Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

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

August 31, 2020

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

COMMENTS OF AT&T

AT&T Services, Inc.[1] ("AT&T") hereby submits these comments in response to the Commission's *Fourth Further Notice of Proposed Rulemaking* in the above-captioned proceeding, which seeks comment on a number of proposed robocall prevention and mitigation measures.[2]

INTRODUCTION AND SUMMARY

AT&T welcomes this latest step in the Commission's ongoing efforts to implement both greater flexibility and heightened accountability for voice service providers, all with the express goal of protecting consumers against the scourge of illegal and unwanted robocalls. Despite the substantial and sustained efforts of providers, handset manufacturers, application providers, regulators, law enforcement, and legislators, illegal robocalls remain a pervasive problem. AT&T takes the problem of illegal and unwanted robocalls to its customers very seriously and, as the Commission is aware, has taken aggressive action on multiple fronts to protect its network and customers. Chief among AT&T's wish list for its robocall mitigation "toolbox" has been its longstanding request for a call blocking safe harbor for provider-initiated call blocking programs

---

1 AT&T Services, Inc. is filing these comments on behalf of its voice services affiliates.

2 *Advanced Methods To Target and Eliminate Unlawful Robocalls; Alarm Industry Communications Committee Petition for Clarification or Reconsideration; American Dental Association Petition for Clarification or Reconsideration*, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking, CG Docket No. 17-59, FCC 20-96 (rel. July 17, 2020) (as appropriate, "*FFNPRM*" or "*Third Report and Order*").

targeting suspected illegal calls.[3] AT&T appreciates the numerous and sustained incremental steps the Commission has taken to get to this point—just one step away from adopting such a safe harbor. AT&T urges the Commission to adopt the safe harbor without further delay.

Likewise, AT&T welcomes the other proposals advanced in *FFNPRM* designed to hold voice service providers accountable for illegal traffic originating on their networks but favors rules that do not impose overly prescriptive (or proscriptive) regulatory requirements. AT&T thus supports the Commission's proposal to require voice service providers to cooperate in the industry traceback process and agrees that the Commission should not affirmatively authorize providers to block calls based solely on STIR/SHAKEN data at this time. AT&T also supports the adoption of USTelecom's robocall mitigation proposal as the most appropriate framework to prevent and mitigate bad traffic on the public switched telephone network. Finally, AT&T welcomes the adoption of a blocked call list requirement so long as it is appropriately tailored to opt-in and opt-out call blocking programs.

DISCUSSION

I. AT&T SUPPORTS THE COMMISSION'S EFFORTS TO ENABLE PROVIDERS TO MORE AGGRESSIVELY TARGET UNLAWFUL OR UNWANTED ROBOCALLS

A. The Commission Should Adopt the Proposed Safe Harbor for Provider-Initiated Call Blocking Programs.

AT&T has long sought a call blocking safe harbor for provider-initiated call blocking programs and thus welcomes the proposal to implement such a safe harbor at long last. As the

[3] To avoid potential confusion, AT&T uses the term "provider-initiated" rather than "network-based" to identify the call blocking programs that would be covered by the proposed call blocking safe harbor. *See FFNPRM* ¶ 104-06. Certain consumer facing, opt-in or opt-out call blocking programs, including AT&T Call Protect, are themselves "network-based." AT&T therefore prefers to distinguish between the two based on their customer facing characteristics. In particular, AT&T Call Protect is offered to AT&T's post-paid mobile wireless customers on an opt-out basis, while AT&T's provider-initiated call blocking program operates without explicit or implicit consumer consent.

Commission is aware, AT&T has led the industry in the area of provider-initiated call blocking of suspected illegal calls, implementing a comprehensive network-based program to block calls that—after thorough analysis and investigation—AT&T's global fraud team reasonably determines are illegal. Under this program, AT&T compiles a suspected robocall report that aggregates call data to help detect suspicious calls. As previously detailed in the record, these data include, but are not limited to: average call duration data, call completion rates, CNAM values, call volumes and the timeframes in which calls are placed, complaint data (including Commission and Federal Trade Commission ("FTC") complaint data), sequential dialing patterns, and call volumes to telephone numbers on the FTC's Do Not Call list. The suspected robocall report is updated on a virtually continuous basis. Based on the information in the suspected robocall report, AT&T investigates suspect telephone numbers using myriad techniques, including by dialing the suspect telephone number or reviewing various other complaint data sources. When an AT&T fraud investigator is reasonably confident that the telephone number is being used to place illegal calls, the investigator implements a block on the telephone number.[4]

