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
	)	
Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991	)	CG Docket No. 02-278

COMMENTS OF INCOMPAS

INCOMPAS, by its undersigned counsel, hereby submits these comments in response to the Federal Communication Commission's ("Commission") *Further Notice of Proposed Rulemaking* (*"Further Notice"* or *"FNPRM"*) proposing to enhance "Know Your Customer" ("KYC") requirements in order to prevent illegal calls from reaching American consumers.[1]

I. INTRODUCTION AND SUMMARY

INCOMPAS members include voice service providers that are active participants in the Commission's ongoing efforts to combat unlawful robocalls, illegal calling, and consumer fraud. Our members have undertaken their KYC efforts under the Commission's well-reasoned, flexible approach requiring providers to implement "affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls" and to exercise due diligence to help ensure its services are not used to originate illegal traffic.[2] In requiring

---

[1] *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) (*"Further Notice"* or *"FNPRM"*).

[2] *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Fourth Report and Order, 35 FCC Rcd 15221, para 36 (2020) ("*Fourth Report and Order*").

voice service providers to adopt measures to prevent new and renewing customers from using their network to originate calls, the Commission indicated that providers would have the "flexibility to determine what works best on their networks" and declined to adopt specific, defined steps.[3] The Commission affirmed this approach in a 2023 *Report and Order* that declined to further clarify the existing requirement finding that an "outcomes-based standard is most appropriate" and that flexibility would allow providers to "adapt to changing calling patterns."[4] INCOMPAS urges the Commission to preserve that flexibility as it evaluates the effectiveness of its current rules and considers further action in this area.

INCOMPAS members are committed to preventing robocalls and fraud and recognize the importance of KYC as one critical element of effective fraud prevention. KYC should be understood as one layer of a multi-faceted approach that also includes robust monitoring, traceback, and call authentication tools, such as STIR/SHAKEN. No single tool, including KYC, is sufficient on its own. Enhanced KYC requirements should not be viewed as a substitute for ongoing traffic monitoring, traceback participation, customer oversight, fraud analytics, and prompt remediation.[5] Bad actors are already satisfying KYC obligations through legitimately

---

[3] *Id*.

[4] *See 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 Ndo. 17-97, et al., FCC 23-37, para. 53 (rel. May 19, 2023) ("*Seventh Report and Order*").

[5] Some INCOMPAS members have adopted the term "Know Your Traffic" ("KYT") to describe robust, ongoing traffic monitoring programs that function as a critical complement to traditional KYC onboarding practices. Members have determined that effective onboarding alone does not solve the fraud problem. Sophisticated bad actors can and do satisfy KYC requirements through legitimately obtained credentials and information, only to begin sending illegal traffic once service is established. A strong KYT program enables providers to detect anomalous traffic patterns, identify indicia of illegal calling activity, and take rapid remedial action after service turn-up. KYT is a distinct but essential pillar of any comprehensive fraud prevention framework,

obtained information while continuing to use voice services to perpetrate fraud, which is why ongoing monitoring and rapid response to indicia of illegal calling remain essential complements to any KYC framework. INCOMPAS supports development of clear, enhanced KYC baseline expectations, provided that those expectations afford sufficient flexibility to account for the wide variety of services and customer types across the calling ecosystem, including consumers, sole proprietors, small businesses, enterprises, schools, governments, and other institutions. A one-size-fits-all approach would produce disparate outcomes, reduce KYC effectiveness, and ultimately fail to deliver meaningful fraud prevention.

INCOMPAS members suggest it is possible for the Commission to achieve these dual goals by first considering a safe harbor framework that would permit the agency to enumerate baseline KYC expectations while allowing providers the flexibility to evolve their requirements and respond to specific risk scenarios as fraudsters' tactics change. A baseline KYC framework should include requirements that providers obtain the following information prior to enabling services, with requisite verification and validation as appropriate:

- Name—with sufficient flexibility to accommodate individuals, businesses, government agencies, and institutional customers, verified against government or trusted third-party issued documentation (*i.e.* a corresponding Tax Identification Number, Business Registration Number, or government-issued personal identification);
- Address—including address validation; and
- Verified email address or alternate phone number—that can be used as a form of verification to support identity confirmation.

