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
	)	

COMMENTS OF INCOMPAS

INCOMPAS, by its undersigned counsel, hereby submits these comments in response to the Federal Communications Commission's ("Commission" or "FCC") *Fourth Further Notice of Proposed Rulemaking* seeking comment on further efforts to implement provisions of the TRACED Act, including the consideration of further safe harbors for call blocking, additional redress measures, and an affirmative obligation for voice service providers under section 201(b) of the Communications Act to manage the threat of illegal robocalls.[1]

I. INTRODUCTION & SUMMARY

With several recent decisions, including setting an industry deadline for the implementation of the STIR/SHAKEN call authentication framework,[2] the selection of a single industry traceback consortium,[3] and the adoption of safe harbors for the use of reasonable

[1] *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking, FCC 20-96 (rel. July 17, 2020) ("*Third Report and Order*" and "*Fourth Further Notice*").

[2] *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, 34 FCC Rcd 3241 (2020) ("*STIR/SHAKEN Order and FNPRM"*).

[3] *See Implementing Section 13(d) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act* (*TRACED Act*), EB Docket No. 20-22, Report and Order and

analytics and the blocking of bad-actor providers,[4] the Commission has made consistent progress towards fulfilling the statutory requirements of the TRACED Act. INCOMPAS and its members are steadfastly committed to working with the Commission on the development and implementation of illegal robocall mitigation and call authentication solutions. As the agency considers further steps to meet its obligations under the Act, INCOMPAS commends the Commission for taking a measured and considerate approach to call blocking as a form of illegal robocall mitigation and for implementing these provisions in a non-discriminatory and competitively neutral manner.

In this comment, INCOMPAS first addresses several of the remaining provisions in section 4 of the TRACED Act under consideration by the Commission. INCOMPAS encourages the Commission not to permit additional call blocking based in whole or in part on caller ID authentication information, and further urges the Commission not to extend a safe harbor over other types of call blocking using this information. Additionally, INCOMPAS urges the Commission to ensure that any new requirements for call authentication imposed on TDM or small voice service providers align with the Commission's rural call completion efforts.

Next, INCOMPAS recommends that the Commission support the development of call authentication solutions, like certificate delegation and enhanced international attestation, in order to achieve a Congressional directive under section 7 of the TRACED Act intended to protect subscribers from calls or texts using unauthenticated numbers. We also urge the Commission to reject its proposal to adopt a safe harbor for network-level blocking of calls.

Further Notice of Proposed Rulemaking, 34 FCC Rcd 3113 (Mar. 27, 2020) ("*Traceback Consortium Order"*).

[4] *Third Report and Order* at paras. 25-45.

With the Commission meeting its statutory obligation to adopt a safe harbor based, in whole or in part, on caller ID authentication information, extending a call blocking safe harbor for network-level blocking of calls that are "highly likely to be illegal" is not only unnecessary, as INCOMPAS explains, it is also inconsistent as currently proposed with the objective criteria for safe harbors that the Commission relied on in the *Third Report and Order*.[5] Finally, INCOMPAS encourages the Commission to consider new redress measures that will notify callers and voice service providers that a call has been intercepted and to require blocking providers to use reasonable means to quickly resolve call blocking disputes.

II. NEW CALL AUTHENTICATION MEASURES SHOULD BE LIMITED AND CONSISTENT WITH THE LANGUAGE OF THE TRACED ACT

As the Commission examines solutions under section 4 of the TRACED Act that would allow voice service providers to use caller ID authentication information to mitigate illegal robocalls, INCOMPAS urges the Commission to continue to take an incremental approach to call blocking, particularly since caller ID authentication information is rarely used, in whole, to identify illicit calls.

a. The Commission's Current Approach to Incorporating Caller ID Authentication Information is Appropriate

INCOMPAS members generally do not rely solely on caller ID authentication information when making a determination about whether or not to block a call that is suspected of being an illegal robocall. Our members call blocking programs are based on a combination of factors, including *inter alia* call volumes and durations, completion ratios, and neighbor spoofing patterns. Caller ID authentication information is typically incorporated by voice service

[5] *Fourth Further Notice* at para. 104.

providers into this analytic framework. When combined, these factors produce a higher likelihood that illegal robocalls will be identified.

