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

August 17, 2022

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 submits these comments in response to the Federal Communications Commission's ("Commission") *Seventh Further Notice of Proposed Rulemaking* in CG Docket No. 17-59 and *Fifth Further Notice of Proposed Rulemaking* in WC Docket No. 17-97 on expanding and clarifying call authentication and robocall mitigation requirements to cover other providers in the call path in order to protect American consumers from illegal robocalls.[1]

I. INTRODUCTION & SUMMARY

INCOMPAS, the Internet and competitive networks association, appreciates the opportunity to submit comments in response to the Commission's further efforts to curb the threat of illegal robocalls. Our members represent a variety of different voice service models, including traditional CLECs and VoIP providers, that serve residential and enterprise customers. These providers are committed to mitigating the threat of illegal robocalls to their customers while working with the Commission to help identify ways to preserve competition and

[1] *Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, Sixth Report and Order in CG Docket No. 17-59, Fifth Report and Order in WC Docket No. 17-97, Order, Seventh Further Notice of Proposed Rulemaking in CG Docket No. 17-59, and Fifth Further Notice of Proposed Rulemaking in WC Docket No. 17-97, FCC 22-37 (rel. May 20, 2022) ("*Gateway Provider Order*" and "*Further Notice"*).

innovation in the market. The *Further Notice* raises a number of complex and important questions on several outstanding issues in call authentication and robocall mitigation and INCOMPAS offers these comments in order to assist the Commission in closing notable gaps in the current regulatory framework.

The proposals that the Commission seeks comment on in the *Further Notice* wrestle with some of the most important topics to INCOMPAS members as they address issues related to what the association refers to as "the wholesale gap." Competitive providers often fill a number of roles in the call path—serving at times as an originating, intermediate, gateway, underlying, reseller or terminating provider—and despite the Commission's best efforts, questions remain about the obligations providers have under the agency's current rules. Over the past year, INCOMPAS has met with the Commission to better understand these obligations, including the STIR/SHAKEN implementation and Robocall Mitigation Database ("RMD") registration requirements and has worked within the STI-GA to address ongoing issues related to driving further implementation of the STIR/SHAKEN call authentication framework, such as token access and third party authentication. Since our providers face many of these issues, or work with enterprise customers or other providers that will require further accommodation in order to provide voice service, it is critical that the Commission close these gaps in order to give affected providers more regulatory certainty.

At the same time that it might be necessary to issue new rules to fill regulatory gaps in the Commission's robocall mitigation framework, INCOMPAS urges the Commission not to create, extend, or clarify obligations without conducting a thorough assessment of the impact its existing requirements are having on illegal robocalls and providers. The Commission has

adopted extensive new rules in its efforts to address these issues in recent years,[2] and INCOMPAS urges the Commission to pause and consider which rules (including those scheduled to go into effect) are conclusively having the intended effect of mitigating illegal robocalls. New rules should definitively fill the aforementioned regulatory gaps, should not put any unnecessary restrictions on providers that impacts their ability to innovate and compete, and must not overburden competitive voice service providers who do not always have the same resources and personnel at their disposal to address these issues as larger providers.

In this comment, INCOMPAS supports the Commission's proposal to require intermediate providers to adopt call authentication requirements, but presents challenges that might reduce the efficacy of such a requirement given the lack of IP interconnection across the networks. Additionally, we urge the Commission to make targeted enhancements to its existing affirmative obligations for providers and argue that an extension of the General Mitigation standard and RMD filing requirement is warranted as long as the Commission maintains a flexible and non-discriminatory approach to these provisions. Next, INCOMPAS urges the Commission to provide further clarity regarding STIR/SHAKEN implementation and RMD filing requirements given ongoing confusion over the obligations of providers that lack control of the necessary infrastructure to implement the call authentication framework. Finally, INCOMPAS recommends, given the success providers have had with such arrangements, that the Commission allow third parties to authenticate caller ID information to satisfy an originating provider's obligation.

[2] *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).

