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

In the Matter of	)	
	)	
Improving the Effectiveness of the Robocall Mitigation Database	)	WC Docket No. 24-213
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	

COMMENTS OF INCOMPAS AND THE CLOUD COMMUNICATIONS ALLIANCE

INCOMPAS
Christopher L. Shipley
Executive Director of Public Policy
1100 G Street NW, Suite 800
Washington, DC 20005
cshipley@incompas.org

CLOUD COMMUNICATIONS ALLIANCE
Joe Marion
President
131 NW 1st Avenue
Delray Beach, FL 33444
(561) 232-3891

October 9, 2026

TABLE OF CONTENTS

I. INTRODUCTION AND SUMMARY……..……..….4

II. THE RMD SHOULD SERVE AS THE SINGLE COMMISSION-VERIFIED SOURCE OF KYUP INFORMATION, AND DOWNSTREAM PROVIDERS SHOULD BE ENTITLED TO RELY ON IT……..……...……...6

A. Collecting KYUP Information in the RMD Should Replace, Not Duplicate, Bilateral Collection…….6

B. Downstream Providers Should Be Able to Treat the RMD as Authoritative…...…..7

C. Bureau Pre-Publication Review Should Include a Shot Clock and an Opportunity to Cure ……..……..8

D. The Commission Should Dedicate Resources Commensurate With Its Priorities….9

III. THE COMMISSION SHOULD KEEP RMD OBLIGATIONS WITH THE PROVIDERS THAT FURNISH PSTN INTERCONNECTION AND ADOPT A CLEAR FUNCTIONAL TEST BEFORE EXTENDING THEM FURTHER…….9

A. A Functional Test Should Place RMD Obligations on the Entity That Provides the PSTN Connection…….10

B. The Further Notice's Reading Is Overbroad and Lacks a Limiting Principle……..12

C. The Further Notice Does Not Provide Adequate Notice, and Any New Interpretation Should Apply Only Prospectively……..12

D. Extending RMD Obligations to Businesses That Use Voice Service Would Not Advance the Commission's Goals……13

IV. FILING CONTENT SHOULD BE CLEAR AND ADMINISTRABLE, AND SENSITIVE BUSINESS INFORMATION SHOULD REMAIN NON-PUBLIC…...….14

A. Codified Filing Categories and Structured Data Will Reduce Inadvertent Errors…14

B. Third-Party and Call Analytics Disclosures Will Improve Transparency and Should Remain Non-Public……...15

C. Registered Agent and Ownership Requirements Should Be Harmonized With Existing Filings and Scaled to Risk……..16

D. Numbering Resources Information Is Competitively Sensitive and Should Not Be Publicly Disclosed……....16

E. Certification Should Be Tied to Knowledge and Materiality……...…17

F. The Commission Should Adopt the Simplified Traceback Certification and the Temporary SPC-Token Exemption……...…17

V. THE COMMISSION SHOULD PRESERVE THE FLEXIBLE "REASONABLE STEPS" STANDARD RATHER THAN IMPOSE A HINDSIGHT "EFFECTIVENESS" TEST……18
A. An "Affirmative, Effective Measures" Standard Would Invite After-the-Fact Findings Against Goot-Faith Programs……18
B. Robocall Mitigation Plans Should Be Risk-Based, and Detailed Plans Should Be Eligible for Confidential Treatment……..19

VI. UPDATE AND RECERTIFICATION RULES SHOULD REDUCE BURDENS WHILE KEEPING THE DATABASE ACCURATE…….....19

VII. SCREENING TOOLS SHOULD TARGET BAD ACTORS WITHOUT CREATING BARRIERS TO ENTRY FOR LEGITIMATE COMPETITIVE PROVIDERS……..20
A. A Universal Letter of Credit, Bond, or Audited Financial Requirement Would Burden Legitimate Entrants More Than Bad Actors……20
B. The Commission Should Scrutinize Nominal U.S. Operations and Extend Foreign Adversary Control Attestations to RMD Filers……....21

VIII. REMOVAL SHOULD FOLLOW CLEAR, CULPABILITY-BASED STANDARDS AND FAIR PROCEDURES……..21
A. The Commission Should Codify Causes for Removal, but Narrow Several of Them…….21
B. Removal Procedures Should Preserve a Meaningful Opportunity to Cure and Respond…….22
C. Suspensions Should Prompt Timely Cures, Not Downstream Policing……...23
D. Customer Notice and Compliance Timing Should Protect Legitimate Customers……..…24

IX. MEASURES TO KEEP REMOVED BAD ACTORS OUT SHOULD BE COMMISSION-RUN, EVIDENCE-BASED, AND PROTECT LEGITIMATE TRANSACTION……...24

X. DOWNSTREAM OBLIGATIONS, SCOPE EXPANSIONS, AND AUDITS SHOULD REMAIN TARGETED AND WORKABLE……25

XI. THE COMMISSION SHOULD PROVIDE ADEQUATE IMPLEMENTATON TIME AND FULLY ASSESS THE COMBINED COSTS OF ITS PROPOSALS……26

XII. CONCLUSION……..27

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

In the Matter of	)	
	)	
Improving the Effectiveness of the Robocall Mitigation Database	)	WC Docket No. 24-213
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	

