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

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate	)	CG Docket No. 17-59
Unlawful Robocalls	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97

COMMENTS OF INCOMPAS

INCOMPAS
Christopher L. Shipley
Attorney & Policy Advisor
1100 G Street NW
Suite 800
Washington, D.C. 20005
(202) 872-5746
cshipley@incompas.org

December 10, 2021

TABLE OF CONTENTS

Page

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
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97

COMMENTS OF INCOMPAS

INCOMPAS, by its undersigned counsel, hereby submits these comments in response to the Federal Communications Commission's ("Commission" or "FCC") *Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17-59 & Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17-97* proposing new caller ID authentication and robocall mitigation obligations on gateway providers in an effort to curb foreign-originated illegal robocalls.[1]

I. INTRODUCTION & SUMMARY

INCOMPAS, the Internet and competitive networks association, commends the Commission for taking public comment on its proposals to mitigate foreign-originated robocalls. As the Commission notes in the *Further Notice*, "[e]liminating illegal robocalls that originate abroad is one of the most vexing challenges we face"[2] and the item raises complex and important

[1] *See Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17-59 & Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17-97, FCC 21-105 (rel. Oct.1, 2021) ("*Further Notice*").

[2] *Further Notice* at para. 1.

questions on how best to resolve this issue. What is clear that is that the Commission continues to move closer to a more comprehensive approach to these issues that requires each stakeholder in the voice services ecosystem to meet the challenge of illegal robocalls and contribute to mitigation efforts. That said, as INCOMPAS discusses below, the Commission should apply call authentication and robocall mitigation obligations to voice service providers in a neutral and symmetric manner. While the item proposes several necessary changes, such as gateway providers' implementation of STIR/SHAKEN and caller ID authentication solutions, it also proposes several robocall mitigation requirements that may unnecessarily burden gateway providers that, if the order is adopted, will already be subject to the obligations imposed on intermediate providers. INCOMPAS also offers comment on some unintended consequences of its proposal to mandate gateway providers to block calls that are highly likely to be illegal.

II. MINOR REVISIONS TO THE DEFINITION OF GATEWAY PROVIDER WILL PROVIDE ADDITIONAL CLARITY FOR INDUSTRY

In the *Further Notice*, the Commission seeks to define "gateway provider" for the first time in an effort to ensure that the Commission's proposals are specifically tailored to have an effect on voice service providers that are facilitating the entry of foreign-originated illegal robocalls onto U.S. networks. The Commission proposes to define "gateway provider" as "the first U.S.-based intermediate provider in the call path of a foreign-originated call that transmits the call directly to another intermediate provider or a terminating voice service provider in the United States."[3] INCOMPAS offers that the Commission may want to consider minor revisions to its proposed definition that would further clarify which providers are serving as gateway providers. Specifically, INCOMPAS believes it may be more accurate to define "gateway

[3] *Further Notice* at para. 33.

provider" as the first intermediate provider in the call path of a foreign-originated call that receives traffic at its U.S.-based facilities before transmitting the call directly to another intermediate provider or a terminating voice service provider in the United States. In this definition, "U.S.-based" would mean "a U.S. located point of presence."

Defining "gateway provider" in this manner would address some of the questions posed by stakeholders leading up to the release of the *Further Notice* about the point in the call path at which a U.S.-based provider or its affiliates becomes a gateway provider. In a recent ex parte notice, iBasis highlighted confusion over the meaning the Commission assigns to the term "U.S.-based."[4] iBasis asks whether the definition would apply to an "intermediate provider that is physically located in the U.S. and receives traffic at a U.S. located POP" or might also include "a U.S.-licensed entity that receives traffic in the foreign country and then transmits it to another, unaffiliated entity in the United States."[5] The edit suggested by INCOMPAS clarifies that the first provider that receives a foreign-originated call at its U.S.-based facilities (with a U.S.-located point of presence) would be identified as a gateway provider and would be subject to the rules proposed in the *Further Notice*. Foreign affiliates of a U.S.-licensed provider or other U.S.-licensed entities that receive traffic in another country and transmit it to United States would not qualify under this proposed revision as gateway providers.

INCOMPAS' proposed revision has the added benefit of providing the Commission with a clear jurisdictional hook for enforcement efforts against gateway providers that transmit illegal

[4] In the *Further Notice*, the Commission specifies that "U.S.-based" means that the provider has facilities in the U.S. including a U.S. located point of presence. *Further Notice* at para. 33.