Launched in 2016, AT&T's provider-initiated call blocking program has now blocked more than 6.5 billion suspected illegal robocalls on AT&T's wholesale IP and mobile networks, benefiting not only consumers purchasing AT&T service but also the networks and customers of AT&T's carrier partners. Further, complaint data gathered by AT&T indicate that the call blocking program is highly accurate. Out of more than 6.5 billion calls blocked, AT&T has reversed call blocks on valid telephone numbers fewer than ten times. Since launching a custom caller announcement, AT&T has received approximately 300 complaints, the vast majority of

[4] *See* Comments of AT&T, CG Docket No. 17-59, WC Docket No. 17-97, at 9 (filed Jan. 29, 2020).

which involved calls that displayed invalid telephone numbers. AT&T estimates that the false positive rate for its provider-initiated call blocking program remains orders of magnitude less than one percent.[5]

These data confirm the Commission's stated belief that "no reasonable consumer would want to receive calls that are highly likely to be illegal, and thus there is no need for consumers to have the opportunity to opt in or opt out."[6] This certainly is true based on AT&T's experience. *First*, it goes without saying that the chief complaint regarding robocalls—from anyone—is that there continues to be too many of them. Consumers, businesses, regulators, and legislators alike desire *more* action to tamp down robocall volumes, not less.

Second, although AT&T has received only a small handful of complaints—and fewer than ten that warranted remedial action—from *callers* related to the provider-initiated call blocking program, AT&T has received zero complaints from *consumers* regarding calls they did not receive, either directly or indirectly from carrier partners. At a minimum, the absence of complaints suggests that consumers do not miss, and do not wish to receive, the suspected illegal calls blocked by AT&T's global fraud team. Likewise, even when taking into account unsubstantiated complaints, the very low number of complaints from callers regarding AT&T's provider-initiated call blocking program indicates that the program is appropriately calibrated to target only those calls—i.e., suspected illegal calls—for which the Commission may reasonably and objectively conclude that consumers do not want to receive.

Third, consumer behavior in relation to analytics-based call blocking services, whether offered on an opt-in or opt-out basis, also is instructive for the Commission. Such consumer

---

5 *See* Letter from Joan Marsh, AT&T, to Mika Savir, FCC, CG Docket No. 17-59, WC Docket No. 17-97, at 5 (filed Feb. 28, 2020) ("AT&T Feb. 28, 2020 CGB Response Letter").

6 *FFNPRM* ¶ 105.

facing call blocking services, including AT&T Call Protect and Digital Phone Call Protect, are enormously popular with consumers. The flexibility afforded by the Commission in the *2019 Call Blocking Declaratory Ruling* further underscores this point.[7] Since AT&T's transition of AT&T Call Protect to an opt-out service more than one year ago, the opt-out rate has remained incredibly low. Thus, notwithstanding the broader net cast by AT&T Call Protect and similar services, which block not only suspected illegal calls but also certain categories of unwanted calls (at the consumer's request), consumers continue to show an affinity for call blocking as a key robocall mitigation mechanism. Consumer behavior thus lends only support, and not opposition, to the adoption of a call blocking safe harbor to cover provider-initiated call blocking programs targeting calls that are highly likely to be illegal.

AT&T supports the proposal to limit the scope of the safe harbor to provider-initiated call blocking programs, such as AT&T's, that include human oversight, reasonable analytics, and network monitoring.[8] However, AT&T urges the Commission to avoid adopting overly prescriptive requirements. Significantly, although provider-initiated call blocking programs that target suspected illegal robocalls are relatively new (including AT&T's, which launched in 2016), voice service providers' efforts to target fraud on their networks and protect their customers are anything but.[9] The proliferation of illegal robocalls in recent years is merely the latest example of fraudsters leveraging technology and evolving their tactics in their pursuit to

---

7 *See Advanced Methods To Target and Eliminate Unlawful Robocalls*, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, 34 FCC Rcd 4876 (2019) ("*2019 Call Blocking Declaratory Ruling*") (authorizing the provision of consumer facing call blocking tools on an opt-out basis).

8 *FFNPRM* ¶ 105.

