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

In the Matter of	)	
	)	
Protecting Consumers from One-Ring Scams	)	CG Docket No. 20-93

COMMENTS OF INCOMPAS

INCOMPAS, by its undersigned counsel, hereby submits these comments in response to the Federal Communications Commission's ("Commission" or "FCC") *Notice of Proposed Rulemaking* on various actions the Commission can take to combat one-ring scams in accordance with section 12 of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence ("TRACED") Act.[1]

I. INTRODUCTION & SUMMARY

INCOMPAS and its members appreciate the Commission's ongoing efforts to combat illegal robocalls and other calling schemes that defraud consumers and undermine confidence in voice service networks. Our members are active participants in industry efforts to eliminate illegal robocalls through traceback and the development of a robust call authentication framework. These companies have also dedicated significant time and resources to protecting customers from other illegal calls, like the one-ring scams identified in the Commission's *NPRM*. That Congress included one-ring scams in the recently passed TRACED Act[2] is further

[1] *See Protecting Consumers from One-Ring Scams*, CG Docket No. 20-93, Notice of Proposed Rulemaking, FCC 20-57 (rel. Apr. 28, 2020) ("*Notice*" or "*NPRM*").

[2] *See* Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act of 2019 ("TRACED Act"), S. 151, 116th Cong. (2019) (enacted) at § 12.

recognition that this type of illegal call represents another front in the battle against illegal robocalls and the bad actors that perpetrate these schemes.

According to our members, this front can be fought using many of the same techniques and practices that voice service providers are using to combat other illegal robocalls and instances of illegal spoofing. Industry appears to be well positioned to meet this challenge using the tools already in its arsenal, such as call analytics, reputational scoring, and traceback protocols. Additionally, the development of the STIR/SHAKEN caller ID authentication framework will give voice service providers the ability to present consumers with valuable information about the attestation level of a call, which should ultimately provide call recipients with better information about the potential for fraud. To combat one-ring scams, INCOMPAS urges the Commission to continue to promote the adoption of these solutions, and encourage the regulatory flexibility that allowed voice service providers to develop them in the first place.

With these solutions in place and in development, INCOMPAS suggests that any new set of measures that the Commission adopts to combat one-ring scams should be minimal and that the Commission should instead focus on consumer education efforts where a lack of awareness about the nature of these calls persists. To that end, INCOMPAS supports allowing voice service providers to block calls from numbers associated with one-ring scams.[3] The association also supports a notification requirement that will quickly alert unassuming consumers that they are dialing an international toll-generating number before connecting the outbound call. However, INCOMPAS opposes any new rule that would require gateway providers to verify the

[3] As we have previously asserted, it is important that the call blocking analytics providers use to identify these numbers are applied in a reasonable, non-discriminatory, and competitively neutral manner. *See* Letter of Christopher L. Shipley, Attorney & Policy Advisor, INCOMPAS, to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59, WC Docket No. 17-97 (filed May 30, 2019), at 2 (offering language that was included in the *Call Blocking Declaratory Ruling* that call blocking programs be applied in a non-discriminatory, competitively neutral manner).

"nature or purpose" of a call with the foreign originator before initiating service as many providers are already using "Know Your Customer" principles to prevent doing business with customers who engage in fraud.

II. IN COMBINATION WITH EXISTING TRACEBACK AND AUTHENTICATION MEASURES, COMPETITIVELY NEUTRAL CALL BLOCKING AND CONSUMER NOTIFICATIONS WILL MITIGATE ONE-RING SCAMS.mbers

In the NPRM, the Commission proposes to allow voice service providers to block calls from phone numbers associated with one-ring scams.[4] To that end, the Commission seeks information on providers' ability to reliably identify such numbers. INCOMPAS members report that the characteristics of one-ring scams are readily identifiable using a combination of data analytics and other measures. The signature of these calls, including that they are noticeably shorter than most illegal robocalls, is readily recognizable, meaning that it can be differentiated from legitimate traffic, such as notification service calls. Based on these factors, voice service providers are able to engage in reputational scoring which can be used to determine whether there is a reasonable basis for blocking such a call. Importantly, our members indicate that the calls can be traced back to the originating provider when their volume rises above the threshold for Industry Traceback Group action. Furthermore, voice service providers are using "Know Your Customer" and other traffic management practices to identify new customers and ensure that they are providing detailed traffic-profile information.[5] If the traffic originated by the

[4] *NPRM* at ¶ 14.

[5] *See* Reply Comments of West Telecom Services, LLC, CG Docket No. 17-59, WC Docket No. 17-97 (filed Aug. 23, 2019), at 3 (describing onboarding procedures for new wholesale customers such as the development of a traffic profile, which includes information like average length of call, estimated call types, and projected call volumes).

customer diverges significantly from the initial profile, then providers have an additional indication that the customer may be engaging in fraudulent activity.

Up to this point, the Commission has taken a measured and deliberate approach to call blocking with consideration given to many of the concerns expressed by our members and others[6] that have highlighted the imbalance that may result if large providers are permitted to use call blocking to discriminate against competitive providers. For example, in 2017, the Commission adopted call blocking rules for invalid, unallocated, and most unassigned numbers, but noted that providers may not block unassigned numbers that are used for lawful purposes, such as intermediate numbers, administrative numbers, or proxy numbers.[7] Additionally, in its 2019 *Call Blocking Declaratory Ruling*, the Commission wisely asserted that voice service providers' opt-out call blocking programs must be based on reasonable analytics and that "such analytics must be applied in a non-discriminatory, competitively neutral manner."[8]

While INCOMPAS has previously questioned the application of call blocking measures in situations where regular voice traffic may be blocked because it resembles the analytical profile of an illegal robocall (for instance, when a provider sends a large burst of automated notifications in a short timeframe), the Commission's call blocking proposals in the instant

---

[6] *See*, *e.g.*, Comments of Twilio Inc., WC Docket Nos. 17-97, 20-67 (filed May 15, 2020), at 8 (urging the Commission to adopt more specific parameters "to ensure that lawful calls are not blocked or stymied by call analytics").