[5] *See* Ex Parte Notice of iBasis, Inc., CG Docket No. 17-59, WC Docket No. 17-97 (filed Sep. 22, 2021), at 2 (suggesting that industry would benefit from a more detailed definition of "gateway provider" given the "complexities around call routing" and providing additional examples of how affiliates may complicate the Commission's efforts to apply a definition to this category of providers).

robocalls or facilitate illegal robocall campaigns. The Commission has enforcement authority over domestic providers and, rather than attempt to adopt new requirements for U.S.-licensed affiliates operating outside the country, the definition would better clarify which U.S.-based providers would be subject to the Commission's rules.

III. GATEWAY PROVIDERS SHOULD BE SUBJECT TO SIMILAR REGULATORY TREATMENT IN THE EFFORT TO MITIGATE ROBOCALLS

In the *Further Notice*, the Commission proposes "to place additional requirements on gateway providers to ensure that they are doing their part to combat the scourge of illegal robocalls" including requiring these providers to implement caller ID authentication and robocall mitigation techniques.[6] While INCOMPAS agrees that the current rules addressing foreign-originated robocalls are "not sufficient to resolve the problem"[7] and appreciates the Commission's efforts to mitigate that threat, INCOMPAS has generally urged the Commission to apply its regulatory requirements for call authentication and robocall mitigation in a neutral and symmetric manner. As USTelecom recently demonstrated in the Commission's proceeding proposing to update its rules regarding direct access to numbers by providers of interconnected voice over Internet Protocol services, the rules that currently apply to voice service providers' efforts to mitigate robocalls are extensive.[8] INCOMPAS posits that many of the potential gaps in its robocall framework could be solved by the symmetrical application of existing requirements to gateway providers. In many cases, the *Further Notice* proposes a series of

[6] *Further Notice* at para. 23.

[7] *Id.* at para. 24.

[8] *See* Comments of USTelecom—The Broadband Association, WC Docket No. 13-97, et al. (filed Oct. 14, 2021), at 4 (describing various robocall mitigation requirements for voice service providers).

additional requirements for gateway providers. Rather than burden gateway providers with obligations the Commission has not assigned to other classes of voice service providers, INCOMPAS urges the Commission to first bring gateway providers into compliance with the current set of requirements for other intermediate providers. The Commission should also consider additional ways to more narrowly target this proceeding so that gateway providers take action to address illegal robocall campaigns as opposed to conversational or roaming traffic that is less likely to be fraudulent in nature.

Call Authentication. INCOMPAS supports the Commission's proposal to require gateway providers to authenticate caller ID information consistent with the STIR/SHAKEN framework for SIP calls that are carrying a U.S. number in the caller ID field.[9] As one of the founding members of the Secure Telephone Identity Governance Authority ("STI-GA"), the industry-led effort to support the timely deployment of the STIR/SHAKEN protocol and framework, INCOMPAS recognizes the value and importance of timely implementation of a call authentication trust anchor as part of the Commission's overall strategy to mitigate illegal robocalls. While not a silver bullet to the robocall problem, end-to-end implementation of the STIR/SHAKEN framework among voice service providers, including gateway providers, will have a significant impact in curtailing illegal robocalls which is critical to restoring consumer trust in the voice network. Broad adoption of the STIR/SHAKEN framework will arm consumers with the knowledge they need to make informed choices about which calls to accept while simultaneously equipping voice service providers with the information necessary to make

[9] *See Further Notice* at para. 38 *et seq*.

responsible and non-discriminatory call blocking decisions.[10] Additionally, as an IP-based solution, cross industry adoption of the STIR/SHAKEN ecosystem may have additional benefits, such as advancing the cause of IP interconnection. The Commission ably highlights this gap in its current regulatory framework and INCOMPAS concurs with the Further Notice that "[r]equiring gateway providers to authenticate caller ID information for all unauthenticated foreign-originated SIP calls will offer information to the downstream providers regarding where a foreign-originated robocall entered the call path, facilitating analytics and promoting traceback efforts."[11] Gateway providers should be encouraged to comply with the call authentication requirements within 18 months, in accordance with the Commission's proposal.[12]

Robocall Mitigation. While the Commission appropriately seizes the opportunity to bring gateway providers into compliance with other voice service providers with respect to call authentication and STIR/SHAKEN implementation, the Commission proposes a number of robocall mitigation requirements that "go beyond those that currently apply to voice service providers" without a clear explanation for why that might be necessary.[13] First, the Commission proposes to require gateway providers to implement STIR/SHAKEN *and* "an appropriate robocall mitigation program" despite the fact that the Commission's rules require other voice

[10] *See Advanced Methods to Target and Eliminate Unlawful Robocalls Calls*, CG Docket 17-59, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking, FCC 20-96 (rel. July 17, 2020) (establishing a caller ID authentication requirement for terminating voice service providers that seek to avail themselves of a safe harbor for the unintended or inadvertent blocking of unwanted calls based on the use of reasonable analytics).