9 *See 2019 Call Blocking Declaratory Ruling* ¶ 23 n.53 (confirming that the obligation of voice service providers to complete calls "does not extend to illegal calls, calls blocked by consumer choice, or calls for which the Commission has authorized blocking"); *Total Telecommunications Services, Inc. and Atlas Telephone Company, Inc., Complainants, v. AT&T Corporation, Defendant*, File No. E-97-003, FCC 01-84 ¶ 34 (2001) (concluding that call blocking commencing in 1995 "was perfectly reasonable in view of the fact that Total and Atlas engaged in an unlawful scheme"); *id.* ¶ 35 (finding that "AT&T's decisions to block traffic to Audiobridge did not violate sections 201, 202, 214, or 251 of the Act").

deceive and defraud American consumers. To be effective at fighting back, providers must be nimble, which, in turn, requires flexibility. AT&T thus urges the Commission to continue its light-touch approach to regulating voice providers' robocall mitigation efforts. And at all costs, the Commission should avoid adopting rules that would impede existing provider-initiated call blocking programs, including AT&T's, which already have demonstrated their effectiveness.

B. The Commission Should Not Authorize Call Blocking Based Solely on STIR/SHAKEN Information at this Time.

Although AT&T does not believe any affirmative proscription is necessary, AT&T agrees with the Commission that it should not authorize call blocking based solely on STIR/SHAKEN data at this time.[10] While STIR/SHAKEN has an important role to play in combating illegal robocalls, the protocols were not designed to be, and presently are not, a suitable tool for determining whether a call is illegal. The Commission's record reflects the opinions of numerous experts who have explained that the presence or absence of STIR/SHAKEN authentication and verification *on their own* are neither necessary nor sufficient to indicate that a call should be blocked. As AT&T's Martin Dolly, a co-author of both the SHAKEN and STIR standards, has noted, the standards validate the caller ID information associated with a call and identify the attesting provider.[11] While this certainly is useful information for providers to have when making blocking decisions, it is important to recognize its limitations. This sentiment was repeated time and again at the Commission's July 11, 2019

---

10 *See*, *e.g.*, *FFNPRM* ¶ 83.

11 *See* Martin Dolly, *An Introduction and Overview of the STIR / SHAKEN Framework*, AT&T (Dec. 4, 2018) (*"AT&T Presentation"*), https://www.sipforum.org/download/an-introduction-and-overview-of-the-stir-shaken framework/?wpdmdl=3530&refresh=5d2e1ad1a6bdc1563302609). Chris Wendt of Comcast, who co-authored both standards, stated that STIR/SHAKEN alone would not determine "whether the call is illegitimate or legitimate, or what the intent of the call is, or what the content of the call is." Chris Wendt, Director of Technical Research & Development for IP Communications, Comcast, and Co-author of SHAKEN and STIR standards, Statement at the FCC Robocall Summit, at 00:08:07 – 00:08:26 (July 11, 2019) ("*Wendt Statement*").

STIR/SHAKEN Robocall Summit.[12] One panelist there noted that even in the case of a fully attested call, "it could still be the devil himself calling from a verified number."[13] Another panelist noted that determinations regarding whether a call is unwanted or illegal were a "hard thing in general," and a more suitable approach is to leave such determinations to "analytics and other tools."[14]

And as the Commission has stated, "SHAKEN/STIR does not authenticate the content of the call," but instead only authenticates the telephone number displayed as caller ID.[15] The Alliance for Telecommunications Industry Solutions ("ATIS")—the industry-led organization helping to successfully establish this important caller ID authentication framework—has explained that the SHAKEN standard "was never intended to be a complete solution for the robocalling problem," and is instead "an important tool in a multi-layered approach."[16] ATIS describes the STIR/SHAKEN standards as a framework designed to achieve two discrete purposes: "the authentication and assertion of a telephone identity by an originating service provider," and "the verification of the telephone identity by a terminating service provider."[17] ATIS has further emphasized that "information on the 'intent' [of a call] was never part of SHAKEN,"[18] and that the standard "verifies that the entity originating a call is entitled to use the phone number displayed – nothing more!"[19] It also has stated that, while SHAKEN is focused

---

12 *See SHAKEN/STIR Robocall Summit*, FCC (July 11, 2019), https://www.fcc.gov/SHAKENSTIRSummit ("*FCC Robocall Summit*").