COMMENTS OF INCOMPAS AND
THE CLOUD COMMUNICATIONS ALLIANCE

INCOMPAS and the Cloud Communications Alliance ("Alliance" or, together, the "joint associations"), by its undersigned counsel, respectfully submit these comments in response to the Federal Communications Commission's ("Commission" or "FCC") *Further Notice of Proposed Rulemaking* proposing reforms to improve the effectiveness of the Robocall Mitigation Database ("RMD").[1]

I. INTRODUCTION AND SUMMARY

INCOMPAS and the Alliance members offering voice services universally participate in the RMD and support the Commission's efforts to remove bad actors from the voice ecosystem.[2]

[1] *Improving the Effectiveness of the Robocall Mitigation Database; Call Authentication Trust Anchor; Advanced Methods to Target and Eliminate Unlawful Robocalls*, WC Docket Nos. 24-213, 17-97, CG Docket No. 17-59, Further Notice of Proposed Rulemaking, FCC 26-49 (rel. July 23, 2026) ("*Further Notice*").

[2] *See* Joint Comments of INCOMPAS and the Cloud Communications Alliance, WC Docket No. 24-213, MD Docket No. 10-234, at 2 (filed Oct. 15, 2024) ("INCOMPAS-CCA 2024 RMD Comments"); Letter from Christopher L. Shipley, Executive Director of Public Policy, INCOMPAS, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 24-213, MD Docket No. 10-234, at 1 (filed Jan. 6, 2025) ("INCOMPAS 2025 RMD *Ex Parte*").

Throughout this proceeding, INCOMPAS and the Alliance have supported a database that is accurate and meaningful, while urging the Commission to provide clear filing requirements, preserve providers' flexibility to mitigate illegal calls in the ways that work best on their networks, and retain oversight of the RMD rather than shifting that role to industry.

The *Further Notice* rightly places several key functions with the Commission. Under its proposals, the Wireline Competition Bureau would screen filings before they are published, the Commission would develop technical tools to detect deficient and duplicative filings, and the Enforcement Bureau would decide whether a provider is removed. The joint associations support this Commission-centered oversight model and urge the Commission to complete it by making the RMD the authoritative source of the business information it is proposing that providers collect about their upstream providers in the companion Know Your Upstream Provider ("KYUP") proceeding.[3] Downstream providers should not also be required to collect, verify, and police the same information bilaterally.

The joint associations' positions in these comments rest on three principles. First, obligations should be proportionate to the risk they address and should preserve the flexibility the Commission has long recognized providers need to respond to evolving threats. Second, the Commission, not providers, should decide who may participate in the voice ecosystem. Third, enforcement should be culpability-based, with notice, an opportunity to cure, and a safe harbor for providers that rely in good faith on the Commission's own determinations.

Applying those principles, INCOMPAS and the Alliance urge the Commission to: (1) make the RMD the single, Commission-verified source of KYUP information and allow

[3] *Call Authentication Trust Anchor; Advanced Methods to Target and Eliminate Unlawful Robocalls*, WC Docket No. 17-97, CG Docket No. 17-59, Further Notice of Proposed Rulemaking, FCC 26-32 (rel. May 21, 2026) ("*KYUP Further Notice*").

downstream providers to rely on it; (2) adopt a clear, functional test that keeps RMD obligations with the providers that furnish PSTN interconnection; (3) adopt clear filing requirements while protecting sensitive business information; (4) preserve the flexible "reasonable steps" mitigation standard; (5) adopt update and recertification rules that reduce burdens; (6) target screening tools at bad actors without creating barriers to entry; (7) adopt clear, culpability-based removal standards and fair procedures; (8) keep the process of excluding removed bad actors under Commission control; (9) keep downstream obligations, scope expansions, and audits targeted and workable; and (10) provide adequate implementation time and a complete assessment of costs.

II. THE RMD SHOULD SERVE AS THE SINGLE, COMMISSION-VERIFIED SOURCE OF KYUP INFORMATION, AND DOWNSTREAM PROVIDERS SHOULD BE ENTITLED TO RELY ON IT

A. Collecting KYUP Information in the RMD Should Replace, Not Duplicate, Bilateral Collection

The *Further Notice* proposes to require RMD filers to submit additional business information, much of which overlaps with the information the *KYUP Further Notice* would require downstream providers to collect from each of their directly connected upstream providers.[4] INCOMPAS and the Alliance support collecting this type of information in the RMD, but as a substitute for the bilateral collection proposed in the KYUP proceeding, not in addition to it.

The *Further Notice* describes the incremental cost of collecting this information in the RMD as "negligible" because providers would already be compiling it for downstream providers

[4] *Further Notice* at para. 50; *see KYUP Further Notice* at paras. 15–25.

under the KYUP proposals.[5] The joint associations question that assessment, but the observation itself points to the better approach. Collecting the information once, centrally, and having the Commission verify it would avoid thousands of redundant bilateral reviews and would be far less burdensome for providers of every size. Every voice service provider must already file in the RMD, which makes it a universally available repository for this information.[6]

A Commission-verified RMD also resolves the delegation concerns INCOMPAS and the Alliance raised in the KYUP proceeding. As explained there, the KYUP proposals would require providers to assess their competitors' regulatory compliance and decide whether to cut off their service, without any Commission involvement in that decision.[7] When the Commission collects and verifies the information and decides who may appear in the RMD, the government, not private competitors, retains decision-making authority.

