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
Executive Director of Public Policy
1100 G Street NW
Suite 800
Washington, D.C. 20005
(202) 872-5746
cshipley@incompas.org

August 9, 2023

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") *Eighth Further Notice of Proposed Rulemaking* in CG Docket No. 17-59 and *Third Notice of Inquiry* in WC Docket No. 17-97 seeking comment on additional measures to stem the tide of illegal robocalls while increasing consumer trust in voice services.[1]

I. INTRODUCTION & SUMMARY

INCOMPAS, the Internet and competitive networks association, welcomes the opportunity to submit comments in response to the Commission's proposals to mitigate illegal robocalls. Achieving the Commission and industry's goal of developing a comprehensive and standardized framework that will address the actions of illegal robocallers on an ongoing basis requires consistent evaluation of the requirements the Commission has adopted and analysis of gaps in the current rules. Our members represent a variety of different voice service models, including traditional CLECs and VoIP providers, that serve residential and enterprise customers.

[1] *Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Seventh Report and Order in CG Docket No. 17-59 and WC Docket No. 17-97, Eighth Further Notice of Proposed Rulemaking in CG Docket No. 17-59, and Third Notice of Inquiry in CG Docket No. 17-59, FCC 23-37 (rel. May 19, 2023) ("*Further Notice*" and "*NOI*").

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

INCOMPAS welcomes the *Further Notice's* simultaneous examination of call blocking, immediate call blocking notification, and call labeling as these three issues should be inextricably linked in providers' efforts to mitigate and eliminate illegal robocalls on their networks. The proposals on which the Commission seeks comment wrestle with important topics to INCOMPAS members who remain concerned that these practices (and the lack of a standardized notification process) may be used by large providers in manners that are discriminatory and anti-competitive. Members continue to have concerns about terminating providers' treatment and removal of critical information and data added to the call at the point of origination. When this information is removed from a call, it can dramatically affect two-way traffic exchange through inadvertent or intentional blocking decisions as well as determinations about how to label voice traffic if at all.

In fact, the "black box" of terminating provider's call analytics is a threat to the Commission's efforts to ensure that calls are delivered in a non-discriminatory and competitively neutral manner and it is becoming clearer that these analytics are deployed unevenly and without transparency and accountability. Indeed, the continued lack of effective feedback to upstream providers from terminating providers and their analytics companies disclosing both blocking and call presentation determinations is significantly impacting the health and future viability of the

entire PSTN. An overzealous focus on robocalling without oversight and accountability at the terminating end threatens to undo decades of competition, innovation, and consumer benefits that sprung from the Telecommunications Act of 1996.

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 carefully 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.

As to the Commission's specific proposals in the *Further Notice*, INCOMPAS first offers comment on some unintended consequences of its proposal to *require* terminating providers to

[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); *Advanced Methods to Target and Eliminate Unlawful Robocalls*, *Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Sixth Report and Order in CG Docket No. 17-59, Fifth Report and Order in WC Docket No. 17-97, Order on Reconsideration 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) (placing new obligations on gateway providers); *Call Authentication Trust Anchor*, WC Docket No. 17-97, Sixth Report and Order and Sixth Further Notice of Proposed Rulemaking, FCC 23-18 (rel. Mar. 17, 2023) (strengthening caller ID authentication requirements for non-gateway intermediate providers and expanding robocall mitigation requirements for all providers).

conduct analytics-based blocking of calls that are highly likely to be illegal. Next, given its increasing usage by carriers, INCOMPAS urges the Commission to adopt SIP Code 608 as the primary mechanism by which providers receive immediate notification and seek redress for blocking of legitimate calls. To do so would be consistent with the Commission's previous decisions in this proceeding and in accordance with requirements in the TRACED Act. Finally, to help restore consumer trust in voice services, INCOMPAS endorses the Commission's proposal to require providers to transmit complete and accurate caller data to call recipients.

With respect to the issues raised in the *NOI*, our members report that some practices for fighting illegal calls, like honeypots, can be valuable tools for identifying the traffic profile of illegal robocalls. However, honeypots could be better leveraged as tools to fight illegal robocalls if the process included transparency requirements into how analytics engines audit these calls and use and share data. Also, INCOMPAS recommends that the Commission initiate a rulemaking that would standardize and create greater transparency around the call labeling process and adopt a labeling notification redress mechanism that would alert the originating provider if a terminating provider re-labels or removes call presentation information.