Furthermore, call authentication frameworks, like STIR/SHAKEN were developed with the intention of providing consumers with additional information about the source of a call so that a called party could make an informed decision about whether to accept it. That voice service providers have been able to factor this information into their call blocking programs is proof that the framework holds tremendous value and will be an important tool in the fight against robocalls; however, STIR/SHAKEN remains under development and is subject to certain limitations that would make the authorization of call blocking based solely on caller ID authentication information unwise at this time. As an IP-based solution, STIR/SHAKEN will not be available to voice service providers with non-IP elements in their networks. Given the inability of some voice service providers to exchange STIR/SHAKEN identity headers, it would be premature for the Commission to permit voice service providers to block calls based on caller-ID authentication information. INCOMPAS concurs with the Commission's analysis that incorporating caller ID authentication information into the reasonable analytics a provider uses for its call blocking program is, at this time, an appropriate approach.

b. Extending a Safe Harbor for Call Blocking Based on Caller ID Authentication Information Is Unnecessary At This Time

With respect to extending a safe harbor to cover blocking based on caller ID authentication information, INCOMPAS contends that the Commission has met the statutory requirements of the TRACED Act under section 4(c)(2) by adopting a safe harbor based on reasonable analytics that requires caller ID authentication information. As such, additional safe harbors that might protect voice service providers from liability for call blocking are unnecessary

at this time, particularly, if as INCOMPAS recommends, the Commission does not authorize blocking based in whole on caller ID authentication information.

Under the Commission's *Call Blocking Declaratory Ruling*, voice service providers are given broad authority to block calls based on reasonable analytics[6] and the *Third Report and Order* now gives providers the opportunity to avail themselves of a safe harbor by including caller ID authentication information in their analytic framework. These decisions provide ample protection for voice service providers that are implementing the STIR/SHAKEN framework into their networks and are applying analytics for call blocking in a non-discriminatory, competitively neutral manner. Additionally, the nation's providers are in varying stages of implementing the STIR/SHAKEN framework, meaning that it will still be some time before caller ID authentication information will be shared between providers in a uniform and consistent manner.

If the Commission does elect to extend a safe harbor, then INCOMPAS recommends that the Commission retain sufficient authority to take action against a voice service provider that uses this liability shield to regularly block legitimate traffic or engage in anticompetitive or discriminatory behavior. INCOMPAS remains concerned about the potential for widespread blocking under a safe harbor, and urges the Commission to hold providers that abuse a safe harbor accountable if it finds, in response to a formal complaint, that the provider inappropriately blocked traffic. Voice service providers that engage in chronic abuse of the safe harbor provisions of the Commission's rules should no longer be permitted to avail themselves of the safe harbor, and would be subject to further Commission review as necessary.

---

[6] *See 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, 34 FCC Rcd 4876, 4898-4902, paras. 71-82 (2019) (*Call Blocking Declaratory Ruling and Further Notice*).

c. The Commission Should Align Rural Call Completion and Call Authentication Requirements for Voice Service Providers Subject To a Compliance Delay

The Commission tentatively concludes in the *Fourth Further Notice* that voice service providers that are subject to a delay in compliance with the call authentications requirements of the TRACED Act will not be blocked because the Commission will not permit blocking based solely on caller ID authentication information.[7] The Commission has proposed granting extensions of the STIR/SHAKEN implementation deadline provisions of the TRACED Act to voice service providers that operate TDM networks as well as small voice service providers with under 100,000 subscriber lines.[8] Several INCOMPAS members work with rural carriers that continue to have significant TDM elements in their networks on media conversion of calls from IP to TDM (and vice versa) before hand off. Our members indicate that the Commission's recent actions with respect to rural call completion and the implementation of the Improving Rural Call Quality and Reliability Act of 2017[9] have alleviated many of the previous concerns related to this issue. Given the strides made in resolving this longstanding issue, INCOMPAS urges the Commission to ensure that any new requirements for call authentication imposed on TDM or small voice service providers do not interrupt the progress that has been made with respect to rural call completion. Permitting these providers to be blocked based on caller ID authentication information would undo this progress and the Commission should give additional consideration to this concern.

---

[7] *Fourth Further Notice* at para. 86.

[8] *STIR/SHAKEN Order and FNPRM* at paras. 76-79.

[9] Improving Rural Call Quality and Reliability Act of 2017, Pub. L. No. 115-129, 132 Stat 329 (2018) (RCC Act).

III. ADDITIONAL CALL AUTHENTICATION SOLUTIONS, LIKE CERTIFICATE DELEGATION, AND ENHANCED INTERNATIONAL ATTESTATION, WILL PROTECT CONSUMERS FROM RECEIVING UNWANTED CALLS.