B. Downstream Providers Should Be Able to Treat the RMD as Authoritative

The *Further Notice* asks whether downstream providers should be required to conduct their own due diligence to determine whether an upstream provider is an alter ego of a provider that has been removed from the RMD.[8] The joint associations oppose that requirement. Identifying alter egos is an investigative function that belongs with the Commission, which has access to the filing history, FCC Registration Numbers, and enforcement records needed to

---

[5] *Further Notice* at para. 50.

[6] *See* Joint Comments of INCOMPAS and the Cloud Communications Alliance, WC Docket No. 17-97, CG Docket No. 17-59, at 10–11 (filed Aug. 10, 2026) ("INCOMPAS-CCA KYUP Comments").

[7] *Id.* at 7–9 (discussing *Carter v. Carter Coal Co.*, 298 U.S. 238 (1936), and *FCC v. Consumers' Research*, 606 U.S. 656 (2025)).

[8] *Further Notice* at para. 116.

perform it. Downstream providers have none of those tools with respect to entities with which they may have no relationship.

On the other hand, INCOMPAS and the Alliance support the *Further Notice's* proposals to include Operating Company Numbers, FCC Registration Numbers, prior business names, and principal identifiers in removal orders, and to make a downloadable list of removed providers available.[9] These measures give downstream providers what they need to comply with the call-refusal rules mechanically and reliably. The Commission should pair them with an express safe harbor: a provider that accepts traffic from an upstream provider whose filing is published and active in the RMD at the time of the call complies with section 64.6305(g) of the Commission's rules and with any KYUP information-collection and verification obligations that the RMD covers.[10]

C. Bureau Pre-Publication Review Should Include a Shot Clock and an Opportunity to Cure

The joint associations support the proposal to have the Wireline Competition Bureau review filings before publication, so that a filing "appears" in the RMD only once it has been accepted.[11] This is the Commission performing the gatekeeping function itself, which is preferable to relying on downstream providers to identify deficient filings after the fact. To ensure that pre-publication review does not unnecessarily delay legitimate providers, the Commission should adopt a shot clock for acting on filings placed in pending status; provide notice and an opportunity to cure ministerial or inadvertent errors before rejecting a filing; and

---

[9] *Id.*

[10] 47 C.F.R. § 64.6305(g); *see Further Notice* at para. 111.

[11] *Further Notice* at para. 69.

establish a clear path for new entrants so that pending status does not become a *de facto* barrier to entering the market.

D. The Commission Should Dedicate Resources Commensurate With Its Priorities

The *Further Notice* seeks comment on the resources needed to implement its proposals.[12] The Commission has repeatedly identified fighting illegal calls as its top consumer protection priority, and it should staff the RMD accordingly or seek appropriations from Congress for that purpose. Fee and bond revenue cannot fill that gap. As INCOMPAS and the Alliance have previously pointed out, application fees collected under section 8 of the Communications Act are deposited in the general fund of the U.S. Treasury and cannot be used to fund RMD administration absent new legislation.[13]

III. THE COMMISSION SHOULD KEEP RMD OBLIGATIONS WITH THE PROVIDERS THAT FURNISH PSTN INTERCONNECTION AND ADOPT A CLEAR FUNCTIONAL TEST BEFORE EXTENDING THEM FURTHER

INCOMPAS and the Alliance strongly support reasonable efforts to protect consumers and prevent illegal robocalls, and its members universally participate in the RMD. The *Further Notice*, however, proposes to define "voice service" to encompass PBXs, dialing platforms, cloud and over-the-top services, call centers, value-added service providers, and telephone number service providers.[14] A reading this broad would be neither a reasonable nor an effective means of achieving the Commission's goals. Furthermore, it risks sweeping in businesses and platforms that use voice service rather than provide it, burdening legitimate services without

[12] *Id.* at paras. 121–123.

[13] 47 U.S.C. § 158(e); *see* INCOMPAS-CCA 2024 RMD Comments at 4–5.

[14] *See Further Notice* at paras. 10–14.

deterring the bad actors responsible for illegal robocalls. The Commission should make clear that this is not its intent and should adopt a clear, functional test that places RMD obligations where they belong.

A. A Functional Test Should Place RMD Obligations on the Entity That Provides the PSTN Connection

INCOMPAS has previously urged the Commission to adopt a simplified, technology-neutral definition of "voice service provider" that is aligned to functional roles in the call path, rather than to specific technologies or regulatory classifications.[15] A functional definition cuts in both directions. An entity that performs provider functions, such as transmitting, reselling, or routing third-party traffic, should be treated as a voice service provider regardless of the technology it uses or the label it adopts, closing the gaps that bad actors exploit by structuring their operations to fall outside current definitions. An entity that uses voice service to place its own calls, or that supports its customers' calls over a PSTN connection furnished by someone else, is an end user of voice service, not a provider of it.