II. THE COMMISSION'S MANDATORY CALL BLOCKING PROPOSALS WILL THREATEN LEGAL TRAFFIC WHILE GIVING BAD ACTORS MORE INSIGHT INTO HOW TO CIRCUMVENT COMMISSION RULES

In the instant proceeding, the Commission is seeking comment on additional requirements for voice service providers with respect to call blocking, including requiring terminating providers to offer analytics-based blocking of calls that are highly likely to be illegal on an opt-out basis without charge to consumers.[3] INCOMPAS has previously expressed its reservations about the unintended consequences of employing call blocking as a solution for

[3] *See Further Notice* at para. 71.

illegal robocall mitigation,[4] as well as call blocking using reasonable analytics that is not applied in a non-discriminatory and competitively neutral manner. The exceptional complexity of communications traffic exchange on the Public Switched Telephone Network (PSTN) ecosystem is often underappreciated and misunderstood. Our members are increasingly tasked with addressing instances of call blocking and false positives in their networks, a situation that continues to be compounded by implementation delays of an immediate call blocking notification and redress mechanism.

Carriers are experiencing instances where its corporate customers experience wide blocking of lawfully placed calls because certain characteristics are similar to those flagged by analytics engines. As an example, banking institutions place numerous calls for fraud alerts and debt collection that may look like unlawful robocalls to a software program, but not only are they legal, they are explicitly consented to by the called party in its contract with the banking institution. This blocking is occurring even when those calls have earned an "A" attestation level in the STIR/SHAKEN call authentication framework. Despite the Commission's requirement that any carrier blocking calls in this manner must have a robust redress process to handle the inaccurate blocking of legitimate calls, companies report that even when they get a block lifted on an outgoing telephone number, the same number is blocked again within a day or two. Until the inadequacy of such redress processes is addressed and the call blocking software industry has matured to accommodate such nuances, the FCC should not mandate any additional call blocking requirements, particularly those that are analytics-based.

[4] *See, e.g.*, Comments of INCOMPAS, CG Docket No. 17-59 (filed Aug. 21, 2020), at 6, 10-12 (discussing how call blocking could undue progress the Commission has made with respect to rural call completion).

It should be noted that the Commission declined to adopt a similar proposal that would have required gateway providers to block calls that are highly likely to be illegal based on reasonable analytics.[5] The Commission determined that it would have to "more strictly define 'reasonable analytics' in order for gateway providers to be certain that they are in compliance with a mandatory blocking rule" and indicated that this could "provide a road map bad actors could use to circumvent blocking."[6] In the instant proceeding, the Commission provides a similar, non-exhaustive list of factors that a voice service provider might consider when blocking calls considered to be "highly likely to be illegal" or "unwanted."[7] According to our members, this guidance would need to be narrowed to remove factors that might otherwise fit the profile of legitimate, wanted robocalls—for example public safety or school district notifications are typically calls with low average duration that are sent out in a large burst in a short timeframe to the public or families that have consented to receiving these notifications. However, such changes could also be used by actors to "more easily circumvent blocking."[8] Given the Commission's previous rejection of a mandate to block calls that are highly likely to be illegal in the *Gateway Provider Order*, the Commission must first reconcile that finding with this proposal, which it does not do in the *Further Notice*.

---

[5] *See Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor,* CG Docket No. 17-59, WC Docket No. 17-97, Sixth Report and Order in CG Docket No. 17-59, Fifth Report and Order in WC Docket No. 17-97, Order on Reconsideration 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, para. 92 (rel. May 20, 2022) ("*Gateway Provider Order*").

[6] *Gateway Provider Order* at para. 92.

[7] *Further Notice* at 72.

[8] *Id.*

If the Commission ultimately decides to adopt a proposal that would require terminating providers to offer analytics-based call blocking, the Commission should first require assurances from terminating voice service providers that their analytics are being applied in a manner that is non-discriminatory and competitively neutral. Furthermore, if the Commission elects to mandate additional blocking, terminating providers should be required to share information about their analytics-based blocking decisions with vetted and trusted providers and provide an opportunity to refine the analytics engines to ensure that legitimate voice traffic is not blocked or relabeled. The Commission must also clarify what existing analytics blocking requirements would attach to this obligation, such as whether manual oversight of the blocking is required, whether the terminating provider must utilize STIR/SHAKEN, and, importantly, if a safe harbor will apply. Finally, the Commission's existing safe harbor for analytics blocking of highly likely to be illegal calls is limited to illegal calls, not calls that are simply "unwanted" which would be captured by this rule.[9] Rather than extend the safe harbor to "unwanted" calls, which may include calls that are highly likely to be illegal but may also include legitimate robocalls, the Commission should apply the same limitation to analytics-based blocking.