[11] *Further Notice* at para. 40.

[12] *See Further Notice* at para. 48.

[13] *Id.* at para. 51

service providers to either implement the framework or implement a mitigation program in the portions of their network on which they have not implemented STIR/SHAKEN. It is unclear why a gateway provider would need to implement a robocall mitigation plan for the portions of its network in which it has implemented STIR/SHAKEN—a caller ID authentication tool designed to alert call recipients to spoofed or potentially fraudulent calls and to better enable tracebacks. Permitting gateway providers to either implement STIR/SHAKEN or a robocall mitigation plan in the portions of their network where they have not implemented the framework should be sufficient to significantly an increase in gateway providers' mitigation efforts and would mirror the obligations of other providers in the call path.

Second, the Commission proposes an enhanced obligation that would require gateway providers to respond fully to all traceback requests from the Commission, civil or criminal law enforcement, and the industry traceback consortium within 24 hours of receiving such a request.[14] The Commission and industry traceback consortium have already implemented a standard requiring voice service providers to respond to tracebacks "in a timely manner" and the Commission presents no evidence that a shorter timeframe will significantly increase the efficacy of those efforts other than to suggest that "time is of the essence in all tracebacks, but particularly for foreign-originated calls."[15] While INCOMPAS defers to the industry traceback group on the appropriate response time for traceback requests, INCOMPAS recommends that the Commission abandon this proposal absent some evidence that gateway providers have not responded to

[14] *See id.* at para. 52.

[15] *Id*.

traceback requests in a timely manner or that the response time has hindered a Commission or law enforcement investigation.

Know Your Customer Requirements. To the extent that the Commission seeks to adopt new "know your customer" requirements for gateway providers, INCOMPAS recommends that they be reasonable and take into consideration that these providers generally do not have a direct relationship with the call originator. As the Commission and others in the record have acknowledged, gateway providers are, in most circumstances, several steps removed from originating providers,[16] and the Commission must provide guidance on how gateway providers should apply such a rule. It is far more likely that gateway providers will see the upstream providers, including foreign intermediate carriers, as their customers as opposed to call originators.

IV. MANDATORY CALL BLOCKING REQUIREMENTS WILL IMPACT LEGAL TRAFFIC AND INCREASE THE RISK OF LIBILITY FOR DOWNSTREAM PROVIDERS

In addition to new STIR/SHAKEN and robocall mitigation requirements, the Commission proposes to require gateway providers to block foreign-originated calls that are "highly likely" to be illegal based on reasonable analytics with the intention of preventing these calls from entering U.S. networks.[17] INCOMPAS has previously expressed its reservations

[16] *See* Comments of the Alliance for Telecommunications Industry Solutions, CG Docket No. 17-59, WC Docket No. 17-97 (filed Dec. 6, 2021), at 6-7 (confirming that gateway providers "in many cases, do not have a direct relationship with the originator, making it significantly more difficult to obtain 'know your customer' information").

[17] *See Further Notice* at para. 66.

about the unintended consequences that may flow from wide-spread call blocking behaviors,[18] as well as call blocking using reasonable analytics that does not incorporate caller ID authentication information (where available) or that is not applied in a non-discriminatory and competitively neutral manner. The exceptional complexity of communications traffic exchange on the Public Switched Telephone Network (PSTN) ecosystem is often underappreciated and misunderstood. For example, our members are increasingly tasked with addressing instances of call blocking and false positives in their networks, a situation that could be compounded by implementation delays of SIP Response Code 607 and 608—the call blocking notification codes adopted by the FCC in 2020 to provide voice service providers with the necessary information to seek redress from downstream providers that either inappropriately or inadvertently block legal traffic.[19]

Furthermore, providers have very recently begun confronting the complex challenge of how to appropriately block traffic from voice service providers that are not listed in the Commission's Robocall Mitigation Database ("RMD").[20] Among other challenges, this new obligation requires providers at the outset to make subjective legal and operational determinations distinguishing voice service providers from intermediate providers from end users and then implement those subjective determinations into process and procedure to manage

[18] *See, e.g.*, Comments of INCOMPAS, CG Docket No. 17-59 (filed Aug. 21, 2020), at 6, 10-12 (discussing how call blocking could undue progress the Commission has made with respect to rural call completion).