[7] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 9706, 9731-9732 (2017) (indicating that these numbers may be used by VoIP providers or dynamically assigned rather than assigned to a specific subscriber).

[8] *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, ¶ 35 (rel. June 7, 2019) ("*Call Blocking Declaratory Ruling*").

proceeding present less risk to competitive providers because the characteristics of one-ring scams can be readily differentiated from lawful calls. Nevertheless, if the Commission adopts call blocking for one-ring scams, INCOMPAS urges the agency to clarify that voice service providers are required to apply the analytics used to identify these scams in a reasonable, non-discriminatory, and competitively neutral manner. This would ensure consistency with the approach taken by the Commission with respect to call blocking programs in 2019, and address the concerns of competitive providers that call blocking could otherwise be used in a discriminatory manner. Additionally, INCOMPAS encourages the Commission to adopt the standardized use of notifications, like cause codes, that alert an originating provider or a call recipient that a call has been intercepted as part of a blocking program.[9] Notifications should be an essential component of any call blocking model for mitigating illegal calls as they give providers the opportunity to seek immediate redress of occurrences of false positives.

INCOMPAS supports the Commission's common sense proposal to require voice service providers to notify a customer dialing an international-toll generating number before connecting the call. While it is likely unnecessary to provide the specific international rate that a caller will be charged by making the call, providing the customer with a standard notification that they are initiating an international call will save many unsuspecting customers from responding to a one-ring scam. Despite the Commission's best efforts to alert the American public, it is clear that a significant portion of callers are still unaware of the specifics of this scam, particularly that the calls most likely originate overseas and that by engaging in a callback, the caller will incur

[9] *See* Comments of INCOMPAS, CG Docket No. 17-59, WC Docket No. 17-97 (filed Jan. 29, 2020), at 4-5 (recommending that the Commission collect data on the use of cause codes such as the 608 (Rejected) Session Initiation Protocol response code).

international charges. A quick, standardized notification will likely alert most consumers to the fact that the originating callers' intentions were fraudulent.

Finally, the Commission seeks comment on whether to consider a one-ring-specific safe harbor.[10] In this proceeding, the Commission seeks to extend the reach of the *Call Blocking Declaratory Ruling,* which permitted voice service providers to engage in opt-out call blocking of unlawful calls based on *any* reasonable analytics, to one-ring scams. The *Call Blocking Declaratory Ruling* grants providers significant authority to engage in robocall mitigation, making a safe harbor or a one-ring-specific safe harbor unnecessary (or redundant), and the results of the Commission's prior actions should be analyzed before further liability protection is considered. Furthermore, the use of a safe harbor for blocking reduces the incentive of voice service providers to improve call-blocking measures or enact formal redress options.

III. A NEW RULE FOR INTERNATIONAL GATEWAY PROVIDERS VERIFYING THE NATURE AND PURPOSE OF FOREIGN ORIGIINATORS WOULD BE UNNECESSARY AND OVERLY BURDENSOME.

In accordance with section 12(b)(6) of the TRACED Act, the Commission seeks comment on potential obligations for international gateway providers, including a requirement that these providers "verify with the foreign originator the nature or purpose of calls before initiating service."[11] As noted above, in addition to actively assessing network traffic for evidence of fraud, providers are increasingly taking steps to understand the traffic profile of their existing and new customers before these customers initiate traffic on their networks.[12] By

[10] *NPRM* at ¶ 17.

[11] *Id*. at ¶¶ 20-21.

[12] For example, INCOMPAS members who are international carriers describe robust processes for onboarding enterprise customers that include: (i) customer contractual provisions requiring the services be used for lawful purposes; (ii) configuring the services so that calls can only

incorporating "Know Your Customer" principles, voice service providers have been able to add objective data points that inform their analysis of and help them to identify suspected one-ring scams. For example, after contracting with a new customer (including provisions that define the penalties for fraudulent use of the network) and establishing a traffic profile, voice service providers can observe the customer's call characteristics and monitor for deviation from the profile or other signs of potential fraud. Also, if a voice service provider receives evidence that a new customer is engaged in fraud, then the customer's traffic can be suspended until they can make a demonstration that the individual or company is not engaged in fraudulent behavior, like one-ring scams.

From an operational standpoint, INCOMPAS members prefer these anticipatory and objective measures to the Commission's proposal to require international gateway providers to verify the "nature and purpose" of the calls before initiating service. 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. Accordingly, INCOMPAS urges the Commission not to pursue a new rule that would require gateway providers to have to put a verification process with foreign originators in place. Instead, the Commission should encourage voice service providers to adopt "know your customers" principles and continue to work with international gateways and

---

originate from telephone numbers provisioned by the carrier itself, or numbers provisioned by different carriers that the customer has verified it has the right to use (including presentation numbers as well as network numbers); and (iii) designing the network ingress points with known customer peering connections. The carrier then rejects any call that attempts to originate on its network using numbers or origination points that are not part of the customer's profile.

the Industry Traceback Group to specifically identify bad actors originating these one-ring scams.

IV. CONCLUSION

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

Respectfully submitted,

INCOMPAS

/s/ Christopher L. Shipley

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

June 19, 2020