II. THE COMMISSION'S EXTENSION OF CALL AUTHENTICATION REQUIREMENTS TO INTERMEDIATE PROVIDERS MUST INCLUDE A CONCOMITANT EFFORT TO RESOLVE IP INTERCONNECTION

Having taken the step to extend caller ID authentication requirements to gateway providers in the *Gateway Provider Order*, the Commission now seeks comment on whether to require domestic intermediate providers to authenticate caller ID information consistent with the STIR/SHAKEN framework for SIP calls. As the Commission highlights in the *Notice*, INCOMPAS has previously argued that end-to end implementation of the STIR/SHAKEN framework among voice service providers will have a "significant impact in curtailing illegal robocalls" which is critical to restoring consumer trust in the voice network.[3] As one of the founding members of the Secure Telephone Identity Governance Authority ("STI-GA"), the industry-led effort to support the development 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. INCOMPAS posits that broad adoption of the STIR/SHAKEN framework will provide 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 responsible and non-discriminatory call blocking decisions.[4] As such, INCOMPAS supports the Commission's proposals to extend its authentication requirement to domestic intermediate providers. INCOMPAS agrees with the Commission that "intermediate providers

[3] See Comments of INCOMPAS, CG Docket No. 17-59, WC Docket No. 17-97 (filed Dec. 10, 2021), at 7 ("INCOMPAS Comments").

[4] *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).

could play a crucial role in further promoting effective, network-wide caller ID authentication"[5] and urges the Commission to require these providers to exchange traffic using the STIR/SHAKEN framework and to authenticate unauthenticated calls they receive.

While INCOMPAS has encouraged end-to-end implementation of the STIR/SHAKEN framework, the Commission should be aware of several challenges that must be addressed in order to make intermediate provider implementation of the framework effective. In our previous filings, INCOMPAS has indicated that cross industry adoption of the STIR/SHAKEN framework, as an IP-based solution, may help advance the cause of IP interconnection.[6] In fact, the issue of IP interconnection will ultimately determine how successful the Commission's efforts to adopt an industry-wide call authentication trust anchor will be. Many competitive voice service providers continue to face obstacles in reaching IP interconnection agreements with industry partners and, as a result, INCOMPAS has joined an industry effort to identify and propose solutions to this existential problem.[7] Until industry settles on readily available

[5] *Further Notice* at para. 163.

[6] INCOMPAS Comments at 8. *See also* Comments of Twilio, Inc., CG Docket 17-59, WC Docket No. 17-97 (filed Dec. 10, 2021), at 4 (arguing that the full benefits of the STIR/SHAKEN authentication framework can only be realized if all providers interconnect on an IP-to-IP basis); Comments of NTCA—The Rural Broadband Association, WC Docket Nos. 17-97, 20-68 (filed Nov. 26, 2021), at 5 (asking the Commission to address the IP interconnection barrier "that will frustrate other STIR/SHAKEN implementations for those small operators that would prefer to evolve to IP-based solutions rather than continuing TDM exchange of calls").

[7] *See* CALL AUTHENTICATION TRUST ANCHOR WORKING GROUP, NORTH AMERICAN NUMBERING COUNCIL, FCC, DEPLOYMENT OF STIR/SHAKEN BY SMALL VOICE SERVICE PROVIDERS (2021), *available at* https://nanc-chair.org/docs/October_13_2021_CATA_Working_Group_Report_to_NANC.pdf (recommending that the Commission permit industry to develop and propose a solution to the SIP interconnection problem within 6-12 months of the date of the report).

solutions to long-standing IP interconnection hurdles or the Commission adopts interconnection requirements, the effectiveness of the STIR/SHAKEN framework will be muted.