III. PROVIDERS SHOULD BE REQUIRED TO USE SIP CODE 608 TO NOTIFY ORIGINATING PROVIDERS AND CALLERS OF BLOCKED CALLS

Since instituting call blocking requirements in an attempt to curb illegal robocalls, INCOMPAS has welcomed the Commission's involvement in identifying and implementing an immediate call blocking notification mechanism that offers providers a means of redress should their calls be intentionally or inadvertently blocked.[10] A redress mechanism is a way to ensure

[9] 47 CFR § 64.1200(k)(3).

[10] *See* Comments of INCOMPAS, CG Docket No. 17-59, 12 (filed Aug. 31, 2020) (urging the Commission to promote the standardization of the use of cause codes to resolve call blocking disputes).

that call blocking is conducted in a non-discriminatory and competitively-neutral manner in accordance with the Commission's rules while also enhancing intermediate and originating providers' abilities to monitor and manage their traffic more effectively. INCOMPAS posits that the regulatory framework for addressing illegal robocalls will be the most efficient once the Commission standardizes a method for immediate call blocking notification.

For the reasons previously stated in this proceeding, INCOMPAS continues to believe that SIP Code 608 is the best solution for immediate call blocking notification.[11] INCOMPAS has advocated for a robust and uniform system of notification and redress so that callers and voice service providers can respond to and correct call blocking in the event of false positives. A notification and redress system that requires the use of SIP Code 608 for notification would not only satisfy the TRACED Act's requirements for the Commission to provide transparency and effective redress to callers, but would be a critical component of the Commission's efforts to successfully mitigate illegal robocalls through call blocking. Such a system would encourage industry cooperation to address erroneous blocking, lead to innovation that will correct ongoing problems, and provide an avenue to help address disputes that may not otherwise be easily resolved between providers. While concerns about overblocking may not immediately abate, providing competitive voice service providers with adequate information via immediate automated notifications to enable effective redress on behalf of their customers for either erroneously or intentionally blocked calls is critical to the Commission's goals of restoring trust in the voice service networks. Consumers are the ultimate beneficiaries of an effective

---

[11] *See*, *e.g.*, Joint Reply Comments of the Voice on the Net Coalition, INCOMPAS, and the Cloud Communications Alliance, CG Docket No. 17-59 (filed Feb. 14, 2022) (arguing that failure to implement SIP Code 608 "will result in legitimate calls being blocked and in onerous redress processes).

notification process as it helps ensure that critical communications reach their intended audience while illegal traffic is identified and mitigated. As such we continue to urge the Commission to require providers to return 608 codes if their analytics determine that a call should be blocked.

One particular benefit of SIP Code 608 is that it is already in use; our members indicate that they are actively receiving these codes from carrier partners when a call is rejected. Since SIP Code 608 was promulgated specifically to address robocall blocking and was designed to provide the actionable information that callers and their service providers need to trigger redress options, our members have been able to quickly address instances of inappropriate call blocking with downstream providers on behalf of their customers. That carriers are actively sending 608 responses is a welcome development given the protestations of other stakeholders about the ability of voice service providers to implement the code in their networks in the near term. This should give the Commission the assurances it needs to rely on its initial selection of SIP Code 608 as the primary means by which terminating providers should notify callers or originating providers of a blocked call.[12] Furthermore, the Commission should move quickly to mandate SIP Code 608 and set a deadline by which all providers will be required to adopt and use the code for notification purposes.

In the alternative, INCOMPAS believes that having a standard is better than no standard—as noted above, providing a means for seeking redress and addressing false positives is critical to the institution of any call blocking regime. The Commission must actively dissuade scenarios in which providers are allowed to use a variety of cause codes to alert originating voice

[12] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Fourth Report and Order, 35 FCC Rcd 15211, 15234-38, paras. 39-47 (2020) ("*December 2020 Call Blocking Order*").

service providers and callers that a call has been blocked.[13] Therefore, if the Commission chooses to require the use of a different SIP code, it should adopt and require immediate implementation of SIP Code 603+ as the next possible option. As INCOMPAS, the Cloud Communications Alliance, and the VON Coalition recently stated "[t]he Commission should ensure that any 603+ standard meets the TRACED Act's requirements of transparent and effective redress, without undue costs to callers."[14] Regardless of the Commission's ultimate decision, any immediate call blocking notification solution must allow for the inclusion of specific information about the blocked call and the contact information for the provider doing the blocking. In either event, INCOMPAS strongly recommends that the Commission not mandate any further call blocking requirements until the Commission settles on a redress mechanisms and has mandated its use by a date certain.