In section 7 of the TRACED Act, Congress directs the Commission to initiate a rulemaking and to take additional steps "to help protect a subscriber from receiving unwanted calls or text messages from a caller using an unauthenticated number."[10] INCOMPAS posits that the Commission can achieve this directive by providing more avenues for unauthenticated calls to receive the appropriate attestation at their origination or gateway entry point. Competitive voice service providers are actively working to develop call authentication solutions, like certificate delegation and enhanced international attestation, that would solve for use cases that are not currently contemplated by the STIR/SHAKEN model. Commission support for these measures will ensure that STIR/SHAKEN takes into consideration a wider range of calls (such as wholesale, enterprise, or international calls) and that the calls consumers receive are authenticated.

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.[11] Despite the fact that these protocols are not yet finalized,

[10] TRACED Act at § 7(a).

[11] *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

certificate delegation has been embraced by industry for its ability to "maintain end-to-end security and trust without compromise"[12] and stands as one of the surest way for third-parties or select voice service providers to achieve authentication and higher levels of attestation if they place outbound calls through providers that may not otherwise have numbering resources.[13]

Further, 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.[14] And while the use of call analytics in call blocking programs 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

---

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

[12] 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.

[13] *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").

[14] *See* Comments of Twilio, WC Docket Nos. 17-97, 20-67 (filed May 15, 2020) at 5 ("Twilio Comments")

authentication regime that permits certified call originators to attest to the authenticity of their traffic, will likely result in the Commission continuing to receive 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.

Enhanced international attestation is another proposed solution that may reduce the number of unauthenticated international calls coming into the United States. Given concerns over illegal spoofing, international calls are more susceptible to interception under domestic call-blocking programs. International calls are also more likely to go unauthenticated or to receive "gateway" attestation through the STIR/SHAKEN call authentication framework upon reaching gateway providers and other domestic networks. However, some international providers have introduced a proposal at the Commission that would encourage the use of voluntary commercial agreements that enables the exchange of caller ID information for purposes of assigning these international calls the appropriate attestation level under the STIR/SHAKEN framework.[15]

Under the proposal, an international voice service provider would segment and deliver its voice traffic to domestic providers via separate trunks that correlates to the three attestation levels of STIR/SHAKEN. Like domestic carriers, international voice service providers maintain robust records for their customers and can quickly determine the location from which a call should be originating and whether it matches a previously agreed upon traffic profile. Based on

[15] *See* Ex Parte of Sheba Chacko, Chief Regulatory Counsel, BT Americas Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket Nos. 17-97 & 20-67 (filed Apr. 21, 2020).

the information passed along by the international provider, domestic carriers could then assign calls the appropriate attestation level and forward the authenticated traffic. It should be noted that the contractual remedies for an international provider's failure to appropriately identify and segment its traffic should provide the appropriate safeguards to ensure that this enhanced international attestation approach will not become a backdoor for illegal robocalls or spoofing. As with certificate delegation, the Commission should encourage this proposal as a means by which to ensure that more traffic is authenticated and receives appropriate attestation.

IV. A SAFE HARBOR FOR NETWORK-LEVEL BLOCKING IS UNNECESSARY AND LACKS THE OBJECTIVE CRITERIA THE AGENCY RELIED ON IN ADOPTING SAFE HARBORS BASED ON REASONABLE ANALYTICS AND BLOCKING OF BAD-ACTOR PROVIDERS.

In adopting safe harbors for call blocking in the *Third Report and Order*, the Commission struck the appropriate balance between meeting the statutory obligations of the TRACED Act, which required the Commission to connect a safe harbor "in whole or in part" to a call authentication framework, and providing voice service providers with assurances that good faith call blocking will not result in liability. As a result, voice service providers can now avail themselves of a safe harbor for call blocking programs based on reasonable analytics that includes caller ID authentication information as well as for blocking bad-actor providers.

At the same time, INCOMPAS commends the Commission for taking into consideration the concerns of competitive voice service providers and others about overbroad blocking and for noting in its analysis of alternative safe harbors that "a broad safe harbor that lacks objective criteria could lead to widespread blocking of wanted calls and abuses such as blocking for anticompetitive reasons."[16] Our members remain concerned about overbroad blocking

[16] *Third Report and Order* at para. 50.

conducted without objective criteria, and INCOMPAS opposes the Commission's proposal to extend its call blocking safe harbor to cover network-based blocking. As questions remain about what analytics are "reasonable" for call-blocking purposes and whether the STIR/SHAKEN framework will meet the needs of competitive voice service providers,[17] INCOMPAS urges the Commission to proceed cautiously with respect to the extension of call blocking safe harbors.