This is primarily because of how metadata can be lost as calls transfer between IP and TDM networks and how analytics engines may, as a result, label and block calls. For example, an originating provider may sign a call with an "A" attestation, but due to a TDM interconnection in the call path, this SHAKEN metadata is lost and an intermediate or terminating provider may be required to give that call a "B" or "C" attestation. The call now lacks the necessary metadata and metrics used by voice service providers and their analytics engines to ensure that the call is appropriately labeled. Requiring intermediate providers to sign calls with a "B" of "C" attestation may, as a result, have a significant impact on call completion rates and could increase the probability that a valid call is blocked by another downstream or terminating provider. While INCOMPAS believes that calls signed with a "B" or "C" attestation do offer service providers and consumers valuable information, flooding the ecosystem with "B" and "C" level calls hurts the value proposition that STIR/SHAKEN is intended to provide. To that end, the Commission should put an equal focus on securing commitments from voice service providers for IP interconnection for the purpose of achieving end-to-end caller ID authentication while extending call authentication requirements to domestic intermediate providers.

Additionally, if the Commission adopts a STIR/SHAKEN requirement, it should give intermediate providers no less than 12 months to comply. The six month deadline currently under consideration by the Commission would impose unnecessary burdens on the personnel and resources of intermediate providers and a longer timeframe would more closely match the deadlines offered to other voice service providers that have been required to adopt the STIR/SHAKEN framework.

III. THE COMMISSION SHOULD BE SELECTIVE IN EXTENDING CERTAIN MITIGATION DUTIES TO ALL DOMESTIC PROVIDERS

In addition to its caller ID information authentication requirements, the Commission proposes to extend a number of current obligations to domestic providers in the call path. INCOMPAS has previously advocated for the Commission to apply call authentication and robocall mitigation obligations to voice service providers in a neutral and symmetric manner, but urges the Commission to make only targeted changes to its' current rules as discussed below.

a. Enhancements to the Existing Affirmative Obligations for All Domestic Providers Should Be Limited and Targeted

24-Hour Traceback Requirement. Leading up to the *Gateway Provider Order*, INCOMPAS argued that 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 a request may be unnecessary given that the existing rule already required all domestic voice service providers to respond to traceback requests "fully and in a timely manner."[8] The Commission clearly felt it necessary to "act aggressively in the international calling context"[9] in adopting its 24-hour traceback requirement for gateway providers given the high volume of illegal robocall campaigns that originate from outside the United States.

While INCOMPAS does not oppose the Commission's proposal to apply a similar traceback compliance deadline to domestic voices service providers, it should be noted that the Commission openly acknowledges that, under the current rule "many, if not most, providers that

[8] 47 CFR § 64.1200(n)(1).

[9] *See Gateway Provider Order* at para. 67.

receive traceback requests already respond in under 24 hours."[10] This is evidence of a rule that works under its current construction and that offers smaller providers and those that may be less familiar with the process the flexibility to alert the Commission and Industry Traceback Group if it cannot complete a traceback request within 24 hours. In adopting a shorter timeframe, INCOMPAS urges the Commission to make accommodations, where possible, for responsive providers that may not be able to complete an investigation within 24 hours.

INCOMPAS members do, however, have concerns over instituting a response time associated with the volume of traceback requests received. For a variety of reasons, the number of tracebacks a service provider receives may not necessarily be an accurate indicator of the relative amount of fraud on a provider's network. Smaller providers that operate notification services and are predominately good actors in the calling ecosystem might receive a high volume of traceback requests while truly bad actors could still slip through the Commission's proposed tier structure. Therefore, INCOMPAS recommends that the Commission abandon proposals to institute a response time associated with the volume of traceback requests a voice service provider receives.

Blocking Following Commission Notification and Downstream Provider Blocking. The Commission also seeks comment on extending its effective mitigation rule by requiring all domestic providers in the call path to block illegal robocall campaigns when notified of such calls by the agency.[11] This would mark a significant shift from the current policy which allows voice service providers to "effectively mitigate the traffic" and requires intermediate providers to notify the Commission if the source comes from an upstream partner. Although INCOMPAS

[10] *Id*.

[11] *Further Notice* at para. 181.

understands the Commission's interest in extending the rule, particularly given its recent decision to require gateway providers to block illegal robocall campaigns following agency notification, our members continue to believe that the ability to investigate and mitigate threats on their network is preferable to a more prescriptive blocking approach.