[19] Petition for Reconsideration and Request for Clarification of USTelecom – The Broadband Association, CG Docket No. 17-59 (filed May 6, 2021); Request of USTelecom – The Broadband Association for Emergency Stay or Waiver in the Alternative, CG Docket No. 17-59 (filed Oct. 26, 2021).

[20] *See* News Release, FCC, FCC Announces That Calls From Providers Not Listed In Robocall Mitigation Database Must Now Be Blocked From Domestic Phone Networks (Sep. 28, 2021), *available at* https://docs.fcc.gov/public/attachments/DOC-376119A1.pdf.

customer accounts and their traffic in largely manual ways because of the limited automated functionality of the RMD itself.

In the instant proceeding, the Commission has incorporated four additional requirements for gateway providers with respect to call blocking. INCOMPAS is encouraged to see caller ID authentication information and competitive neutrality addressed included in these requirements. INCOMPAS similarly supports the requirements that providers manage call blocking with human oversight and network monitoring sufficient to ensure that it blocks only calls that are highly likely to be illegal and that they cease blocking calls once the provider has actual knowledge that the blocked calls are likely lawful.

To this point, the Commission has permitted voice service providers to block calls on a permissive basis using reasonable analytics that incorporate caller ID authentications solutions. Providers that do so, or conduct call blocking at the network level are protected by a safe harbor assuming they comply with Commission's call blocking requirements. However, it should be noted that the new call blocking regime established by the Commission has created unintended consequences that must be weighed as the Commission considers new blocking mandates for gateway providers. Earlier this year, a case was filed in U.S. District Court in which intermediate carriers in a call path, with no direct relationship or knowledge of robocall campaigns, have had legal action brought against them by plaintiffs contending that those carriers had an obligation under the Telephone Consumer Protection Act ("TCPA") to block certain calls. The case has raised specific questions about the circumstances under which an intermediate carrier's transmission of calls originating from non-standard telephone numbers

constitutes a violation of the TCPA.[21] This case, which represents a situation in which an invalid and unwanted call is delivered in the intermediate part of the call, raises serious liability concerns that could arise for gateway providers if the Commission adopts additional call blocking proposals but does not include a safe harbor for blocking errors—which may include both mistaken "over-blocking as well as mistaken "under-blocking" by providers in any given call stream. An explicit safe harbor in these circumstances, like those that have been adopted for using call analytics, will provide appropriate liability protection for downstream intermediate and gateway providers that have reasonably appropriate process and procedures in place to comply with the Commission's call blocking mandates, but yet cannot be expected to be able to execute any such blocking to perfection in all instances. Recognition of the inherently complex and often imperfect nature of the interconnected ecosystem in the context of Commission call blocking mandates is a necessary and appropriate component to the Commission proposed rules in this proceeding.

Additionally, carriers are experiencing instances where its corporate customers experience wide blocking of lawfully placed calls using automatic dialers because certain characteristics are similar to those used by call analytics software (whose authors are not under the Commission's jurisdiction). As an example, banking institutions place numerous calls for fraud alerts and debt collection that may look like unlawful robocalls to a software program, but not only are they legal, they are explicitly consented to by the called party in its contract with the

[21] *See* Diana Mey, *et al.* v. All Access Telecom, *et al.*, No.: 5:19-CV-00237-JPB (N.D. W.Va. filed Apr. 23, 2021). In September, Bandwidth Inc., which was named as one of defendants in the case, had its Motion for Primary Jurisdiction Referral denied. That motion would have referred key policy questions to the Commission and asked whether an intermediate carrier can be held liable for transmitting traffic originating from non-standard telephone numbers.

banking institution. This blocking is occurring even when those calls have earned an "A" attestation level. Despite the FCC's "safe harbor" requirement that any carrier blocking calls in this manner must have a robust redress process to handle the inaccurate blocking of legitimate calls, companies report that even when they get a block lifted on an outgoing telephone number, the same number is blocked again within a day or two. Until the inadequacy of such redress processes is addressed and the call blocking software industry has matured to accommodate such nuances, the FCC should not mandate any additional call blocking requirements.

