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 Consumer and Governmental Affairs Bureau's ("CGB" or "Bureau") *Public Notice* seeking input for a report examining the effectiveness of call-blocking measures on unlawful robocalls[1] following the Federal Communications Commission's ("Commission" or "FCC") adoption of the *Call Blocking Declaratory Ruling and Third Further Notice* in 2019.[2]

In the face of the continuing need to eliminate illegal and fraudulent robocalls, INCOMPAS commends the Commission for taking a measured and incremental approach to call blocking that has allowed voice service providers to address this pernicious challenge while simultaneously working to protect our communications ecosystem for legitimate calls. Since the adoption of the *Call Blocking Declaratory Ruling and Third Further Notice*, INCOMPAS members have been actively engaged in efforts to mitigate illegal robocalls and develop

---

[1] *See Consumer and Governmental Affairs Bureau Seeks Input for Report on Call Blocking*, CG Docket No. 17-59, WC Docket No. 17-97, Public Notice (rel. Dec. 20, 2019) ("Notice").

[2] *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 (2019) ("*Call Blocking Declaratory Ruling and Third Further Notice*").

measures to minimize the rate of "false positives." This includes using analytics to identify fraudulent calls and participating in the implementation of the STIR/SHAKEN caller ID authentication framework. Nevertheless, despite serious efforts of well-intentioned providers to refine these measures, call blocking in a highly complex communications environment continues to carry a high risk that lawful traffic may be inadvertently intercepted before being completed, and in some recent instances, INCOMPAS members and their customers have been adversely affected. INCOMPAS encourages the Commission to, in part, measure the effectiveness of call blocking tools by how they minimize the rate of blocking "false positive" traffic (i.e. wanted communications). Furthermore, as the Commission studies the ramifications of its recent decisions to permit voice service providers to offer their customers call-blocking programs, INCOMPAS urges the agency to conduct a thorough review and analysis regarding what call-blocking treatments should be considered to be "reasonable analytics" as well as specific information concerning how cause codes should or can be expected to be used by providers in response to a blocked call.

For INCOMPAS members, the effectiveness of call-blocking tools is complicated by the fact that the Commission allows providers to "offer opt-out call-blocking programs based on *any* reasonable analytics designed to identify unwanted calls."[3] As a result, providers are forced to navigate and manage a variety of different call-blocking treatments and factors and when calls are blocked there is often a lack of clarity and notice from the blocking carrier as to the particular reasons why the calls are blocked. Many INCOMPAS members have developed relationships with their call partners to identify the necessary channels to quickly resolve false positives, however, this may not address all instances in which legitimate calls are blocked.

[3] *Call Blocking Declaratory Ruling and Third Further Notice* at 4887 (emphasis added).

INCOMPAS members have experienced differentiated results depending on the given call analytics provider used by a terminating carrier and are often forced to rely on customers to bring notices of blocked calls to their attention. For example, at the end of 2019, a customer that was sending two-factor authentication requests to participating subscribers via voice communications channels alerted its provider, an INCOMPAS member, that such notices were being blocked and not being received by customers seeking to use its service and causing a disruptive consumer experience as a result.[4] Without adequate transparency, industry standards or proper notification about the methods leading to the actual call blocking, it may be impossible for the provider to make changes or work with its customer to avoid the situation in the future. Members have also expressed concerns that automated emergency notifications or where end users may opt-in to security services and wish to receive automated security-related notifications, could be blocked since it shares similar traits to the two-way call authentication described above. Our members indicate they are seeing an increase in such use cases and together with their end-user customers, seek assurances that these calls will not blocked under an overly-broad umbrella of "reasonable analytics."

