neighbor" spoofing. As the Commission is aware, neighbor spoofing occurs when a robocaller spoofs a telephone number with a particular NPA-NXX (*e.g.*, 202-555-XXXX) and then autodialers telephone numbers with the identical NPA-NXX combination.¹⁸ Neighbor-spoofed robocalls tend to have a higher call-answer rate, because consumers are more easily duped into answering a call from a number that they (at least partially) recognize, and because consumers are less likely (at least initially) to identify the call as a robocall and ignore the call when the calling number is similar to their own telephone number.

¹⁶ FTC Comments at 2; *see also id.* at 4 ("Call-blocking technology, if implemented on a widespread basis, could reduce revenues for illegal telemarketing operations, thereby making it more difficult to operate profitably."); Comcast Comments at 17 (supporting the adoption of a rule "that affirmatively authorizes voice providers to block calls determined to be illegal spoofed robocalls using *any* reasonable method based on objective criteria"); *id.* at 11 (advocating that voice providers "be equipped with an array of tools for addressing illegitimate robocalling practices").

¹⁷ *See* Comments of AT&T, CG Docket No. 02-278, WC Docket No. 07-135, at 2-4 (filed Jan. 23, 2015).

¹⁸ *See, e.g., Adrian Abramovich, Marketing Strategy Leaders, Inc., and Marketing Leaders, Inc., Notice of Apparent Liability*, File No. EB-TCD-15-00020488, 32 FCC Rcd 5418 ¶ 12 (2017) ("*Abramovich NAL*").

Neighbor-spoofed robocalls also are more difficult for providers to identify and block. As an initial matter, the spoofed number often is a legitimate telephone number, and may even be assigned and in use at the time the robocaller spoofs it. Moreover, because the robocall typically is directed to fewer telephone numbers (*i.e.*, only those telephone numbers with the same or similar NPA-NXX combination), such a robocall may not be flagged as potentially problematic and warranting investigation. But even in cases where AT&T identifies illegal or deceptive robocall campaigns using neighbor spoofing techniques, AT&T currently has limited flexibility to target such campaigns as a result of the call blocking rules and precedent, discussed above.

Robocallers are relentless in their pursuit to deceive and defraud American consumers. Indeed, neighbor spoofing is just one example. AT&T identifies hundreds of illegal or highly suspicious robocall campaigns and traffic trends on its network *every single day*. Just as disturbing, fraudsters and unscrupulous telemarketers constantly adjust their tactics to evade detection and continue their illegal activity. The problem of illegal and deceptive robocalls thus requires that industry efforts to block such calls be as dynamic and adaptable as the activities of the criminals that providers seek to block. Modifications to existing Commission rules will be needed to afford voice service providers with similar dynamism and adaptability.

B. The Commission Should Establish a “Reasonable Best Efforts” Safe Harbor Standard.

Against this backdrop, the need for a call blocking safe harbor is crystal clear. Indeed, while AT&T supports the Commission’s efforts to ensure high-quality rural call completion and believes that existing Commission rules regarding other inappropriate call blocking practices can and should remain in place to address those important concerns, voice service providers require more flexibility to enable the innovation and experimentation necessary to more effectively

address the robocall problem,¹⁹ and which the current rules would not allow. An appropriately tailored safe harbor would provide the needed flexibility.

AT&T proposes that the Commission issue a notice of proposed rulemaking to adopt a “reasonable best efforts” standard that would apply to the inadvertent blocking of legitimate voice calls. Under the proposed standard, a voice service provider that mistakenly blocks legitimate traffic to end users would not be deemed to violate the Act or the Commission’s rules, and such blocked call(s) would not be attributable towards the carrier’s call completion rates, so long as the provider has made “reasonable best efforts” to avoid such call blocking. AT&T further proposes that the Commission define “reasonable best efforts” to require that a provider: (i) cooperate with and participate in industry-led efforts designed to address the issue of illegal, deceptive, and unwanted robocalls, and (ii) adopt and implement policies and procedures detailing its practices to identify and address such robocalls, including procedures to cease blocking of any calls upon learning they are legitimate calls. With respect to the scope of policies and procedures that would satisfy the latter prong, the Commission should rely on the non-exhaustive list of activities identified as “reasonable efforts” that a provider may take to confirm a call it blocks is, in fact, illegal, including: “soliciting and reviewing information from other carriers, performing historical and real-time call analytics, making test calls, contacting the subscriber of the spoofed number, inspecting the media for a call (audio play back of the Real Time Protocol stream to understand the context of the call), and checking customer complaint sites.”²⁰

¹⁹ See, e.g., FTC Comments at 8.