13 *See* Scott Hambuchen, Chief Information Officer, First Orion, Statement at the FCC Robocall Summit, at 1:43:21 – 1:43:40 (July 11, 2019).

14 *Wendt Statement* at 00:08:07 – 00:08:26.

15 Report on Robocalls: A Report of the Consumer and Governmental Affairs Bureau, Consumer and Governmental Affairs, ¶ 21 (Feb. 14, 2019), https://docs.fcc.gov/public/attachments/DOC-356196A1.pdf.

16 ATIS SHAKEN FAQ, at 7, https://www.atis.org/01_strat_init/dlt/docs/shaken-faq.pdf ("*SHAKEN FAQ*").

17 ATIS Standard on Signature-based Handling of Asserted information using toKENs (SHAKEN), Alliance for Telecommunications Industry Solutions, Approved January, at 3, ATIS-1000074.

18 *SHAKEN FAQ* at 7.

19 Jim McEachern, *SHAKEN & Know Your Customer*, ATIS, at 3 (Oct. 2018), https://access.atis.org/apps/group_public/download.php/43134/IPNNI-2018-00129R001.pptx (emphasis in original).

on "verifying the source of the call," other separate, yet complementary, mechanisms (such as network intelligence, know-your-customer initiatives, and other call analytics) focus on the "intent of the call."[20] In short, more is needed today than STIR/SHAKEN information to enable a provider to determine whether a call should be blocked.[21]

C. The Commission Should Require Voice Providers To Cooperate with Tracebacks Initiated Through the Registered Traceback Consortium.

AT&T supports the Commission's proposal to require voice providers to cooperate with traceback requests. The Industry Traceback Group ("ITG") overseen by USTelecom—now the industry's Registered Traceback Consortium—has been an unqualified success in the fight against illegal and unwanted robocalls. Since its inception, the ITG and its members have made numerous efforts to refine and expand the traceback process through mechanization, including through an online portal that automatically generates emails to solicit traceback information as each upstream provider is identified. Today, many tracebacks are completed within a matter of hours, even with multiple providers in a call's path between the terminating provider and originating provider. In addition, recognizing early on that broad industry participation would be integral to the success of traceback efforts, the ITG has worked tirelessly to expand the membership of the group, including by proactively soliciting non-USTelecom members. ITG

---

20 *Id.* at 13.

21 *See 2019 Call Blocking Declaratory Ruling* ¶ 53. AT&T expects that technical network-related errors will be responsible for most, if not all, instances in which STIR/SHAKEN verification fails—particularly in these still early days of implementation—and not because the calling party spoofed the originating telephone number or attempted to subvert the STIR/SHAKEN process. Such "failures" are to be expected as implementation expands and providers continue to learn from the individualized carrier-to-carrier implementations. Thus, for these and potentially other reasons, a call that fails STIR/SHAKEN verification may be perfectly legitimate and, in fact, wanted by the receiving party. Similarly, a call that has been authenticated and verified under STIR/SHAKEN may be an illegal (or unwanted) call, as the example above from the July 11, 2019 Summit demonstrates. The mere fact that the call received full attestation and verification cannot demonstrate that the call is legal and wanted and thus should not be determinative of whether a provider blocks the call. Rather, providers should consider STIR/SHAKEN attestation information, together with other data points, to make a reasonable determination about blocking.

membership, which began with just three members in 2015, now stands at more than 40, and more than 250 entities have cooperated in tracebacks initiated through the ITG process.

The results of these efforts are self-evident to the law enforcement community. Indeed, the ITG has aided the efforts of investigators across levels of government. Time and again, when law enforcement targets illegal robocallers, the ITG almost inevitably supplied information key to propelling the investigation to the charging phase.[22] As the National Association of Attorneys General recently acknowledged, "the partnership between the ITG and the state attorneys general is a crucial one."[23] AT&T thus wholeheartedly supports the proposal to adopt a traceback mandate. Quite simply, given the tremendous success and effectiveness of the traceback process, coupled with the enormous burden that illegal robocalls place on consumers, businesses, and provider networks, there is no justifiable basis to refuse to fulfill a traceback request.