V. APPLYING CALL AUTHENTICATION AND ROBOCALL MITIGATION OBLIGATIONS TO GATEWAY PROVIDERS OBVIATES THE NEED FOR THE FOREIGN SERVICE PROVIDER PROHIBITION

In addition to the proposed requirements for gateway providers, the Commission seeks comment on alternative approaches to stop illegal foreign-originated robocalls and on the status of the foreign provider prohibition. This requirement in Section 64.6305(c) prohibits U.S. intermediate and terminating voice service providers from accepting calls from foreign voice service providers that use NANP numbers, if that voice service provider has not registered in the RMD.[22] In supporting two Petitions for Reconsideration of this provision, INCOMPAS raised several concerns about the difficulties associated with educating and registering foreign providers in a U.S. database, jurisdictional uncertainties that might subject foreign voice service providers to U.S. tax or enforcement authority, and reconciling international privacy and data protection requirements with participation in the RMD.[23]

[22] 47 C.F.R § 64.6305(c).

[23] *See* Joint Reply Comments of INCOMPAS and the Cloud Communications Alliance, WC Docket No. 17-97 (filed Feb 8, 2020), at 4.

Given the potential scope of the new requirements on gateway providers, including application of caller ID authentication implementation and robocall mitigation provisions intended for intermediate providers, the Commission should be confident that these measures will be effective in stopping illegal robocall traffic from entering the U.S. market. These new requirements alone would appear to obviate the need for the foreign provider prohibition or for foreign providers to register in the Commission's RMD. As such, INCOMPAS urges the Commission to eliminate the foreign provider prohibition from its rules.

VI. COMMISSION OUTREACH IS NECESSARY TO ADDRESS FOREIGN-ORIGINATED ROBOCALLS

Finally, INCOMPAS urges the Commission to conduct additional outreach to its foreign counterparts, both independently and in conjunction with the U.S. Department of Justice, as a supplemental approach to the challenge of ending foreign-originated illegal robocalls. Particularly given the proliferation of foreign call centers that originate illicit robocalls to U.S. destinations and the restrictions inherent to U.S. voice service providers to effectuate the establishment of enforcement policies and policy changes in other countries, INCOMPAS implores the Commission to engage with foreign governmental agencies and encourage them to do more to combat the origination of illegal robocalls that reach U.S. networks.[24] The value of collaboration among U.S. agencies and their foreign counterparts in the fight against illegal robocalls is well-

[24] *See* Nigel Chiwaya, *Pandemic lockdowns have curbed robocalls. The telecom industry is trying to keep them from coming back.*, NBCNEWS (June 7, 2021, 12:44 PM), https://www.nbcnews.com/news/us-news/pandemic-lockdowns-have-curbed-robocalls-telecom-industry-trying-keep-them-n1269831 ("India, along with Pakistan and the Dominican Republic, are among the main origin points for illegal robocalls involving Social Security, debt collection and bogus utilities, said Josh Bercu, vice president of policy and advocacy at USTelecom, the association that organizes the industry's robocall tracing efforts. 'Those types of pure fraud almost always are coming from overseas,' Bercu said.")

established, and an increase in such efforts would both contribute to the elimination of sources for such illegal robocalls and the ability of U.S.-based providers to shift some of their focus to other originators of illegal robocalls that would tend to be more within their control.[25] While INCOMPAS members are confident that some of the proposals in the item will have a positive impact on the problem, it is also important for the Commission to encourage the further implementation of caller ID authentication solutions like STIR/SHAKEN and to work with other countries to significantly expand enforcement efforts.

VII. CONCLUSION

For the reasons stated herein, INCOMPAS urges the Commission to consider the recommendations in its comments as it examines the issues raised in the *Further Notice*.

Respectfully submitted,

INCOMPAS

/s/ Christopher L. Shipley

Christopher L. Shipley
INCOMPAS
1100 G Street NW
Suite 800
Washington, D.C. 20005
(202) 872-5746

December 10, 2021

[25] *See, e.g.,* News Release, U.S. Dep't. of Justice, Owner and Operator of India-Based Call Centers Sentenced to Prison for Scamming U.S. Victims out of Millions of Dollars (Nov. 30, 2020), *available at* https://www.justice.gov/opa/pr/owner-and-operator-india-based-call-centers-sentenced-prison-scamming-us-victims-out-millions (explaining how an investigation conducted by the U.S. Immigration and Customs Enforcement's Homeland Security Investigations, Treasury Inspector General for Tax Administration, and Department of Homeland Security Office of Inspector General led to the indictment of a call center owner and operator as well as 60 conspirators).