Applying that principle, RMD filing, call authentication, and traceback obligations belong with the voice service provider that furnishes the PSTN interconnection. In nearly every case, the end user has a direct relationship with that provider, and that provider is already registered in the RMD and subject to the Commission's rules. The marketplace generally reflects two arrangements. In the first, the voice service provider that supplies the PSTN connection also supplies or integrates the cloud PBX, contact center, or other application. A government agency with a long-term contract for PSTN service from a national carrier, for example, may add a cloud PBX to that service. The carrier is registered in the RMD and covers

[15] Comments of INCOMPAS, CG Docket Nos. 17-59, 02-278, at 15–16 (filed June 25, 2026) ("INCOMPAS KYC Comments").

the agency's PSTN activity; neither the agency nor the cloud PBX provider should be required to file simply because the agency's PSTN service now runs through a cloud application. In the second, the end user connects PSTN service from one or more voice service providers to its own PBX, dialing platform, contact center, or other application, using, for example, one provider's PSTN service with its PBX and another's with its contact center. Each voice service provider remains responsible for the PSTN service it provides. Offering a platform that a customer can connect to PSTN service does not, by itself, create a separate RMD filing obligation for the platform or its customer.

The Commission's traceback framework confirms that this is the correct allocation. Cloud services and calling tools cannot facilitate a traceback, even when connected to PSTN service. Traceback runs through the voice service provider that has the PSTN relationship with the customer; that provider holds the customer relationship and the call records, and bears the obligation to respond. Requiring platforms to file in the RMD would add entries to the RMD without adding a single traceback point of contact.

The Commission should therefore confirm that an entity is an end user of voice service, and not a voice service provider, where the PSTN interconnection used with its service is furnished by a separate voice service provider that is subject to the Commission's RMD, call authentication, and traceback rules. At a minimum, that test should encompass: (1) platforms and applications for which a voice service provider bundles the PSTN service; (2) platforms and applications that customers connect to PSTN service obtained from their own voice service providers; and (3) services where their customers (i) cannot themselves originate, receive, or participate in interconnected calls; or (ii) can only request that the entity place a call, which the entity itself initiates and conducts as part of a broader service; and (iii) the entity obtains the

voice service it uses as an input to that service from a voice service provider subject to the Commission's RMD, call authentication, and traceback rules. This test addresses entities that use or enable PSTN service furnished by others. Entities that sell PSTN calling service to their own customers, including on a resale basis, remain voice service providers under the Commission's existing rules.

B. The *Further Notice's* Reading Is Overbroad and Lacks a Limiting Principle

By the Commission's own criteria, value-added service providers and similar callers are not voice service providers, because they do not themselves provide interconnection with the PSTN. They obtain that interconnection as customers of voice service providers that are already subject to the Commission's RMD, call authentication, and traceback rules. The *Further Notice's* suggestion that "interconnected" may be read with extraordinary breadth, and that "indirect" furnishing of service may suffice,[16] underscores the problem. Under that reading, virtually any business able to place a call that ultimately reaches the PSTN through a third-party voice service provider could itself become a voice service provider. The *Further Notice* identifies no limiting principle that would prevent that result, and an expansion of the Commission's regulatory reach of that magnitude would raise serious questions as to whether Congress authorized it.[17]

C. The *Further Notice* Does Not Provide Adequate Notice, and Any New Interpretation Should Apply Only Prospectively

The *Further Notice* does not identify with reasonable specificity which entities would be covered. Its discussion of undefined terms such as "service," "furnish," "interconnected," and

[16] *See Further Notice* at para. 12.

[17] *See West Virginia v. EPA*, 597 U.S. 697 (2022).

"enables," together with the suggestion that "indirect" furnishing may suffice, leaves affected businesses unable to determine whether they are subject to the proposal, and therefore unable to comment meaningfully on it as the Administrative Procedure Act requires.[18] Because the *Further Notice* does not identify the covered entities with reasonable specificity, any final rule that materially departs from its specific proposals would not be a logical outgrowth of the *Further Notice* and would require further notice and an opportunity for comment.

Moreover, although the *Further Notice* characterizes its proposal as a clarification rather than an expansion of the entities required to certify in the RMD, it would in substance impose new obligations on entities that have reasonably and in good faith understood themselves to be end users or value-added service providers under the existing rules. Any new interpretation should therefore apply prospectively only, following a reasonable transition period, and should not form the basis for enforcement for conduct predating its adoption.

D. Extending RMD Obligations to Businesses That Use Voice Service Would Not Advance the Commission's Goals

Even if the Commission had the authority to extend RMD obligations to callers, doing so would be unreasonable. Businesses that use voice calling as one feature of a broader product are in the business of using the PSTN, not providing access to it. They cannot reasonably be expected to track, or to commit resources to complying with, complex and evolving requirements designed for companies that provide interconnection to the PSTN. Imposing those requirements could slow the development of innovative consumer services, including emerging automated and AI-enabled tools, without any corresponding benefit to consumers.

[18] *See* 5 U.S.C. § 553(b)–(c).