While intermediate and terminating providers have been successful in investigating illegal robocall campaigns and taking mitigation steps to remove those calls before they can be completed, call blocking in these circumstances would be extremely difficult to implement. For intermediate and terminating providers in particular, blocking illegal robocall campaigns would require extensive information about the kind of traffic that would need to be blocked. Our members would prefer to first work with upstream and originating providers to properly mitigate the problematic calls before cutting off traffic from entire providers.

Additionally, INCOMPAS has repeatedly raised concerns that call blocking could be used to erect barriers to competition and discriminate against competitive providers and their legitimate use cases.[12] The association remains concerned that a rapid expansion of call blocking rules could have a detrimental impact to the intrinsic value of the broader global communications ecosystem that supports legitimate calls. Without effective notification mechanisms in place, callers and their providers may have limited ways in which to seek redress for blocked calls.[13] In

[12] *See, e.g.*, Comments of INCOMPAS, CG Docket No. 17-59, WC Docket No. 17-97 (filed Apr. 30, 2021).

[13] INCOMPAS suggests that the Commission work with standards-making bodies to complete the standardization process for SIP Codes 607 and 608, and take steps to ensure that temporary substitutes, like 603+, include the critical features and functions to meet calling parties' requirements for immediate call blocking notification and redress for analytics-based blocking and that the standard be subject to testing to ensure it is effective. *Accord* Joint Ex Parte Presentation of Voice on the Net Coalition, Cloud Communications Alliance, and INCOMPAS, CG Docket No. 17-59 (filed June 30, 2022), at 1.

instances in which the Commission is notifying providers of illegal robocall campaigns, INCOMPAS urges the Commission not to expand the effective notification rule to include blocking.

However, INCOMPAS does support the Commission's proposal to require intermediate and terminating providers to block traffic, to the extent possible, from bad-actor providers that the Commission has identified as having failed to take the appropriate steps to mitigate illegal robocall campaigns on their own networks. INCOMPAS recognizes the need to hold bad-actor providers accountable for originating or perpetuating illegal traffic, and a single, uniform rule across all provider types is preferable as it will close loopholes and give greater assurances that all providers will engage in robocall mitigation efforts. Our members acted quickly in response to the Commission's most recent attempt to hold accountable bad-actor providers that were initiating illegal, automobile warranty robocall campaigns on their networks by either terminating their customer relationship with these providers or by blocking their traffic where it could be identified.[14] In these situations, INCOMPAS urges the Commission to provide intermediate and terminating providers with sufficiently detailed information to block calls from bad-actor providers, given that many do not have a direct relationship with the originating provider.

Effective Measures to Prevent New and Renewing Customers from Originating Illegal Calls. INCOMPAS maintains that the most effective way to ensure that providers are taking affirmative, effective measures to prevent new and renewing customers from using their network to originate illegal calls is to maintain the flexible approach adopted in the *Fourth Call Blocking*

[14] *See FCC Enforcement Bureau Warns All U.S.-Based Voice Service Providers To Avoid Or Cease Carriage Of Auto Warranty Robocall Traffic From Cox/Jones/Sumco Panama Operation*, File No. EB-TCD-21-00031913, Order, DA 22-784 (rel. July 21, 2022).

Order.[15] Originating providers remain in the best position to know whether robocall campaigns are legitimate or fraudulent. Automating fraud analysis and mitigation allows for illegal robocall campaigns and bad actors to be blocked early and quickly, and any prescribed approach would not offer providers the flexibility required to effectively monitor non-conversational traffic for various legitimate use cases. As part of their robocall mitigation plan, originating providers should provide with some particularity a list of the measures taken and information collected to ensure that new and renewing customers will not originate illegal robocall campaigns on their networks. Should the Commission adopt due diligence requirements for intermediate providers, INCOMPAS recommends that the Commission follow the approach it took in the *Gateway Provider Order* and adopt a "Know Your Upstream Provider" requirement. Like gateway providers, intermediate providers are unlikely to know direct information about the originating caller, but likely have in place commercial agreements with upstream providers that includes assurances that this provider will not originate illegal robocalls.