First, the Commission's previous decision to adopt call blocking based on any reasonable analytics provides voice service providers with ample permission to block calls that are "highly likely to be illegal." Second, as noted above, the Commission identified in the *Third Report and Order* multiple concerns with extending broader liability protections to safe harbors that lack objective criteria. Under this proposal, which was fashioned by the associations pushing for a broader safe harbor, voice service providers could avail themselves of a safe harbor by managing their network-level blocking with "sufficient human oversight"—a subjective management standard that "would make it extremely difficult to determine whether a particular approach is reasonable, both for callers and other voice service providers that are concerned about anticompetitive behavior and enforcement."[18] Additionally, each of the Commission's previous decisions on call blocking provided consumers with some opportunity to control their experience or opt-out of a call-blocking program. Taking them entirely out of the equation and permitting a network-level blocking safe harbor sets a troubling precedent for consumers and is not necessary to achieve the goals of Congress and the Commission to protect consumers from illegal robocalls.

If the Commission does adopt a safe harbor for network-level blocking, INCOMPAS reiterates it earlier recommendation that the Commission retain the authority to investigate and

[17] *See* Section III, *supra*.

[18] *Third Report and Order* at para. 50.

nullify the safe harbor for voice service providers that regularly block legitimate traffic or engage in anticompetitive or discriminatory behavior.

V. THE COMMISSION SHOULD CONSIDER NEW REDRESS MEASURES INCLUDING NOTIFICATION CODES AND EXPEDITIOUS DISPUTE RESOLUTION

INCOMPAS applauds the Commission's consideration of new redress requirements for voice service providers in order to minimize the occurrence of "false positives." To be truly effective, call-blocking tools must let providers know that blocking has occurred so that if a false positive needs to be addressed, the blocked caller or provider has that opportunity. Furthermore, call blocking disputes need to be resolved in a timely and efficient manner.

With respect to notifying providers that a call has been intercepted as part of a blocking program, INCOMPAS encourages the Commission to consider ways to promote the standardization of the use of cause codes, such as the RFC8688 / 608 (Rejected) Session Initiation Protocol response code, across IP networks to provide greater certainty, transparency and notice among interconnected carriers concerning call blocking. Cause codes contain a header that provides interconnected carriers with blocking treatment information so that originating or sending carriers can make necessary and appropriate operational and routing decisions. RFC8688 specifically contains a header that provides the caller with the blocking provider's contact information so that an originating provider can seek immediate redress for a call blocked in error. Although SIP cause codes may be unavailable to TDM call originators (it is not currently possible to map the notifications to code that could be triggered by TDM networks), standardized codes would be helpful to providers managing IP traffic.

Additionally, the Commission seeks comments on requiring voice service providers to respond to disputes about erroneous call blocking within a set time period. INCOMPAS

recommends that the Commission refrain from establishing a specific timeframe for a response, but to require voice service providers to use reasonable means to resolve call blocking disputes expeditiously. Given the differences in the resources and capabilities of the nation's voice service providers, a flexible approach to handling disputes is warranted. However, if the Commission determines that a specific timeframe is needed, INCOMPAS sees the Industry Traceback Group's ("ITG") policies and procedures as being instructive on this issue. In its application to the Commission to become the single industry traceback consortium, the ITG conveys the amount of time a voice service provider is permitted to complete a traceback investigation, which is reasonably comparable to the investigation a provider would have to complete to resolve a call blocking dispute. The ITG's guidance notes that a "prompt response" to an industry traceback request should be acknowledged within one business day and completed within 72 hours from initiation.[19] Based on this, and in the alternative to the flexible approach suggested above, INCOMPAS offers that voice service providers be given no less than 72 hours to resolve call-blocking disputes and 24 hours to provide acknowledgement of a request. .

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 *Fourth Further Notice*.

[19] *See* Letter of Patrick Halley, Senior Vice President, Policy & Advocacy, USTelecom—The Broadband Association, to Marlene H. Dortch, Secretary, FCC, EB Docket No. 20-22, ITG Policies at 8 (filed May 21, 2020) .

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

August 31, 2020