The Commission need not take that step to achieve its goals. Its existing framework already reaches these calls through the voice service providers that carry them. Those providers are subject to the Commission's know-your-customer ("KYC") obligations, which the Commission is refining in a parallel proceeding,[19] as well as its traceback and call authentication rules. Responsible businesses that offer calling-enabled features also deploy their own safeguards, such as acceptable use policies, technical restrictions on prohibited calls, call-pattern analytics, rate limits, and customer verification. Upstream KYC and traceback obligations, combined with these measures, are a more targeted and effective means of deterring bad actors than extending RMD obligations to every business that builds voice features into its products. That approach is consistent with the joint associations' view that KYC practices are one layer of a multi-layered approach to fraud prevention that also includes traffic monitoring, traceback, and call authentication.[20] More broadly, definitions as unsettled as those in the *Further Notice* weigh against layering new prescriptive, classification-dependent obligations on top of them.[21]

IV. FILING CONTENT SHOULD BE CLEAR AND ADMINISTRABLE, AND SENSITIVE BUSINESS INFORMATION SHOULD REMAIN NON-PUBLIC

A. Codified Filing Categories and Structured Data Will Reduce Inadvertent Errors

INCOMPAS and the Alliance support the *Further Notice's* proposals to codify the five categories of information that RMD filings must contain, to collect structured information

[19] *See Advanced Methods to Target and Eliminate Unlawful Robocalls; Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket Nos. 17-59, 02-278, Further Notice of Proposed Rulemaking, FCC 26-27 (rel. May 1, 2026).

[20] INCOMPAS KYC Comments at 2–3.

[21] *See* INCOMPAS-CCA KYUP Comments at 22–23.

through the RMD form itself, and to require that uploaded robocall mitigation plans be submitted as machine-readable PDFs.[22] These changes respond directly to the associations' long-standing concern that the primary problem with RMD filings has been a lack of clarity and guidance about what a compliant filing must contain, which exposes good-faith providers to inadvertent errors.[23] For the same reason, INCOMPAS and the Alliance support resolving the contradiction between the two existing certifications regarding prior actions and investigations, and simplifying the related description requirements.[24]

B. Third-Party and Call Analytics Disclosures Will Improve Transparency and Should Remain Non-Public

INCOMPAS and the Alliance support requiring filers to disclose whether they rely on third parties for call analytics, call signing, KYC and KYUP functions, and RMD filing, and supports the *Further Notice's* proposal to keep that vendor information non-public.[25] Requiring providers to describe their call analytics measures will also improve transparency about how traffic is blocked and labeled across the ecosystem.[26] The blocking and mislabeling of legitimate traffic by analytics companies and larger providers has been a long-standing concern for competitive providers and their customers.[27]

---

[22] *Further Notice* at paras. 18, 60–61.

[23] INCOMPAS-CCA 2024 RMD Comments at 2–3; INCOMPAS 2025 RMD *Ex Parte* at 1–2.

[24] *Further Notice* at paras. 33–37.

[25] *Id.* at paras. 38, 63.

[26] *Id.* at para. 57.

[27] *See* INCOMPAS KYC Comments at 12.

C. Registered Agent and Ownership Requirements Should Be Harmonized With Existing Filings and Scaled to Risk

The joint associations support requiring filers to designate a U.S. registered agent, provided the requirement is harmonized with the agent-for-service designation in FCC Form 499 so that providers can designate a single agent for both purposes.[28] Any requirements to submit expanded ownership and identity information, such as government identification, photographs of principals, citizenship, and the identities of all owners holding 10 percent or more, should be scaled to risk, and all personal identifiers should be kept non-public.[29] Collecting this information from every filer and exposing it publicly would create the very data-security risks the Commission has said it intends to avoid. Providers should also be able to incorporate information already submitted through Form 499 and CORES by reference rather than re-entering it.

D. Numbering Resource Information Is Competitively Sensitive and Should Not Be Publicly Disclosed

INCOMPAS and the Alliance oppose public disclosure of providers' number blocks and reseller customer lists.[30] This information is competitively sensitive, and publishing it in a database that any party can search would give competitors insight into providers' customer relationships and network resources without any corresponding benefit for robocall mitigation. Any numbering information the Commission collects should be treated as confidential.

---

[28] *Further Notice* at para. 43.

[29] *Id.* at paras. 42, 50, 62–63.

[30] *Id.* at para. 48.

E. Certifications Should Be Tied to Knowledge and Materiality

The *Further Notice* proposes several new certifications.[31] The joint associations support the proposed STIR/SHAKEN attestation certification once the Commission has adopted clear criteria for each attestation level, as INCOMPAS and the Alliance urged in the KYUP proceeding.[32] INCOMPAS and the Alliance also support the proposed lack-of-candor certification, if it is limited to material statements the provider knew or should have known were false and providers have an opportunity to correct inadvertent errors.

The joint associations oppose, as drafted, the proposed certification that the filer complies with all applicable rules governing illegal calls.[33] Because an invalid certification is itself a ground for removal, this certification would convert any rule violation, however minor or inadvertent, into a basis for removing a provider from the RMD and cutting off its traffic. At a minimum, the certification should be limited to knowing noncompliance.

