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

In the Matter of	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97
	)	
Implementation of TRACED Act Section 6(a) — Knowledge of Customers by Entities with Access to Numbering Resources	)	WC Docket No. 20-67

REPLY COMMENTS OF INCOMPAS

INCOMPAS, by its undersigned counsel, hereby submits these reply comments in response to the Federal Communications Commission's ("Commission" or "FCC") *Further Notice of Proposed Rulemaking*[1] seeking comment on further efforts to combat illegal spoofing and implement caller ID authentication pursuant to the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence ("TRACED") Act in 2019.[2]

I. INTRODUCTION AND SUMMARY

INCOMPAS, the Internet and competitive networks association, remains committed to Commission-led and industry-wide efforts to mitigate illegal robocalls and implement caller identification authentication. As the Commission points out, STIR/SHAKEN "is one important solution that should be part of an arsenal of effective remedies to combat robocalls" and our members are engaged in various activities, including industry traceback and standards setting,

[1] *See Call Authentication Trust Anchor, Implementation of TRACED Act Section 6(a) — Knowledge of Customers by Entities with Access to Numbering Resources*, WC Docket No. 17-97, WC Docket No. 20-67, Report and Order and Further Notice of Proposed Rulemaking, FCC 20-42 (rel. Mar. 20, 2019) ("*Report and Order*" and "*Further Notice*").

[2] Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence ("TRACED") Act, S. 151, 116th Cong. (2019).

that allows us to share vital information across the membership about ways to curb illegal calls. At the same time, INCOMPAS members aim to strike a balance between this important consumer protection goal and preserving competitive providers' ability to compete in the marketplace, develop innovative communications services, and access numbering resources.

In these reply comments, INCOMPAS urges the Commission streamline certification requirements for voice service providers that must implement a robocall mitigation program during the time a compliance extension has been granted. Additionally, we provide our perspective on the use of call analytics in such programs, and ask the Commission to ensure that robocall mitigation programs are consistent with the objectives of advancing competition and innovation in the communications marketplace and include transparency, notification, and redress requirements in order to address the issue of false positives and inadvertent call blocking. Finally, INCOMPAS highlights the record support for the certificate delegation process and implores the Commission to ensure these protocols are incorporated into the STIR/SHAKEN call authentication framework.

II. THE COMMISSION SHOULD ADOPT STREAMLINED CERTIFICATION AND NON-DISCRIMINATION REQUIREMENTS FOR ROBOCALL MITIGATION PROGRAMS

In the *Further Notice*, the Commission contemplates the application of a TRACED Act provision that would require any voice service provider that has been granted an extension of compliance to "implement an appropriate robocall mitigation program to prevent unlawful robocalls from originating on the network of the provider."[3] INCOMPAS explained in its comments that an extension of the implementation deadline for the STIR/SHAKEN framework was warranted for small voice service providers as well as those providers that are capable of

[3] TRACED Act § 4(b)(5)(C)(i).

demonstrating that the current call authentication standards may not be able to adequately accommodate differences in the type of technology that a provider is using. Accordingly, these providers would be subject to the TRACED Act's robocall mitigation requirement during the time of the extension.

In order to meet the requirement, the Commission should institute a non-prescriptive public certification process (maintained by the agency) in which, consistent with the language of the TRACED Act, a provider certifies that its robocall mitigation program prevents unlawful robocalls from originating on its network. Taking additional steps to ensure providers make details of their robocall mitigation programs available to the Commission both regularly and upon request will benefit the entire ecosystem greatly but at relatively low cost. While, USTelecom proposes to require providers to confirm that they are "committed to cooperating with law enforcement and the industry traceback consortium in investigating and stopping any illegal robocallers,", this additional confirmation is unnecessary as the industry traceback consortium is already required to publicly identify voice service providers in the Commission's Annual Robocall Report that participate or refuse to participate in private-led efforts to trace back the origin of suspected unlawful robocalls.[4] Further, the Commission itself should explicitly retain the ability to quickly ascertain which voice service providers have cooperated with the enforcement efforts of the Industry Traceback Group by seeking the current list of participating providers from USTelecom as well.