IV. THE COMMISSION CAN INCREASE TRUST IN THE CALLER ID BY REQUIRING PROVIDERS TO TRANSMIT ACCURATE CALLER DATA TO CALL RECIPIENTS

The Commission's proceeding on eliminating and mitigating illegal robocalls is entirely about restoring consumer trust in the nation's voice service networks and preventing citizens from being defrauded by criminals. To achieve these worthy goals, the Commission should make every effort to arm consumers with as much information as possible for them to make informed decisions about whether a caller poses a potential risk. As a member of the Secure Telephone Identity Governance Authority, INCOMPAS believes that consumers will benefit

[13] INCOMPAS members report that some carriers are sending 503 codes ("service unavailable disconnect code") to alert providers of call blocking. This code contains no usable information and does not sufficiently provide originating providers with the information to take next steps, if warranted, to begin the redress process or further investigate possible fraud on the network.

[14] *See* Letter of INCOMPAS, Cloud Communications Alliance, and the VON Coalition to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59, 3 (filed June 30, 2022).

from receiving information about a call's attestation level and the level of confidence a provider has about the call's point of origin. Providing an indication of the caller ID authentication status (*i.e.* a green STIR/SHAKEN checkmark) to the call recipient is an important step towards regaining consumer trust in voice networks. However, INCOMPAS agrees with the Commission proposal to require voice service providers to combine the display of STIR/SHAKEN status with caller name information as it will offer consumers that positive assertion that the call is indeed coming from the individual or business listed in the call data.

As the Commission considers this proposal, INCOMPAS urges the Commission to analyze how terminating providers are treating and manipulating call presentation, including caller name information and call labeling. INCOMPAS members can confirm the Commission's observation that "[m]obile phones do not routinely display information from caller ID (CNAM) databases."[15] What we are observing in the marketplace is that not only are callers not getting the CNAM information that they have been historically accustomed to but calls are also being mislabeled as spam (or "spam likely"). As a result, call recipients are not getting the information they need to make informed decisions about the identity of the caller, even if the caller is legitimate. A filing by Unified Office, Inc. recently raised concerns about terminating providers and their analytics company deleting or removing a customer's name from the Caller ID field resulting in the mislabeling of calls across all attestations levels as "spam likely" or "something else not recognized by the called party."[16] As indicated by Unified Office's CEO, Ray Pasquale, "[t]he resulting confusion over the labeling of calls is contributing to the loss of trust and

[15] *See Further Notice* at par. 95.

[16] *See* Letter of Glenn Richards, Counsel for Unified Office, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 17-97, 4-5 (filed June 21, 2023).

confidence in our public communication network, which is the opposite of what the FCC had intended in this ruling."[17] Unfortunately, the Unified Office comments illuminate that some of the most feared risks with adopting an entirely new blocking and labeling regime that dramatically reverses a number of the long-standing tenets of interoperability and traffic exchange are now a reality.

In order to promote accurate caller data to call recipients, INCOMPAS strongly recommends advancing the use of Rich Call Data ("RCD") as the preferred method for sharing such information, so long as it is managed in a standardized and competitively neutral manner. RCD utilizes flexible IP technology that can seamlessly integrate into the SIP header which would align with STIR/SHAKEN's reliance on IP technology and further advance the IP transition. The Commission's primary objective should remain the rapid promotion of IP interconnection to ensure both STIR/SHAKEN authentication and RCD information can be efficiently received by terminating parties, avoiding any loss over TDM networks. INCOMPAS sees RCD as the superior choice to the currently available alternatives. While consumers value call identifying information, CNAM does have a number of limitations that can be improved upon in an all-IP environment. For example, there are multiple CNAM databases, creating multiple sources and problems can arise with terminating providers properly updating their CNAM databases to retrieve accurate CNAM information during calls, leading to either incomplete or outdated CNAM information being displayed. Finally, it is essential to acknowledge the various reasons why CNAM may not be populated, including the legitimate uses cases that may not want their information displayed (*e.g.* a shelter for victims of domestic violence, Planned Parenthood). Consequently, providers should reasonably expect that

[17] *Id*. at 5.

terminating providers and their analytics engines should generally not apply a negative call labeling when an "A"-attested call is received without any CNAM information.