AT&T recommends that the Commission's rule require voice service providers to "cooperate with" traceback requests, rather than "respond to" them. In particular, a voice provider should not be permitted merely to "respond" in a way that stalls completion of the traceback. Whatever the precise language the Commission chooses, it should make clear that a voice provider is required to provide the information requested that will enable either continuation or completion of the traceback. There otherwise is no need for the Commission to granularly define the terms of traceback cooperation or response.[24] The ITG already has written

---

22 *See*, *e.g.*, Letter from Rosemary C. Harold, FCC, and Lois C. Greisman, FTC, to Jonathan Spalter, USTelecom (May 20, 2020), https://docs.fcc.gov/public/attachments/DOC-364482A2.pdf; https://www.ustelecom.org/wp-content/uploads/2019/08/State-AGs-Providers-AntiRobocall-Principles-With-Signatories.pdf.

23 Letter from Tim Fox, President, National Association of Attorneys General, to Jonathan Spalter, President & CEO, USTelecom, at 2 (May 4, 2020), https://www.naag.org/assets/redesign/files/sign-on-letter/Final%20NAAG%20Letter%20-%20USTelecom.pdf. *See also* Letter from the Honorable Ajit V. Pai, Chairman, FCC, to the Honorable Maggie Hassan, U.S. Senate, at 1 (Aug. 6, 2020), https://docs.fcc.gov/public/attachments/DOC-366160A2.pdf (noting the role of the Commission's partnership with the ITG and the FTC in "tackl[ing] the threat of COVID-19 robocall scams").

24 *See FFNPRM* ¶ 97.

policies and procedures governing the completion of tracebacks.[25] Any traceback mandate should require only that a voice provider take actions consistent with the ITG's governing policies. Significantly, the traceback mandate should not require *membership* in the ITG. To the contrary, non-ITG members routinely participate in tracebacks.

The burden associated with a wide ranging traceback mandate also should inform the Commission's decision making.[26] Accordingly, the Commission's traceback rule should be limited to responding to traceback requests from the Registered Traceback Consortium.[27] While members of the ITG have successfully streamlined the traceback process through the Registered Traceback Consortium and, in turn, adapted internal procedures to enable rapid response times to such traceback requests, the same cannot be said of traceback requests submitted directly to voice service providers. The Registered Traceback Consortium has a simple, straightforward intake process available to the Commission and law enforcement to initiate tracebacks. To the greatest extent possible, all traceback requests should route through the Registered Traceback Consortium and, at a minimum, any regulatory obligation to comply with traceback requests should be limited to the well-established ITG process.[28]

D. The Commission Should Adopt USTelecom's Robocall Mitigation Proposal as a Measure To Prevent and Mitigate Illegal Traffic.

The *FFNPRM* seeks comment on proposed rules that would require voice service providers, including intermediate and terminating providers, to "take effective steps to mitigate

---

25 USTelecom, ITG, USTelecom's Industry Traceback Group Policies and Procedures (Jan. 2020), https://www.ustelecom.org/wp-content/uploads/2020/02/USTelecom_ITG-Policies-and-Procedures_Jan-2020.pdf.

26 *See FFNPRM* ¶ 97.

27 At the same time, the Commission should take care not to prohibit tracebacks initiated by service providers based on information gleaned from their own networks and investigations.

28 The Commission therefore should strike the following language from its proposed traceback mandate: "the Commission, law enforcement, or." The subpoena process nevertheless would remain available to law enforcement.

illegal traffic" and for originating providers to take such steps "to prevent new and renewing customers" from originating illegal traffic.[29] Rather than adopt open-ended and onerous requirements that target all providers, and in an effort to advance the objectives underlying these proposals, as well as satisfy the obligations imposed under Section 4 and 7 of the TRACED Act,[30] the Commission instead should adopt USTelecom's robocall mitigation program.[31]

AT&T is particularly concerned to the extent any rule requiring "effective" steps or measures could subject voice service providers to complaints or liability in the event the steps or measures taken are not universally and completely effective. As the Commission is aware, there is no silver-bullet solution to the problem of illegal and unwanted robocalls.[32] And while AT&T and other providers have gone, and continue to go, to great lengths to protect consumers from them—investing hundreds of millions of dollars in new technologies and services, as well as making significant network upgrades to enable broad deployment of STIR/SHAKEN[33]—none of these efforts necessarily are guaranteed to be "effective" in every circumstance.