Additionally, the Commission seeks comment on allowing voice service providers to use call analytics as part of any robocall mitigation program. In the *2019 Declaratory Ruling*, the Commission determined that voice service providers might offer opt-out call-blocking programs

[4] TRACED Act § 13(b)(2)-(3).

based on "any reasonable analytics designed to identify unwanted calls" to mitigate the receipt of illegal robocalls.[5] In response to competitive concerns by stakeholders like INCOMPAS, the Commission thoughtfully included a requirement that "such analytics must be applied in a non-discriminatory, competitively neutral manner."[6] Despite the inclusion of this language, INCOMPAS remains concerned about the application of call analytics to robocall blocking programs and believes that the variety of factors and algorithmic modeling that are being employed by voice service providers has resulted in blocking legitimate traffic to communications end users.[7] Other stakeholders that have either had communications blocked or believe that "more specific parameters" for call analytics are needed to address the issue of false positives share this perspective.[8] Indeed, a number of questions persist about calls being blocked under the overly-broad umbrella of "reasonable analytics" and INCOMPAS has asked the Commission to provide additional analysis of "reasonable" call-blocking treatments in the

[5] *Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, FCC 19-51, ¶ 34 (rel. June 7, 2019) ("*2019 Declaratory Ruling*").

[6] *Id*. at ¶ 35.

[7] *See* Comments of INCOMPAS, CG Docket No, 17-59, WC Docket No, 17-97 (filed Jan. 29, 2020) at 3 ("INCOMPAS Comments") (reporting that one INCOMPAS member was alerted by a customer that was sending two-factor authentication requests to participating subscribers via voice communications channels that such notices were being blocked).

[8] *See* Comments of Twilio, WC Docket Nos. 17-97, 20-67 (filed May 15, 2020) at 8 ("Twilio Comments") (claiming that "[i]nconsistent and non-transparent analytics have resulted in noticeable mislabeling of lawful calls that are critical to public health and the well-being of consumers"); Comments of American Financial Services Association, WC Docket Nos. 17-97, 20-67 (filed May 15, 2020) at 2 (suggesting that the Commission establish algorithmic transparency and accountability requirements for labeling and blocking).

agency's upcoming report on the availability and effectiveness of call blocking tools and the impact of the Commission's actions on mitigating illegal robocalls.[9]

If the Commission requires voice service providers to include call analytics as part of any robocall mitigation program, INCOMPAS urges the Commission to first clarify, like it did in the *2019 Declaratory Ruling*, that "such analytics must be applied in a non-discriminatory, competitively neutral manner." Furthermore, the Commission must ensure that robocall mitigation programs are subject to transparency, notification, and redress requirements that will address the issue of false positives. To achieve this, the Commission should first permit and encourage information-sharing between the providers that would allow an examination of the analytical factors that are being used to identify illegal robocalls. INCOMPAS members have expressed concerns that other communications that share similar traits to two-factor authentication, like automated emergency or security-related notifications could be blocked by programs based on unknown analytical factors. Establishing a process by which providers may voluntarily share information in order to resolve instances of false positives should alleviate most concerns about the use of call analytics in robocall mitigation programs and about the potential for use cases like those mentioned above to be blocked. Instituting transparency and effective redress requirements in this instance for robocall mitigation programs would also mirror the treatment that the TRACED Act requires the Commission to take with respect to opt-out robocall blocking services offered pursuant to the *2019 Declaratory Ruling* where the agency must ensure those programs "are provided with transparency and effective redress options for both consumers and callers."[10] Additionally, an effective robocall mitigation program will include notification

[9] INCOMPAS Comments at 3.

[10] TRACED Act § 10(b)(1)(A)(i)-(ii).

requirements so that providers or end users can be alerted when a call has been blocked (for instance, through the use of cause codes) as well as a means for redress through a web portal or dedicated contact person.

Finally, INCOMPAS maintains that the Commission should exercise caution in its consideration of a broader safe harbor for blocking, labeling and trust identification decisions based on reasonable analytics. The broad use of a safe harbor for default blocking would bring significant anticompetitive risks and reduce incentives for voice service providers to improve call-blocking programs or enact effective redress procedures. Both the Commission and Congress have taken aggressive action over the last year to provide voice service providers with certainty, absent a broad safe harbor, that they can take the actions necessary to combat illegal robocalls. The Commission's *2019 Declaratory Ruling* permits call blocking programs based on *any reasonable* analytics, a decision that would seemingly obviate the need for such a broad safe harbor as it grants providers significant authority to engage in robocall mitigation. INCOMPAS urges the Commission to analyze the early results of its actions before extending liability protection via a broad safe harbor. Furthermore, the TRACED Act does not contemplate a broad safe harbor, but rather one that connects it "in whole or in part" to a call authentication framework.[11] INCOMPAS believes this legislative directive is imperative to ensuring that the STIR/SHAKEN framework is of value ultimately and not potentially entirely disregarded in favor of preferred "reasonable analytics." If the Commission were to determine that for the purposes of robocall mitigation "[a] safe harbor limited to call-blocking based solely on failed SHAKEN/STIR authentication would be too limited,"[12] or the opposite extreme that a safe

[11] TRACED Act § 4(c)(1)(B).