²⁰ 2016 Strike Force Report at 40 (Attachment 2). As the 2016 Strike Force Report explains, such a list of policies and procedures would be non-exhaustive and thus capable of evolving as new best practices evolve and change. See *id.*

AT&T submits that a broad safe harbor is necessary and appropriate for at least two reasons. First, an overly specific safe harbor would threaten the efficacy of industry’s efforts to combat robocalls. Indeed, the Commission should be careful to avoid handing robocallers a playbook detailing how to avoid detection/blocking on providers’ networks. For example, if the Commission were to establish a specific robocall threshold as part of any safe harbor, robocallers would quickly adjust to ensure that the number of autodialed calls placed do not exceed the threshold, and thus ensure that providers would not block their robocalls. Such a specific standard necessarily would damage providers’ efforts to combat the robocall problem.

Second, the Commission’s safe harbor standard should be flexible enough to allow—indeed, *encourage*—the development of new tools and practices to more effectively tackle the problem of illegal and deceptive robocalls. As the FTC explained in its comments, “[d]etermining whether a call is likely illegal is a dynamic process that can require analyzing multiple sets of available data, making reasonable judgments based on current and past data, adjusting analysis to stay ahead of illegal call tactics, and continual development of new techniques to detect illegal calls.”²¹ AT&T knows this process well, as it monitors its network for suspicious traffic patterns on a daily basis and, as appropriate, blocks illegal or deceptive traffic traversing AT&T’s wholesale network. Moreover, AT&T agrees that, while progress is being made, the best tools and practices for addressing unwanted robocalls likely have yet to be developed. Accordingly, the Commission should take care to avoid a rigid safe harbor standard, as such a standard (at worst) would lock providers into specific call blocking practices—even if ineffective—or (perhaps at best) would impede the innovation and experimentation that is imperative to target robocalls.

²¹ FTC Comments at 8.

The safe harbor detailed herein is consistent with safe harbor proposals in the opening comments of the FTC and Comcast. In particular, the FTC supported a safe harbor that would require providers to “develop an internal protocol that relies on multiple data points for flagging a presumptively illegal call, is managed by a dedicated team, and includes an effective mechanism to address inadvertent blocking of legitimate callers.”²² Likewise, Comcast recognized the need for safe harbor protections “for entities acting in good faith” that would “preserve providers’ flexibility to implement reasonable tools and not mandate that providers obtain an ‘opt-in’ from subscribers in order to block calls, given the reasonable presumption that subscribers would prefer not to receive these calls.”²³ AT&T wholeheartedly agrees and would welcome the incorporation of such principles into any safe harbor the Commission ultimately adopts.

Critically, AT&T’s proposed safe harbor would not implicate the Commission’s legitimate interest in addressing rural call completion concerns or other inappropriate call blocking activity. The Commission recognized this distinction in 2015, agreeing that “the policy implications raised in this proceeding [regarding robocall-targeted call blocking initiated at the consumer’s request] are separate and distinct from the requirement of carriers to complete calls and refrain from engaging in abusive and anticompetitive practices.”²⁴ The proliferation of robocalls—whether illegal and/or deceptive, or simply annoying—undermines the public’s confidence and trust in our nation’s communications network. Put another way, consumers are less inclined to purchase services that cause them to be subjected to robocalls.²⁵ The

²² *Id.*

²³ Comcast Comments at 5, 9, 12, 16-17 (supporting the adoption of safe harbors for provider-initiated blocking relying on SHAKEN/STIR, Do-Not-Originate, traceback, and other “as-yet undeveloped” methodologies).

²⁴ *2015 Omnibus TCPA Order* ¶ 158 (citation omitted).

²⁵ Likewise, to the extent a voice service provider could (and did) choose to block calls in a manner that would result in the frequent blocking of legitimate calls, consumers would be expected to respond in a

Commission's interest in preserving a reliable, ubiquitous communications network thus now compels greater flexibility with respect to provider-initiated call blocking. Moreover, commenters who oppose a safe harbor offer no basis on which the Commission reasonably could conclude that voice service providers would engage in call blocking for any inappropriate purpose on the pretext of targeting illegal and deceptive robocalls. The Commission therefore can and should find that, far from raising public policy concerns, the impetus of providers to block robocalls aligns with the public interest.