F. The Commission Should Adopt the Simplified Traceback Certifications and the Temporary SPC-Token Exemption

The joint associations support the proposed simplified certifications regarding 24-hour traceback responses and cooperation with the Industry Traceback Group ("ITG").[34] The two groups also support encouraging participation in the ITG's automated traceback platform, but the Commission should provide cost relief for small providers and preserve a non-automated option for providers for which automated participation is impractical.

---

[31] *Id.* at paras. 20–22.

[32] INCOMPAS-CCA KYUP Comments at 17–18.

[33] *Further Notice* at para. 22.

[34] *Id.* at paras. 23–24.

INCOMPAS and the Alliance strongly support the proposed temporary exemption for providers that have applied for, but not yet received, an SPC token.[35] This exemption resolves a real conflict for new competitive entrants, which cannot obtain a token without an RMD filing and cannot complete a compliant RMD filing without a token. The duration of the exemption should reflect actual Governance Authority processing times, and extensions should be available where delays are outside the provider's control.

V. THE COMMISSION SHOULD PRESERVE THE FLEXIBLE "REASONABLE STEPS" STANDARD RATHER THAN IMPOSE A HINDSIGHT "EFFECTIVENESS" TEST

A. An "Affirmative, Effective Measures" Standard Would Invite After-the-Fact Findings Against Good-Faith Programs

The *Further Notice* proposes to replace the current requirement that providers take "reasonable steps" to mitigate illegal robocalls with a requirement that they implement "affirmative, effective measures."[36] The joint associations oppose this change. The Commission has repeatedly endorsed a flexible, outcome-based approach to mitigation that allows providers to determine what works best on their networks and to adapt to changing calling patterns.[37] An "effectiveness" standard would invite after-the-fact findings that a good-faith mitigation program was inadequate simply because some illegal calls were not stopped.

---

[35] *Id.* at paras. 30–32.

[36] *Id.* at para. 53.

[37] *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Fourth Report and Order, 35 FCC Rcd 15221, para. 34 (2020); *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, FCC 23-37, para. 53 (rel. May 19, 2023); *see also* INCOMPAS KYC Comments at 1–2.

If the Commission nonetheless adopts the new standard, it should provide safe-harbor guidance on what qualifies as "affirmative" and "effective," and it should confirm that the fact that an individual illegal call reached consumers does not, by itself, demonstrate that a provider's program is ineffective.

B. Robocall Mitigation Plans Should Be Risk-Based, and Detailed Plans Should Be Eligible for Confidential Treatment

INCOMPAS and the Alliance support a risk-based approach to the level of detail required in robocall mitigation plans, with plans focused on describing the practices a provider uses beyond any baseline the Commission adopts.[38] The joint associations oppose requiring providers to report mandatory effectiveness metrics, which would not translate meaningfully across providers with different network architectures, customer bases, and traffic profiles. The Commission should also recognize that highly detailed public mitigation plans risk giving bad actors a roadmap for evading the very measures those plans describe. Detailed plans should therefore be eligible for confidential treatment under the RMD Protective Order.

VI. UPDATE AND RECERTIFICATION RULES SHOULD REDUCE BURDENS WHILE KEEPING THE RMD ACCURATE

INCOMPAS and the Alliance support replacing the current requirement to update RMD filings within 10 business days of any change with a 30-day window for material changes, combined with annual recertification.[39] The joint associations oppose requiring more frequent affirmative recertifications, each of which could become a trigger for suspension. The two associations also support barring providers from deleting their filings while a Show Cause Order

[38] *Further Notice* at paras. 55–56.

[39] *Id.* at para. 64.

is pending, and supports creating an "inactive" status for providers that stop offering voice service or merge with another provider.[40]

With respect to annual recertification, INCOMPAS and the Alliance support a short grace period, direct notice to filers before the recertification deadline, and codifying that the filing fee is paid at recertification.[41] Our organizations continue to believe that the fee should be a one-time charge rather than a recurring one.[42] The joint associations opposes the proposal to have filings lapse automatically after one year.[43] Automatic lapse would create large numbers of technical violations, and the resulting downstream blocking would fall on legitimate customers who had no role in a missed deadline.

VII. SCREENING TOOLS SHOULD TARGET BAD ACTORS WITHOUT CREATING BARRIERS TO ENTRY FOR LEGITIMATE COMPETITIVE PROVIDERS

A. A Universal Letter of Credit, Bond, or Audited Financials Requirement Would Burden Legitimate Entrants More Than Bad Actors

The joint associations oppose requiring all RMD filers to obtain a letter of credit or bond or to submit audited financial statements.[44] Such a requirement would impose real costs and barriers to entry on small and new competitive providers, while well-funded bad actors could simply capitalize shell companies to satisfy it. If the Commission adopts any financial-assurance requirement, it should be limited to providers that exhibit some factors indicating a bond or letter

[40] *Id.* at para. 65.

[41] *Id.* at paras. 92–94.

[42] INCOMPAS-CCA 2024 RMD Comments at 5; INCOMPAS 2025 RMD *Ex Parte* at 2 n.4.