[12] Comments of CTIA, WC Docket Nos. 17-97, 20-67 (filed May 15, 2020) at 27.

harbor could allow for virtually unchecked call-blocking devoid of any STIR/SHAKEN considerations it could significantly decrease the fundamental efficacy of the framework including decreasing the likelihood that providers that have not already adopted the framework would do so before the TRACED Act's compliance deadline.

III. BROAD SUPPORT FOR CERTIFICATE DELEGATION DEMONSTRATES THE CLEAR VALUE OF INCORPORATING THESE PROTOCOLS INTO THE STIR/SHAKEN FRAMEWORK

The Commission's consideration of a potential extension of the call authentication compliance deadline due to undue hardship for enterprise calls produced a groundswell of support for the idea of incorporating certificate delegation protocols into the STIR/SHAKEN framework.[13] INCOMPAS members view effective delegation of certificate authority as a means to enhance the application of STIR/SHAKEN and provide their customers with an opportunity to sign calls for a wide range of use case scenarios where valid and successful service models may utilize numbers from third-parties or multiple underlying carriers. Developing protocols for certificate delegation will support consumer demands for a wide range of technologically advanced use cases, beyond enterprise calls, and provide for a more robust use of call authentication in the marketplace.[14] Despite the fact that these protocols are not yet

---

[13] *See* Comments of Cloud Communications Alliance, WC Docket Nos. 17-97, 20-67 (filed May 15, 2020) at 3 (noting that "prompt adoption of certificate delegation protocols fulfills Congress's mandate [in section 4(b)(5)(D) of the TRACED Act] that the Commission 'enable as promptly as reasonable full participation of all classes of providers of voice service and types of voice calls to receive the highest level of trust'").

[14] *See* Comments of Sorenson Communications, LLC., WC Docket Nos. 17-97, 20-67 (filed May 15, 2020) at 2 (urging the Commission to adopt delegate certificate mechanisms to ensure that STIR/SHAKEN does not interfere with telecommunications relay services); *see also* Comments of Securus Technologies, Inc., WC Docket Nos. 17-97, 20-67 (filed May 15, 2020) at 3-4 (indicating that the company, an inmate calling service provider, "faces challenges implementing the STIR/SHAKEN Framework for calls originating on its network that use a toll-free number"

finalized, certificate delegation has been embraced for its ability to "maintain end-to-end security and trust without compromise"[15] and stands as one of the surest way for third-parties or select voice service providers to achieve higher levels of attestation if they place outbound calls through providers that may not otherwise have numbering resources.[16]

Further, as discussed above, advancing the usefulness of the STIR/SHAKEN framework in a manner that better fits the realities of a complex marketplace will support more trustworthy and transparent call analytics outputs to the benefit of all consumers. Certificate delegation is a standards-based enhancement of STIR/SHAKEN that, with the right resources and support, could help cure many of the concerns raised in the record about participation in the framework and the occurrence of false positives. As noted, voice service providers continue to express their concerns that the current use of call analytics results in legitimate outbound calls being mislabeled, increasing the likelihood that these calls will be prevented from reaching consumers.[17] And while the use of call analytics in call blocking program is undoubtedly an important aspect of the Commission's efforts, an over reliance on analytics that does not take full advantage of an enhanced call authentication regime that permits certified call originators to attest to the authenticity of their traffic, will likely result in the Commission continuing to receive

---

and that certificate delegation would allow it to sign calls it would not be able to otherwise without an underlying incumbent provider).

[15] Ex Parte Letter of Beth Choroser, Vice President, Regulatory Affairs, Comcast Corporation to Marlene Dortch, Secretary, Federal Communications Commission, WC Docket Nos. 17-97, 20-67 (filed May 12, 2020) at 2.

[16] *See* Comments of BT Americas Inc., WC Docket Nos. 17-97, 20-67 (filed May 15, 2020) at 11 (remarking that BT could become interested in certificate delegation for foreign-originated calls "if a broader application of the delegation concept were contemplated that included delegating signing authority to providers").

[17] *See e.g.*, Twilio Comments at 5.

complaints about mislabeling and false positives. Indeed, call analytics and authentication go hand-in-hand and the Commission should promote and require both remedies as part of its "arsenal . . . to combat robocalls." Therefore, INCOMPAS renews its call to have the Commission incorporate a certificate delegation model into the STIR/SHAKEN framework, and urges the Commission to implement transparency, notification, and redress requirements to ensure that these remedies are working appropriately for voice service providers, their customers, and consumers.

VII. CONCLUSION

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

Respectfully submitted,

INCOMPAS

/s/ Christopher L. Shipley

Christopher L. Shipley
Attorney & Policy Advisor
INCOMPAS
2025 M Street NW
Suite 800
Washington, D.C. 20036
(202) 872-5746

May 29, 2020