To put it another way, network limitations exist. In particular, intermediate and/or terminating often have more limited visibility that would make an *obligation* to block calls (or otherwise "mitigate bad traffic") originating from a particular source inappropriate.[34] In

---

29 *FFNPRM*, App. B (proposed 47 C.F.R. §§ 64.1200(n)(2)-(3); *see also id.* ¶¶ 98, 101.

30 Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105 §§ 4, 7 (2019) ("TRACED Act"); *see also FFNPRM* ¶ 89 (seeking comment on how "implementation of 'effective robocall mitigation programs' [could] help protect consumers from receiving unwanted unauthenticated calls").

31 *See* Letter from Farhan Chughtai, USTelecom, to Marlene Dortch, FCC, CG Docket No. 17-59, at Attachment (filed Mar. 6, 2020) ("USTelecom Mar. 6, 2020 Ex Parte").

32 *See*, *e.g.*, *FFNPRM* ¶ 102 (seeking comment on "how to define 'effective measures' … recognizing that no methods will be perfect").

33 *See* Reply Comments of AT&T, WC Docket Nos. 17-97, 20-67, at 18 (filed May 29, 2020) (explaining that implementation costs associated with STIR/SHAKEN, "including undertaking the associated upgrades to the major providers' IP networks, easily will exceed hundreds of millions of dollars," while "[r]etiring the PSTN would cost orders of magnitude more – in the billions").

34 *FFNPRM* ¶¶ 100, 98.

particular, because of the redundancies across networks, there are myriad entry points into another provider's network that are available to originating providers. Indeed, it is not unusual for a call to traverse multiple intermediate networks before reaching the terminating provider. With the exception of the provider that exchanges traffic directly with the originating provider, intermediate and terminating providers further downstream typically lack the ability to identify the originating provider for any particular call. Even in circumstances when identifying the originating provider would be feasible, a downstream provider may have limited options—i.e., blocking *all* traffic from the transit provider(s) routing the calls into the terminating provider's network—to eliminate the suspected illegal traffic.[35] The Commission should not adopt a rule that, reasonably read, would require subsequent intermediate and terminating voice service providers—providers that receive calls from an offending originating provider *indirectly*—to make a choice between potential action by the Enforcement Bureau or over-inclusive blocking with a high likelihood to impact legitimate traffic.[36]

USTelecom's robocall mitigation program offers a more appropriate framework to target the providers that—willfully or through negligence—originate substantial volumes of illegal voice traffic. At the same time, the proposal offers a less-onerous, more flexible approach, reserving the most stringent regulatory requirements (and punishments) for those persistently problematic service providers.[37] Under USTelecom's proposal, every provider would be

---

35 *See id.* ¶ 100 (recognizing that "compliance with this requirement may lead to the blocking of calls"). AT&T agrees that the language of proposed Section 64.1200(n)(2) arguably would impose a blocking obligation. *See id.*, App. B (proposed rule 47 C.F.R. § 64.1200(n)(2)).

36 To the extent the proposed rule's application would be limited to the voice service provider with immediate privity to the offending originating provider or call originator, the Commission's intention should be more clearly stated in the rule itself. In addition, based on the foregoing discussion, the Commission should distinguish between any definition of "effective measures" and the definition of "effectively mitigate" adopted in the companion *Third Report and Order*. *See Third Report and Order* ¶ 41 & App. A (adopting 47 C.F.R. § 64.1200(f)(17)).

37 USTelecom Mar. 6, 2020 Ex Parte, Attachment at 5.

required to certify, for all traffic not signed with STIR/SHAKEN,[38] that it has an appropriate robocall mitigation program designed to prevent the origination of illegal calls and has measures in place to identify if its network is being used to generate such illegal calls, and to quickly mitigate such activity once detected. The provider's certification would "confirm that it (i) takes reasonable steps to avoid originating illegal robocall traffic and (ii) that it is committed to cooperating with law enforcement and the industry traceback consortium in investigating and stopping any illegal robocallers that it learns are using its service to originate calls."[39] Because prevention is so critical to addressing the scourge of illegal robocalls, AT&T also supports appropriate modification of USTelecom's proposal so that each provider's certification (and obligations) extends to *all* traffic originating on its network, regardless of STIR/SHAKEN.