Recognizing that industry is still in the early stages of using call blocking to combat unlawful robocalls, INCOMPAS urges the Commission to provide additional clarity on what call-blocking treatments could be categorized as "reasonable" in the report. Providing analysis of the common practices used will assist all communications end-users, as well as competitive and smaller providers, understand precisely how analytics used by larger carriers work and

[4] *See* Letter from Mark Brennan, Counsel to the American Association of Healthcare Administrative Management, *et al*., CG Docket Nos. 02-278, 17-59, WC Docket No. 17-97 (filed May 28, 2019) (indicating that the effect of the *Call Blocking Declaratory Ruling* would be to treat "'alerts and reminders' sent from legitimate companies in the same manner as fraudulent and scam calls").

provide a greater understanding of the steps that these providers need to take to ensure that legitimate traffic is not blocked. This would comport with the requirements of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act that the call-blocking programs initiated under the *Call Blocking Declaratory Ruling* "are provided with transparency and effective redress options" for consumers and callers.[5] Furthermore, in the proposed Data Analytics Robocall Technology (DART) Act, Congress contemplates providing the Commission with the authority to conduct a pilot program that would require voice service providers to quickly address notifications of false positives and evaluate "the means by which to address future calls from the number."[6] A pilot program, such as the one proposed in the DART Act, could provide meaningful data about what constitutes reasonable analytics and should be considered by the Commission.

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. To that end, INCOMPAS recommends that the Commission provide data in the report about the use of cause codes such as the 608 (Rejected) Session Initiation Protocol ("SIP") response code.[7] This response code could be standardized and implemented across networks to provide the necessary notice to a caller or provider that a call has been blocked. The code contains a header that provides the caller with the blocking provider's contact information so that

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

[6] Data Analytics Robocall Technology Act of 2019, S. 2204 (116th Congress), § 2.

[7] E.W. Burger & B. Nagda, *RFC 8688 A Session Initiation Protocol (SIP) Response Code for Rejected Calls*, INTERNET ENGINEERING TASK FORCE (Dec. 2019), https://tools.ietf.org/pdf/rfc8688.pdf.

either the caller or the originating provider can seek immediate redress. The use of industry-established standardized cause codes could have alerted our member discussed above to the issues that its customer was having with its two-way authentication and allowed the provider to quickly resolve the issue on the customer's behalf.

The Commission should also consider the impact that IP interconnection and traffic exchange has on the effectiveness of robocalling mitigation utilizing the STIR/SHAKEN framework and attendant call-blocking measures. As noted recently by NTCA—The Rural Broadband Association, "the lack of 'basic rules of the road' for IP interconnection for voice traffic" stands as the "primary barrier to industry-wide implementation of SHAKEN/STIR."[8] A call originated on an IP network receives an identity header that is removed when the call is exchanged between an IP and TDM network. Calls without this authentication are more likely to be blocked by call-blocking applications, even if the call is legitimate.[9] Industry would benefit from a uniform implementation of the SHAKEN/STIR framework; however, without IP interconnection and exchange of traffic such uniform implementation will be deterred.

Finally, INCOMPAS urges the Commission to continue to exercise caution when considering new proposals to broaden call-blocking rules or safe harbor protections for providers

[8] Letter of NTCA—The Rural Broadband Association, CG Docket No. 17-59, 71-97, CC Docket No. 01-92, 10-90 (filed Jan. 16, 2020).

[9] In its letter to the FCC, NTCA describes this as a "reverse call completion problem" as rural callers without access to IP networks would appear unauthenticated when reaching urban areas. INCOMPAS is equally concerned about the disparate treatment of legitimate calls and the impact this will have on competitive and smaller providers. *Cf*. Letter of John Ayers, Vice President of Corporate Development & Government Affairs, First Orion Corporation, CG Docket No. 17-59, WC Docket No. 17-97 (filed Jan. 24, 2020) (reporting that there are "legitimate calling scenarios not currently contemplated by the basic SHAKEN/STIR framework" that must be addressed in these "early days" of integration of call authentication frameworks and analytics).

that employ call-blocking tools that cannot take into account the current divide over IP and TDM networks.

For the reasons stated herein, INCOMPAS urges the Commission to consider the recommendations in its comments as it examines the issues raised in the *Notice* related to the forthcoming report on the implementation and effectiveness of blocking measures.

Respectfully submitted,

INCOMPAS

/s/ Christopher L. Shipley

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

January 29, 2020