C. Microsoft's Call Blocking Example Demonstrates the Need for a Robust Safe Harbor.

By the same token, the Commission should not allow the risk that a provider will inadvertently block legitimate traffic to immobilize the efforts of the Commission and others committed to tackling the scourge of illegal and deceptive robocalls. Microsoft in its comments opposed a safe harbor and provided an example of allegedly "legitimate" SkypeOut calls that were blocked by "a major U.S. carrier ... under the misperception that they constituted illegal robocalls."²⁶ Microsoft's opposition is misplaced, and the call blocking example it cited should not dissuade the Commission from establishing a safe harbor.

AT&T has experience with outbound-only voice services, including SkypeOut, in this context. Skype does not assign telephone numbers to SkypeOut users or require SkypeOut users to populate the caller ID field with a valid, verified telephone number when placing a call. Rather, as Microsoft explained, "Skype populates otherwise-unpopulated caller ID fields on SkypeOut calls with a valid telephone number allocated to Skype (and within Skype's pool of

²⁶ similar manner. The key point is that, given the flexibility to more aggressively combat robocalls, voice service providers by and large have every incentive to weed out the bad from the good. Microsoft Comments at 6-7.

numbers available for assignment) but not assigned to a specific user.”²⁷ AT&T refers to such telephone numbers as aggregation lines, because voice traffic from multiple unaffiliated users is grouped using a common telephone number and thus identifiable on AT&T’s network as traffic originating from a single source.

Because an aggregation line can generate significant volumes of traffic, it is not uncommon for traffic associated with such a line to be flagged as suspicious by AT&T (and likely other providers).²⁸ And although Skype’s CLEC partner at times places a line announcement on Skype aggregation lines to identify the telephone numbers as ones associated with a VoIP provider, this is not a consistent practice by Skype or among outbound-only voice service providers more generally.²⁹ As a result, ostensibly “legitimate” traffic originating from certain outbound-only voice services shares many of the same characteristics as traffic originating from an illegal or deceptive robocalling operation making use of an unallocated or unassigned telephone number. Indeed, traffic delivered using an aggregation line can be indistinguishable from illegal robocalling traffic to an intermediate or terminating carrier, notwithstanding the good-faith efforts of the carrier(s) to investigate the suspicious traffic.³⁰

²⁷ *Id.* at 14.

²⁸ As a threshold matter, and independent of the volume of traffic delivered using a Skype aggregation line, the suggestion that all SkypeOut traffic is “legitimate” is disingenuous. *Id.* at 6. As discussed below, outbound-only voice services like SkypeOut are ripe for exploitation by fraudsters and other bad actors. See Section II *infra*.

²⁹ For example, AT&T is aware of an aggregation line used by an outbound-only voice service provider that, as recently as July 31, 2017, repeats a generic line announcement (“no routes found”) rather than an announcement that specifically identifies the telephone number as one associated with a VoIP service provider. The same line also appears on consumer complaint websites. In fact, AT&T identified 167 pages of complaints associated with the aggregation line on a *single* complaint website.

³⁰ When AT&T blocks calls, it relies on multiple, varied investigative protocols to determine whether the traffic is prohibited under the terms of its business contracts. For example, AT&T makes test calls to telephone numbers to determine whether the number is valid and in use. In addition, AT&T’s fraud management team researches telephone numbers associated with suspicious traffic on robocall complaint websites. To the extent AT&T has reason to believe that a legitimate telephone line is being illegally spoofed, AT&T routinely coordinates with the wholesale customer handing off the traffic to seek the customer’s assistance in identifying any illegal or prohibited activity. As a result of these and other investigative protocols, the inadvertent blocking of legitimate traffic is unlikely to occur in situations that

While the inadvertent blocking of *any* legitimate traffic is regrettable, the Commission should not allow the perfect to be used as the enemy of the facts-based, good-faith efforts of providers to address the scourge of illegal and deceptive robocalls. More specifically, far from making the case against a safe harbor, the Microsoft SkypeOut example demonstrates precisely why a robust safe harbor is needed. Absent flexibility to continue to develop, test, and refine methods of blocking illegal and deceptive robocalls, providers will be reluctant to implement measures to address the scourge of illegal and deceptive robocalls.³¹ For example, AT&T’s analytics-based call blocking program to date has been limited to the blocking of traffic deemed prohibited under its business contracts, which necessarily limits the scope—and efficacy—of AT&T’s blocking efforts.³² Moreover, there are other concrete and more effective steps that stakeholders, including Skype, can and should be taking to avoid the inadvertent blocking of legitimate calls placed by their users, as discussed below. AT&T urges the Commission to establish an appropriately tailored safe harbor.