II. BLOCKED CALL LISTS ARE A USEFUL REDRESS TOOL FOR OPT-IN/OPT-OUT BLOCKING SERVICES BUT ARE IMPRACTICAL, COSTLY, AND UNNECESSARY FOR PROVIDER-INITIATED CALL BLOCKING PROGRAMS TARGETING ILLEGAL CALLS

Finally, the Commission seeks comment on its proposal "to require terminating voice service providers to provide a list of individually blocked calls that were placed to a particular number at the request of the subscriber to that number."[40] Appropriate redress mechanisms should be a critical part of any call blocking program or service. AT&T therefore supports the adoption of a blocked call list requirement tailored to consumer-facing opt-in and opt-out call blocking services.[41]

---

38 AT&T supports extending the certification requirement to *all* traffic originating on a provider's network.

39 USTelecom Mar. 6, 2020 Ex Parte, Attachment at 4. A service provider whose end users are incapable of originating large volumes of calls should be permitted to certify that it has an appropriate program because the risk that they will become part of illegal robocallers' attack vector is low. USTelecom's proposal also would establish a public database that includes all providers' certifications and would require transit service providers to confirm that their customers have such certifications on file and are in good standing." *Id.*, Attachment at 3.

40 *FFNPRM* ¶ 111.

41 *Id.* ¶ 111.

Nevertheless, the distinguishing characteristics of consumer facing opt-in or opt-out call blocking services, on the one hand, and provider-initiated call blocking programs that are not provided on an opt-out basis, on the other, warrant a separate approach for redress. While blocked call lists are made available to AT&T customers through AT&T Call Protect, AT&T Call Protect Plus, and Digital Phone Call Protect, AT&T has implemented alternative redress mechanisms for its provider-initiated call blocking program.[42] For example, as the Commission is aware,[43] when an AT&T fraud investigator blocks a telephone number placing calls to AT&T's Mobility, U-verse, Prepaid, or Cricket customers, the caller receives the following announcement: "Your access to this network is restricted. Please contact 1-888-212-6040 if you feel you have reached this recording in error." The same message repeats in Spanish. AT&T's fraud team also actively collects and investigates complaints that could indicate a blocking error and maintains a single point of contact to facilitate receipt of redress requests.[44]

But AT&T's global fraud team has no readily available mechanism to automatically generate blocked call lists for customers or, for that matter, the end-user customers of third-party providers that also benefit from AT&T's provider-initiated call blocking program. Rather, generating such lists must be compiled manually and thus would impose a significant and costly burden to the extent AT&T were required to provide blocked call lists on demand on anything but a limited basis. Moreover, any such blocked call list would be of limited (if any) utility to consumers. As the *FFNPRM* acknowledges, "no reasonable consumer would want to receive

---

42 For AT&T Call Protect and AT&T Call Protect Plus, blocked call lists are available through the companion AT&T Call Protect application. *See* https://www.att.com/features/security-apps/#FAQ5. Digital Phone Call Protect customers may access their blocked call list through the myAT&T application or online portal. *See* https://www.att.com/support/article/u-verse-voice/KM1235421/.

43 *See* AT&T Feb. 28, 2020 CGB Response at 5.

44 In addition to the toll-free telephone number, consumers and/or callers who feel their calls were blocked in error may email AT&T's global fraud team at the following address: dl-GFMOBusinessFra@att.com.

calls that are highly likely to be illegal."[45] Further, AT&T's provider-initiated call blocking program has a narrow scope—high-volume, suspected illegal calls—with an incredibly low error rate and virtually no substantiated complaints. It thus stands to reason that consumers do not want, and would have no need for, a list of suspected illegal calls that they did not receive. Finally, to the extent AT&T were required to divert resources to generate blocked call lists for its provider-initiated call blocking program, AT&T's fraud investigators would have less time to devote to investigating suspected illegal robocalls. AT&T therefore urges the Commission to limit any blocked call list requirement to opt-in and opt-out call blocking services and enable providers to leverage the existing capabilities of such services (such as the companion applications to such services) to satisfy the requirement.

CONCLUSION

AT&T welcomes the Commission's latest efforts to aggressively combat illegal robocalls. Consistent with the foregoing discussion, AT&T supports the adoption of a call blocking safe harbor for provider-initiated call blocking programs, a traceback mandate, USTelecom's robocall mitigation proposal, and a rule requiring providers of opt-in or opt-out call blocking services to offer consumers with a blocked call list.

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

August 31, 2020

[45] *FFNPRM* ¶ 105.