[43] *Further Notice* at para. 93.

[44] *Id.* at paras. 70–73.

of credit would be warranted, such as previous removal from the RMD. Any such financial-assurance requirement should be waived after a period of compliant operation and scaled to provider size. The Commission should also ensure that domestic providers do not bear obligations that the Commission cannot practically impose on, or enforce against, foreign filers.[45]

B. The Commission Should Scrutinize Nominal U.S. Operations and Extend Foreign Adversary Control Attestations to RMD Filers

The joint associations also supports closer scrutiny of filers whose U.S. presence is nominal.[46] Additional disclosures should be tied to specific risk indicators, such as a hosted server being the only U.S. presence, a shared address, or the absence of U.S. employees, rather than imposed on all domestic filers. INCOMPAS and the Alliance also support extending Foreign Adversary Control attestations to RMD filers, which closes a meaningful national security gap for providers that do not otherwise hold authorizations requiring such attestations.[47]

VIII. REMOVAL SHOULD FOLLOW CLEAR, CULPABILITY-BASED STANDARDS AND FAIR PROCEDURES

A. The Commission Should Codify Causes for Removal, but Narrow Several of Them

INCOMPAS and the Alliance support codifying the causes for removal from the RMD, which will give providers clear notice of the conduct that can result in removal.[48] Several of the proposed causes, however, should be narrowed. Non-material "deficient" filings should never

[45] *See* INCOMPAS-CCA 2024 RMD Comments at 6.

[46] *Further Notice* at paras. 15, 47.

[47] *Id.* at para. 78.

[48] *Id.* at paras. 80–81.

lead to removal without a completed cure process. With respect to "enabling the transmission of illegal calls," the two groups oppose a negligence standard and urges the Commission to adopt a knowing-or-reckless standard, consistent with the culpability-based approach INCOMPAS and the alliance have advocated for throughout these proceedings.[49]

"Repeated appearance in tracebacks" should also not be a stand-alone cause for removal for intermediate and wholesale providers, which appear in tracebacks by the nature of their role in the call path. This cause should be limited to originating providers. Removal for accepting calls from a prohibited provider should be subject to the safe harbor for good-faith reliance on the RMD described *supra* in Section II. Removal for "inadequate robocall mitigation measures" should await the clear guidance described *supra* in Section V. Removal for lack of candor should require a material misstatement and either an intent to deceive or a failure to correct after notice. Finally, a single missed traceback request should not warrant removal; the Commission should instead apply a threshold of repeated failures within a defined period and distinguish late responses from non-responses.

B. Removal Procedures Should Preserve a Meaningful Opportunity to Cure and Respond

The joint associations supports the proposed three-step removal process for deficient filings, with a minimum cure period.[50] INCOMPAS and the Alliance oppose the premise that every other cause for removal is "willful by definition," and opposes shortening the response window in the two-step process from 10 days to five.[51] Five days is not enough time for a

[49] *See* INCOMPAS-CCA KYUP Comments at 23–24; INCOMPAS-CCA 2024 RMD Comments at 5; *see also* 47 U.S.C. § 503(b)(2)(E).

[50] *Further Notice* at paras. 82–83.

[51] *Id.* at para. 84.

provider to cure a problem, respond to the Commission, and notify its customers. Any one-step removal process should be limited to a narrow set of egregious causes, such as impersonation of another provider, national security findings, and final enforcement orders, and should be followed by prompt post-removal review.[52] INCOMPAS and the Alliance can support a limit on cure opportunities if it applies only to material violations.[53]

C. Suspensions Should Prompt Timely Cures, Not Downstream Policing

The joint associations support a visible "past due" status for providers that miss a recertification deadline, accompanied by reminders, a cure period, and automatic reinstatement once the provider recertifies and pays the required fee.[54] INCOMPAS and the Alliance oppose giving a suspension the same downstream blocking effect as a removal, and opposes having suspensions trigger permissive blocking or "enhanced due diligence" by downstream providers.[55] Those measures would put providers back in the position of policing their competitors, which is precisely the role the two groups have urged the Commission not to assign to industry.[56] Instead, the two associations support the proposed "active," "suspended," and "removed" status indicators, which will make compliance straightforward for downstream providers.[57]

---

[52] *Id.* at para. 85.

[53] *Id.* at para. 86.

[54] *Id.* at paras. 87–91.

[55] *Id.* at para. 90.

[56] *See* INCOMPAS-CCA 2024 RMD Comments at 7; INCOMPAS KYC Comments at 12.

[57] *Further Notice* at para. 95.