II. THE COMMISSION ALSO SHOULD TAKE STEPS TO ENCOURAGE BROADER PARTICIPATION BY STAKEHOLDERS TO COMBAT ILLEGAL AND DECEPTIVE ROBOCALLS

The call blocking example provided by Microsoft underscores the need for *all* stakeholders in the voice services ecosystem—whether facilities-based, like AT&T, or non-

do not involve the use of aggregation lines. In any event, AT&T also has established procedures for reversing a block in the event it learns of an impact on legitimate traffic.

³¹ See, e.g., FTC Comments at 8; Comcast Comments at 9 (“Absent a safe harbor, voice providers may be reluctant to implement reasonable robocall mitigation techniques that, while highly effective, may not be completely error-free and could otherwise expose providers to enforcement action for inadvertently blocked calls.”).

³² The more than two billion calls blocked by AT&T thus represent only a small subset of the illegal and/or deceptive call flow that could be addressed through provider-initiated call blocking that relies on data analytics, consumer complaints, and other criteria. Cf. *Abramovich NAL* ¶ 1 (identifying “one of the largest spoofed robocall campaigns that the Commission has ever investigated, involving nearly 100 million robocalls during a three-month period in 2016”). As ZipDX recognized, AT&T’s analytics-based call blocking program has been more effective than other widely known consumer opt-in call blocking tools. See Comments of ZipDX, CG Docket No. 17-59, at 18-19 (filed June 27, 2017).

facilities-based, like Skype—to affirmatively target and address the problem of illegal and deceptive robocalls. While AT&T shares Microsoft’s concerns regarding robocalls used to facilitate tech support scams,³³ the NPRM appropriately is focused on the much broader universe of illegal robocalls overall. AT&T urges the Commission to take steps to encourage—if not compel—all stakeholders to take action to combat illegal robocalls, including through the implementation or modification of procedures to prevent or discourage robocallers from using services for nefarious purposes.

As discussed above, illegal robocallers and other fraudsters will use every available avenue to pursue their unlawful objectives. This includes the exploitation of weaknesses in a voice service provider’s platform that enable a bad actor to operate anonymously. It is no secret that outbound-only voice services like SkypeOut include such vulnerabilities.³⁴ AT&T submits that users of such services who engage in illegal robocalling (or other illegal activity) should not be able to avoid detection merely because the provider does not assign individual telephone numbers to users or otherwise take steps to uniquely identify traffic of each user. On the contrary, outbound-only voice service providers can and should explore ways to more actively and effectively monitor traffic patterns by their users for the purpose of investigating suspicious activity (and terminating the service of bad actors), as well as identifying and escalating call completion issues in a timely manner.³⁵

³³ See Microsoft Comments at 2.

³⁴ Indeed, the “feature that prevents calls lacking caller ID from ringing,” *see id.* at 14, exists precisely *because* fraudsters and other bad actors use services that do not assign unique individual telephone numbers (such as SkypeOut) to avoid detection.

³⁵ In AT&T’s experience, troubleshooting a call completion issue takes hours or days, not months. As noted above, AT&T has the appropriate procedures in place to quickly reverse a call block that is affecting legitimate traffic, and AT&T expects that most other carriers have similar procedures, but a carrier cannot address an issue about which it (or, apparently, the service provider of the originating calls) is not aware.

CONCLUSION

AT&T stands ready, willing, and able to continue to assist the Commission's efforts to combat illegal and deceptive robocalls. Consistent with the proposals set forth herein, AT&T urges the Commission to issue a notice of proposed rulemaking to establish a safe harbor standard enabling voice service providers to more effectively target this serious problem.

Respectfully submitted,

/s/ Amanda E. Potter
Amanda E. Potter
Gary L. Phillips
David Lawson
AT&T SERVICES, INC.
1120 20th Street, NW
Washington, DC 20036

Its Attorneys

July 31, 2017