These baseline measures are consistent, in part, with the enhanced KYC requirements the Commission incorporated into its 2024 *Consent Decree* in the *Lingo Telecom* proceeding,

(cont.) and any safe harbor or compliance standards adopted in this proceeding should account for providers' ongoing traffic monitoring capabilities alongside their onboarding practices.

demonstrating that such standards are both achievable and already recognized by the Commission as appropriate benchmarks for voice service providers.[6] INCOMPAS also supports a risk-based overlay for higher-volume or higher-risk customers but urges the Commission to reject specific proposal in the *Further Notice* that are operationally unworkable or harmful to legitimate customers, including mandatory IP address collection, mandatory periodic re-verification, and the proposed $2,500 per-call penalty framework as currently structured.

With respect to the other proposals in the *Further Notice*, INCOMPAS recommends that the Commission:

- Ensure that any KYC framework is open, competitively neutral, and does not require use of proprietary or industry-controlled solutions that create barriers for competitive providers and new entrants;
- Reject the proposed expansion of downstream blocking authority tied to KYC noncompliance, which would harm competition and generate significant false-positive blocking of legitimate calls; and
- Strengthen information sharing frameworks, adopt a technology-neutral definition of "voice service provider," and provide an implementation timeline of at least twelve months following OMB approval.

INCOMPAS and its members stand ready to work with the Commission to achieve these goals, and these comments reflect that commitment to developing a KYC framework that effectively combats the threat of unlawful robocalls while preserving the flexibility and competition that benefit consumers and the broader communications ecosystem.

[6] *Lingo Telecom, LLC*, Order, File No.: EB-TCD-24 00036425, Consent Decree, Attachment 1, Operating Procedures (rel. August 21, 2024)

II. THE COMMISSION SHOULD ADOPT A SAFE HARBOR FRAMEWORK WITH FLEXIBLE BASELINE KYC REQUIREMENTS

A. A Safe Harbor Approach Best Balances Clarity and Flexibility

The *Further Notice* seeks comment on whether the Commission should issue baseline KYC guidance or expectations that act as a regulatory safe harbor, rather than adopting specific KYC requirements.[7] INCOMPAS and its members strongly support the safe harbor approach as it would permit the Commission to enumerate baseline KYC expectations while allowing providers the flexibility to evolve their requirements and respond to specific risk scenarios as fraudsters' tactics change. Providers that satisfy baseline safe harbor requirements would have a presumption of compliance, while providers that elect to implement alternative or supplementary measures could demonstrate compliance through the outcomes-based standard the Commission has long endorsed.[8]

Rigid, mandatory checklists can create a false sense of assurance with respect to compliance rather than actual fraud prevention. Further, adopting strict, static requirements raises the additional risk that rules become obsolete as bad actors adapt their practices faster than regulatory amendments can keep pace. By contrast, a safe harbor with flexible baseline requirements allows providers to allocate resources and scrutiny to actual threats, reducing real-world harm while providing the regulatory certainty that providers and the Commission need.

[7] *See Further Notice* at para. 26.

[8] *See Fourth Report Order* at para. 34; *Seventh Report and Order* at para. 53.

B. Baseline KYC Requirements Should Cover Core Identity Information with Appropriate Verification, But IP Addresses are an Inadequate Proxy for Customer Identity

The *Further Notice* proposes to require originating providers to obtain, at a minimum, the name, physical address, government-issued identification number, and an alternate telephone number of any new and renewing customer before granting access to services.[9] On name, address, and identification number, INCOMPAS supports the collection of this core identity information as baseline requirements, provided they are implemented with sufficient flexibility to accommodate the full range of customer types across the calling ecosystem.

The Commission should make clear that the name requirement can be satisfied by the legal name of an individual, business, government agency, or institution, and that government employees need not provide personal information when obtaining service on behalf of a government agency. Providers can verify that the name of the customer matches a corresponding tax IP, business registration number, or personal identification for smaller businesses. Addresses too should include validation, but the Commission should not broadly exclude shared office locations, as that restriction would impose unreasonable burdens on providers to verify whether a given address is a shared workspace — a determination that is frequently not possible without extensive investigation.