If domestic providers take reasonable and effective measures to stop the origination of illegal robocalls, then INCOMPAS urges the Commission to reject proposals to adopt strict liability standards if a customer uses an originating provider's network to place illegal calls. Assuming that domestic providers have certified in their robocall mitigation plan that they have taken affirmative and effective measures to prevent the origination of illegal robocalls, the Commission would be better served allowing these providers to take immediate action to terminate its relationship with a bad actor customer. Despite continuing good faith efforts of domestic providers, managing global communications traffic flows are extremely complex and

[15] *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Fourth Report and Order, 35 FCC Rcd 15221, 15232-33, paras. 32-36 (2020) ("*Fourth Call Blocking Order*").

today's mitigation measures are not infallible, even while the methods of illegal robocallers continue to be extreme. To abandon a standard of reasonableness in favor of strict liability would unfairly punish providers that are attempting to be good partners in the fight against fraudulent robocalls.

Furthermore, the Commission asks whether providers should focus their robocall mitigation efforts on non-conversational traffic, which the Commission defines as "traffic that has an average call duration of less than two minutes."[16] INCOMPAS asserts that "non-conversational traffic" as it is currently defined is too subjective a standard to be relied on and therefore a focus on such calls would be inappropriate. By creating such as distinction between conversational and non-conversational traffic, the Commission may be inadvertently providing certain industry sectors with competitive advantages. Although conversational traffic is less often correlated with fraud or spam traffic, not all non-conversational traffic is fraud or spam. INCOMPAS members operate services with valid use cases for traffic the Commission's seeks to define as non-conversational, including high-volume, short duration type calls, such as appointment reminders and school notices. These services offer a variety of public benefits and the Commission should focus its attention on the measures providers are taking to mitigate the origination of illegal robocalls, rather than the form these calls take.

b. While an Extension of the General Mitigation Standard and Robocall Mitigation Database Filing Requirement Is Warranted, the Commission Should Maintain Regulatory Symmetry and Its Flexible Approach to Meeting These Requirements.

INCOMPAS supports the Commission's proposal to extend a general mitigation standard to all voice service providers that have implemented STIR/SHAKEN in the IP portion of their networks and to all intermediate providers. Our voice service provider members are uniformly

[16] *Further Notice* at para. 185.

taking "reasonable steps" in good faith to ensure that they are not originating or terminating illegal robocall campaigns and our intermediate providers have in place network management policies to ensure to the greatest degree possible they do not process or carry such traffic. Consequently, INCOMPAS does not object to the Commission's proposal to require domestic providers to file a mitigation plan detailing the steps and practices they are taking to prevent the origination of fraudulent calls along with a certification in the Robocall Mitigation Database. If the Commission adopts an extension to the General Mitigation Standard, the agency should provide 60 days for providers to comply.

However, the association urges the Commission to abandon more prescriptive rules meant to ensure that providers take "reasonable steps" to mitigate illegal calls. While providers may internally adopt traffic monitoring for upstream service or traffic monitoring metrics, INCOMPAS urges the Commission to give providers the necessary flexibility in determining which measures to use to mitigate illegal calls on their networks. Every use case is different, especially in the enterprise arena, and providers need to be able to apply the metrics that match the use cases of their customers. The Commission also asks if VoIP providers should be held to a higher burden with respect to meeting the "reasonable steps" standard. The threat of illegal robocalls is an industry issue and impacts every type of provider. INCOMPAS offers that, for regulatory symmetry, VoIP providers be held to the same standard as other providers under the Commission's rules.

Finally, INCOMPAS supports the Commission's proposals to extend to all domestic providers the obligation to certify to the status of their STIR/SHAKEN implementation and to file a robocall mitigation plan in the RMD. INCOMPAS agrees with the Commission it would be helpful for providers to "describe with particularity" their robocall mitigation techniques,

contractual requirements, and know-your-customer process in the plan, but believes that additional information requirements suggested by the Commission may be unnecessarily burdensome and are unlikely to enhance compliance.