D. Customer Notice and Compliance Timing Should Protect Legitimate Customers

The joint associations support requiring removed providers to notify their customers, with notice sequenced so that legitimate customers can migrate to another provider before traffic is cut off.[58] INCOMPAS and the Alliance also support replacing the fixed two-business-day deadline for downstream providers to stop accepting traffic with a default minimum period, combined with Enforcement Bureau discretion to extend it, particularly for large-scale removals like those in August 2025.[59] At the same time, the associations oppose requiring downstream providers to notify an upstream provider's customers, which would raise CPNI and competitive-sensitivity concerns.[60] Finally, a mandatory blocking order under section 64.1200(n) should not automatically trigger removal from the RMD without a separate process.[61]

IX. MEASURES TO KEEP REMOVED BAD ACTORS OUT SHOULD BE COMMISSION-RUN, EVIDENCE-BASED, AND PROTECT LEGITIMATE TRANSACTIONS

INCOMPAS and the Alliance support Commission efforts to detect alter egos of removed providers that attempt to re-enter the RMD.[62] Any rebuttable presumption that a new filer is an alter ego, however, should apply only to high-confidence matches, such as the same OCN, FRN, or principals, and not to shared vendors, shared office space, or similar business names, all of

[58] *Id.* at para. 96.

[59] *Id.* at paras. 113–115; *see Robocall Mitigation Database Filers*, Order, EB-TCD-25-00038590, DA 25-737 (rel. Aug. 25, 2025).

[60] *Further Notice* at para. 97.

[61] *See* 47 C.F.R. § 64.1200(n).

[62] *Further Notice* at paras. 99–100.

which are common among legitimate providers. Bona fide, arm's-length acquisitions of or by previously removed entities should also have a clear path forward. The two associations support codifying the criteria and procedures for reinstatement, which will give removed providers that have corrected their conduct a transparent path back into the RMD.[63]

INCOMPAS and the Alliance support time-limited participation bars for egregious or repeated misconduct, provided they are imposed only after notice, an opportunity to be heard, and an evidentiary hearing where material facts are disputed.[64] Bars should not extend to consultants, counsel, or filing agents absent a finding that they knew of the misconduct. The joint associations opposes automatic consequences for a removed provider's Section 214 authorizations, numbering access, or SPC token.[65] Any such consequences should proceed under the review procedures that govern each authorization, with the Commission making the relevant determinations.

X. DOWNSTREAM OBLIGATIONS, SCOPE EXPANSIONS, AND AUDITS SHOULD REMAIN TARGETED AND WORKABLE

INCOMPAS and the Alliance support establishing a minimum frequency for downstream providers to check the RMD, provided the obligation can be satisfied through the RMD's API or CSV download, is scaled for small providers, and is accompanied by a reasonable implementation period.[66] Before extending call-refusal obligations to all voice calls, including

[63] *Id.* at para. 101.

[64] *Id.* at paras. 102–107.

[65] *Id.* at paras. 108–110, 119.

[66] *Id.* at para. 112.

calls that do not use NANP resources, the Commission should develop a record on the operational effects on lawful international wholesale traffic.[67]

The joint associations oppose requiring or permitting providers to block text traffic based on a provider's RMD status.[68] Messaging is a separate ecosystem with its own governance structures, and it is already affected by competitive distortions from gatekeeper-controlled registries and vetting arrangements.[69] The Commission's authority to extend RMD-based blocking to messaging is also doubtful. Finally, the two associations support targeted and for-cause audits, including audits of reinstated providers, but opposes random audits of all filers.[70] Any associated record retention obligation should align with the four-year period discussed in the Commission's KYC proceeding.[71]

XI. THE COMMISSION SHOULD PROVIDE ADEQUATE IMPLEMENTATION TIME AND FULLY ASSESS THE COMBINED COSTS OF ITS PROPOSALS

The joint associations support applying new filing content requirements at the next annual recertification after the Commission's systems are ready to accept them.[72] For new substantive obligations, the Commission should provide at least 12 months following OMB

[67] *Id.* at para. 117.

[68] *Id.* at para. 118.

[69] *See* INCOMPAS KYC Comments at 13.

[70] *Further Notice* at para. 120.

[71] *See* INCOMPAS KYC Comments at 10.

[72] *Further Notice* at para. 129.

approval, so that providers, particularly smaller competitive providers, have time to make the necessary system changes, train staff, and inform customers.[73]

In assessing costs and benefits, the Commission should not assume that good-faith providers already maintain all of the newly required information, or that the costs of the RMD proposals are "negligible" because providers would incur them anyway under the KYUP proposals.[74] Neither set of costs can be justified by assuming the other. The Commission should assess the combined costs of the RMD and KYUP proposals, which further supports collecting the relevant information once, in the RMD, as described above.

XII. CONCLUSION

INCOMPAS and the Alliance share the Commission's goal of removing bad actors from the voice ecosystem and protecting consumers from illegal calls. For the reasons stated herein, the joint associations urge the Commission to adopt its RMD reforms consistent with the recommendations in these comments, keeping oversight of the database with the Commission, preserving providers' flexibility, and ensuring that enforcement is grounded in culpability and fair process.

Respectfully submitted,

INCOMPAS

/s/ Christopher L. Shipley

Christopher L. Shipley
Executive Director of Public Policy
1100 G Street NW, Suite 800
Washington, DC 20005
cshipley@incompas.org

[73] *See* INCOMPAS KYC Comments at 16.

[74] *Further Notice* at paras. 50, 135–137.

CLOUD COMMUNICATIONS ALLIANCE

/s/ Joe Marion

Joe Marion
President
Cloud Communications Alliance
131 NW 1st Avenue
Delray Beach, FL 33444
(561) 232-3891

October 9, 2026