Regarding an alternate contact, INCOMPAS urges the Commission to accept either an alternate telephone number or a verified email address as equally acceptable options. Requiring an alternate telephone number in all cases would disadvantage legitimate customer categories who do not have one, including domestic violence survivors, foreign visitors such as temporary workers and students, and individuals who have recently let prior service lapse. A verified email

[9] *See Further Notice* at para. 9.

address serves the same authentication and contact functions as an alternate phone number and should be expressly recognized as an acceptable alternative.

The *Further Notice* proposes, for high-volume customers, to also require collection of the customer's IP address from which each call will be placed.[10] INCOMPAS suggests that it is not necessary to collect IP addresses as this is inconsistent with the modern hybrid work environment and 21st century travel and connectivity habits. Customers routinely make calls from multiple locations, devices, and networks. The IP address associated with a call at any given moment is an inadequate proxy for customer identity, changes constantly, can be obscured by VPNs and other routing technologies, and can reflect the address of a shared network or infrastructure provider rather than the customer itself. Collecting IP addresses would impose significant operational burdens, raise substantial privacy concerns, generate data of limited investigative value, and should be withdrawn.

C. Baseline Requirements Should Be Supplemented by Risk-Based and Proportional Approaches

INCOMPAS supports the *Further Notice's* recognition that enhanced KYC requirements should include risk-based approaches that require higher levels of scrutiny for certain customers including high-volume customers.[11] Risk-based approaches enable providers to allocate resources and scrutiny to actual threats, reducing real-world harm while avoiding the over-collection of information that raises privacy concerns and burdens legitimate customers. From INCOMPAS members' experience, static rules will not keep pace with fraudsters. Providers

[10] *Id*. at para. 9 (proposing to require collection of the customer's IP address from which each call will be placed for high-volume customers).

[11] *Id*. at para. 13.

must retain flexibility to adopt different forms of validation, verification, and heightened scrutiny to respond to evolving threats. The *Further Notice* asks whether the Commission should consider a tiered approach where KYC requirements become more stringent for high-volume callers or callers engaged in certain traffic patterns.[12] INCOMPAS supports a risk-tiered approach as part of a safe harbor framework, provided that the Commission defines "high-volume" thresholds with sufficient clarity to give providers workable compliance guidance, and that smaller providers serving primarily low-volume consumer customers are not subjected to enterprise-level KYC burdens that are disproportionate to their risk profiles.

At the same time, INCOMPAS notes that not all international or cross-border calling reflects heightened fraud risk. Legitimate businesses routinely use voice services to conduct customer support operations, provide technical assistance, and maintain communications with U.S.-based customers from abroad. A rigid, origin-based approach that categorically treats foreign callers as high-risk would penalize these lawful use cases and undermine the competitiveness of providers who serve global enterprises. Instead, the Commission should afford providers the flexibility to assess the risk profile of cross-border traffic based on the totality of the customer relationship, including the nature of the business, the volume and pattern of calls, and other indicia of legitimacy, and to require enhanced verification measures where the risk profile warrants them.

[12] *See id.* at para. 13 (seeking comment on a tiered approach where KYC requirements become more stringent for high-volume callers, callers using specific types of calling equipment associated with robocalling, or callers engaged in certain traffic patterns).

The *Further Notice* also identifies certain red flags that should trigger closer verification.[13] INCOMPAS supports a risk-trigger approach as part of any verification framework. However, INCOMPAS urges the Commission to make clear that business registration in a state other than the apparent state of operations should not automatically constitute a red flag. Many businesses register in states different from where they are headquartered for entirely legitimate legal and financial reasons, and treating this as inherently suspicious would generate a significant volume of false positives and impose unnecessary compliance burdens on legitimate businesses.

III. THE COMMISSION SHOULD ADOPT RISK-TRIGGERED REVERIFICATION AND A REASONABLE RETENTION PERIOD

A. Risk-Triggered Reverification Is Superior to Mandatory Periodic Reverification

The *Further Notice* also seeks comment on two approaches to reverification: risk-based re-verification triggered by changes in traffic patterns or other red flags, and mandatory periodic re-verification on an ongoing basis, such as annually.[14] INCOMPAS strongly supports the risk-triggered approach and opposes mandatory periodic reverification.