INCOMPAS therefore recommends that the Commission urge finalization of industry standards related to RCD so that RCD can be incorporated into the existing STIR/SHAKEN framework and governance structure to enhance caller name information presentation.

V. THE COMMISSION SHOULD TAKE IMMEDIATE ACTION TO BRING MORE TRANSPARENCY AND ACCOUNTABILITY TO ROBOCALL MITIGATION TOOLS SUCH AS HONEYPOTS AND CALL LABELING

a. Honeypots Are a Valuable Tool in the Fight Against Illegal Robocalls, But Could Be More Effective if Providers More Readily Shared Results and Uses

In the *NOI*, the Commission seeks comment on tools voice service providers currently use to identify and combat illegal calls.[18] The Commission is particularly interested in information regarding the use of honeypots, as well as any anticipated benefits or concerns that could arise from its use. Generally, INCOMPAS members recognize honeypots as a valuable tool for service providers to identify illegal traffic, however the lack of transparency into how terminating providers and their analytics engines use honeypots, including how they may choose to share their data should be addressed by the Commission.

Currently, honeypots are being used to inform providers on the terminating end on how to block substantially similar future calls, as opposed to stopping current illegal robocall campaigns. There is no audit or feedback process to notify originating providers of issues identified in their calls by honeypots. Without putting a notification or feedback system in place, there is no way for originating providers to address or understand why their calls were captured, a step that could further assist originating providers eliminate illegal calls. Without this

[18] *NOI* at paras. 106-108.

transparency and valuable information sharing, the use and sharing of honeypot data continues to create real risks of blocking or mislabeling legitimate traffic. Non-transparent blocking and labeling harms the communications ecosystem and tilts the scales in favor of those that control call presentation and may not advance the cause of eliminating illegal robocalls as effectively as possible. Given providers dedication to resolving the illegal robocall problem and their track record of working together to solve this issue, the Commission should promote systems that create transparency between providers and sharing of honeypot data in order to effectively eliminate illegal robocalls.

b. The Commission Should Initiate a Rulemaking Proceeding to Standardize Call Labeling In Order To Prevent Manipulation of Call Data at the Terminating End

The Commission also seeks comment on the current state of call labeling.[19] As noted above, INCOMPAS members remain concerned about terminating providers (often wireless carriers) treatment of call presentation and caller ID authentication and view call labeling as an issue that is as important as blocking and notification. Call labeling, like so many issues that occur on the terminating end, requires additional transparency. The Unified Office filing shows that the "black box" of terminating provider's analytics engines can result in legitimate traffic (that contains appropriate attestation and caller name information) being relabeled as "spam likely" to the confusion and frustration of callers and consumers. INCOMPAS recommends that the Commission initiate a *Notice of Proposed Rulemaking* that would standardize call labeling and add transparency between providers through the inclusion of a redress mechanism for originating providers and callers. Similar to the way the Commission is seeking SIP code

[19] *Id*. at paras. 110-112.

notification for immediate call blocking notification, when a call is relabeled, originating service providers should be notified and informed of the specific label that is used for that call—such as "spam likely." The industry has already worked on best practices related to redress mechanisms in call blocking and labeling that the Commission can look to for guidance.[20]

In addition to the lack of transparency, INCOMPAS members are concerned that analytics engines are leading to calls being inappropriately or incorrectly "over-labeled." For example, new numbers with no previous data being mislabeled automatically as spam. That new number could be a consumer with a legitimate purpose whose calls are not being answered because of this mislabeling. This leads to a guilty until proven innocent ecosystem that ultimately harms the consumer. Without Commission intervention, overblocking and mislabeling will further erode consumer confidence in voice service networks, despite the great efforts many in industry are making to mitigate and eliminate robocalls on their networks.

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* and *NOI*.

Respectfully submitted,

INCOMPAS

/s/ Christopher L. Shipley

Christopher L. Shipley
Executive Director of Public Policy

Taylor Abshire*
** Legal Intern Supervised by an Attorney*

[20] *See Best Practices Relating to Redress Requests*, USTelecom Blocking and Labeling Working Group (2023), *available at* https://ustelecom.org/wp-content/uploads/2021/08/USTelecom-Blocking-and-Labeling-WG-Best-Practices-Relating-to-Redress-Requests-8-18-21.pdf.

INCOMPAS
1100 G Street NW
Suite 800
Washington, D.C. 20005
(202) 872-5746
cshipley@incompas.org

August 9, 2023