IV. FURTHER CLARIFICATION OF THE COMMISSION'S RULES FOR PROVIDERS THAT LACK CONTROL OF THE NECESSARY INFRASTRUCTURE TO IMPLEMENT STIR/SHAKEN IS NEEDED

Despite the Commission's previous efforts to clarify that STIR/SHAKEN implementation "does not apply to providers that lack control of the network infrastructure necessary to implement" the framework,[17] INCOMPAS urges the Commission to provide further clarity regarding STIR/SHAKEN implementation and Robocall Mitigation Database filing requirements given ongoing confusion over providers' obligations. As the Commission indicates in the *Further Notice*, many providers, including resellers, have filed in the RMD "irrespective of any obligation to do so"[18] and absent a requirement to implement STIR/SHAKEN. Offering greater clarity over the subset of non-facilities-based small voice service providers that are obligated under the *Small Provider Order* to implement STIR/SHAKEN and non-facilities-based small providers that do not have control of the necessary infrastructure to implement STIR/SHAKEN will dispel some of the confusion that is occurring in the RMD.

With respect to requiring these providers to engage in robocall mitigation efforts, INCOMPAS believes providers that are otherwise unable to implement STIR/SHAKEN should be required to conduct some essential robocall mitigation tasks that will protect consumers from

---

[17] *Call Authentication Trust Anchor, Implementation of the TRACED Act Section 6(a) Knowledge of Customers by Entities with Access to Numbering Resources*, WC Docket Nos. 17-97, 20-67, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3241, 3260, paras. 40 (2020).

[18] *Further Notice* at para. 214.

illegal robocalls. First, as noted above, it is prudent for all voice service providers to develop and have on file a robocall mitigation plan that addresses illegal robocall campaigns. Whether or not these providers will be required to enter their program details in the RMD, these providers' plans should include the same detailed steps for mitigating illegal robocalls and identifying bad actors as other providers that are required to include this information in the RMD. Providers that lack control over network infrastructure also possess valuable information about their customers that an underlying provider (or a third party that signs calls on the resellers behalf) may be able to use when conducting investigations or reviewing traceback requests. INCOMPAS would support the Commission adopting a requirement on providers that lack control of network infrastructure to relay this information to its underlying provider in a timely manner.

V. THIRD PARTY CALLER ID AUTHENTICATION SHOULD BE ALLOWED TO SATISFY AN ORIGINATING PROVIDER'S STIR/SHAKEN OBLIGATION

Next, the Commission asks whether to clarify its rules to allow third parties to authenticate caller ID information on behalf of originating providers. INCOMPAS represents competitive voice service providers that operate a number of voice service models, including some that have taken on responsibility for signing calls on their customers' behalf or that work with downstream providers to sign their calls. Resellers or third parties that originate calls may not have control over their network infrastructure, the technical capabilities, or personnel to be able to implement and maintain the STIR/SHAKEN framework on their own. However, it is possible for these providers to partner with an underlying or downstream provider to meet call authentication requirements, including signing calls through the STIR/SHAKEN framework. For those that cannot maintain the framework natively, third party authentication has been a way for these providers to adequately meet the Commission's current requirements to transmit authenticated caller ID information to the next voice service provider.

As indicated in the *Further Notice*, TransNexus classified the arrangements in which a downstream provider signed calls using an originating service provider's SHAKEN certificate as "legitimate outsourcing."[19] INCOMPAS agrees with this assertion. TransNexus also highlighted that intermediate providers had signed calls for an upstream service provider using the intermediate provider's SHAKEN certificate, leading to a high number of SHAKEN implementation filings in the Robocall Mitigation Database.[20] Given the success these providers have had with these arrangements, INCOMPAS strongly urges the Commission to allow a third party to authenticate caller ID information to satisfy the originating provider's obligation. INCOMPAS also suggests that, in order to address the gap identified above by TransNexus, the Robocall Mitigation Database be modified so that either arrangement be permitted as a way to bring an originating service provider into compliance with the Commission's requirements to transmit calls with authenticated caller ID information.

VI. 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*.

[19] Comments of TransNexus Comments, WC Docket No. 17-97 (filed Nov. 12, 2021), at 3.

[20] *Id*.

Respectfully submitted,

INCOMPAS

/s/ Christopher L. Shipley

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

August 17, 2022