Mandatory periodic reverification is not practical in many scenarios and would harm consumers and businesses by potentially interrupting or terminating phone service unnecessarily. Elderly consumers may not be able to easily comply with recurring verification requirements and would risk losing service for non-compliance. Voice service providers with large numbers of authorized users face significant administrative burdens in managing verification cycles across

[13] *See id.* at para. 21 (identifying red flags including a registered agent or virtual office as a physical address, newly created website, suspicious email address, registration in a state other than the state in which the business purports to be located or incorporated, and payment via cryptocurrency).

[14] *See id.* at paras. 22-23.

their entire customer base. These burdens would fall disproportionately on smaller providers who lack the operational infrastructure to manage mass reverification programs.

Risk-triggered reverification requiring reverification when traffic patterns deviate from expected behavior or other red flags appear directs scrutiny toward situations where there is an actual basis for concern. This approach is more effective, more proportionate, and less harmful to legitimate customers. The Commission should adopt risk-triggered reverification as the standard and reject mandatory periodic reverification.

B. The Commission Should Adopt a Reasonable Retention Period

The Commission also suggests that originating providers be required to retain KYC information and supporting records for four years following termination of the customer relationship, matching the statute of limitations period for spoofing and intentional TCPA violations.[15] INCOMPAS does not object to a four-year retention period in principle, as it is aligned with applicable statutory limitations periods. The Commission should ensure, however, that any retention requirements are accompanied by clear data security obligations that are proportionate to the sensitivity of the information being retained, and that smaller providers are not subjected to data security mandates that exceed the resources available to them. The Commission should also consider whether providers should be permitted to satisfy the retention requirement through use of compliant third-party data retention services rather than in-house systems.

[15] *Id*. at para. 24 (proposing to require retention for the entirety of the applicable statute of limitations period, which is four years in the case of spoofing or intentional violations of section 227(b)).

IV. THE COMMISSION SHOULD RECONSIDER THE PROPOSED PER-CALL PENALTY FRAMEWORK AND REJECT DOWNSTREAM BLOCKING TIED TO KYC NONCOMPLIANCE

A. Per-Call Penalties Must Be Limited to Calls Involving Actual Fraud or Deceptive Intent

The *FNPRM* proposes to codify a $2,500 per-call base forfeiture amount for violations of section 64.1200(n)(4).[16] The Commission reasons that a per-call approach best correlates penalties to the volume of illegal calls made and thus the harm caused.[17] INCOMPAS understands the Commission's objective but strongly opposes the per-call penalty framework as currently structured, because it would expose providers to open-ended liability for good-faith compliance efforts that a future Commission might retroactively determine to be inadequate.

Section 64.1200(n)(4) requires providers to take "affirmative, effective measures" to know their customers and exercise due diligence in ensuring that services are not used to originate illegal traffic.[18] A finding that a provider's KYC process was inadequate does not necessarily mean that any particular call originated on that provider's network was illegal. Imposing a $2,500 per-call penalty for every call made on a provider's network during a period of alleged KYC noncompliance would be disproportionate and could be threatening to smaller competitive providers. The Commission should make clear that any per-call liability is expressly limited to calls made with the intent to defraud or deceive, or to calls where fraud or deception actually took place, not to all calls made on a provider's network.

---

[16] *See id.* at para. 25 (proposing to codify a $2,500 per call base forfeiture amount for violations of section 64.1200(n)(4)).

[17] *See id.* at para. 25.

[18] 47 CFR § 64.1200(n)(4).

INCOMPAS also notes that providers should not be required to provide customer information to law enforcement or the Commission in the absence of a lawful order compelling the provider to do so. There are existing legal frameworks governing the provision of customer information to law enforcement, and the Commission must operate within those frameworks.

B. The Commission Should Not Permit Downstream Blocking Tied to KYC Noncompliance

Furthermore, INCOMPAS strongly opposes the Commission's proposal to broaden downstream provider blocking requirements so that any provider downstream of an originating provider that fails to comply with KYC requirements must block that originating provider's traffic.[19] Existing Commission rules already allow for or require blocking in defined scenarios, such as when a provider fails to appear in the Robocall Mitigation Database. Expanding provider discretion to block traffic based on *perceived* KYC noncompliance would result in blocking of legitimate calls and would significantly increase the likelihood of anticompetitive conduct.

INCOMPAS members have repeatedly experienced blocking and mislabeling of legitimate traffic by analytics companies and larger providers acting as gatekeepers, with disparate impacts on competitive providers. Permitting downstream blocking tied to KYC noncompliance would add another vector for such conduct and should be rejected. The Commission has ample existing enforcement tools, including the per-call forfeiture it proposes, to address KYC noncompliance without empowering downstream providers to make unilateral blocking decisions that affect the entire market.

[19] *See Further Notice* at para. 27 (seeking comment on whether to broaden downstream provider blocking requirements so that any provider downstream of an originating provider that fails to comply with KYC requirements must block that originating provider's traffic).

In the alternative, should the Commission choose to explore a blocking regime for providers that are aware of non-compliance with KYC requirements, INCOMPAS urges the agency to encourage, and establish a legally protected framework for, providers to first share relevant intelligence with the originating provider or a neutral third party so that the originating provider has an opportunity to investigate and remediate the problem before traffic is blocked. Any framework the Commission adopts should preserve voluntary flexibility while ensuring that blocking decisions are not mandated, standardized, or weaponized as a competitive tool.

V. ANY KYC FRAMEWORK MUST BE OPEN, COMPETITIVELY NEUTRAL, AND NON-PROPRIETARY

INCOMPAS urges the Commission to ensure that any enhanced KYC framework relies on open, competitively neutral, non-proprietary solutions. Experience has demonstrated that bottleneck proprietary vetting services, industry-mandated registries, or KYC obligations developed by or for the benefit of large or dominant providers breed discriminatory outcomes that harm competition, consumers, innovators, and small businesses.

To the extent the Commission references third-party verification services in its final rules, it should make clear that internal implementations of equivalent verification processes are equally acceptable. The Commission should not require adoption of a specific proprietary solution or permit any industry body to mandate KYC requirements across the ecosystem. Provider-led messaging registries and whitelisting arrangements have created competitive distortions in related contexts, imposing costs on competitive providers that gatekeepers do not impose upon themselves. The Commission must ensure that any KYC framework does not replicate those dynamics.

The *Further Notice* also seeks comment on whether originating providers should be exempted from directly collecting KYC information when such information can be obtained

from credible alternative sources such as credit reports, similar to the financial services industry exemption.[20] INCOMPAS supports such an exemption. Allowing providers to satisfy KYC requirements through credible third-party data sources reduces compliance burdens, particularly for smaller providers, while still ensuring that meaningful identity verification takes place.

VI. THE COMMISSION SHOULD STRENGTHEN INFORMATION SHARING FRAMEWORKS AND CLARIFY THE DEFINITION OF "VOICE SERVICE PROVIDER"

A. Existing Information Sharing Frameworks Are Insufficient

The Commission's current framework for information sharing, including the Section 222(d)(2) exception for sharing information when related to fraud,[21] does not sufficiently enable timely, proactive collaboration among providers. Providers require clear authority and explicit safe harbor protections to share fraud-related intelligence in good faith without risk of liability, including liability for defamation, anticompetitive behavior, or equal access concerns.

INCOMPAS urges the Commission to expand permissible information sharing frameworks to enable both cross-industry and intra-industry sharing, as tying data across industries is a key pillar of identifying and stopping the threat of unlawful robocalls. Fraud perpetrated through voice networks frequently has financial industry counterparts, and enabling providers and financial institutions to share relevant intelligence in a legally protected framework would significantly enhance the effectiveness of fraud detection and prevention. The Commission's discussion of financial sector KYC parallels in the *FNPRM* underscores the

[20] *See id.* at para. 16 (seeking comment on whether an exemption should be adopted when KYC information can be obtained from alternative sources such as credit reports, similar to the financial services industry exemption).

[21] 47 U.S.C. § 222(d)(2).

importance of this cross-sector coordination. Intra-industry information sharing is equally critical, and in many respects even more immediately impactful, because bad actors who are denied service by one provider will simply seek to turn up problematic routes on other networks if carriers cannot share intelligence. Carriers must have legal authority and safe harbor protections necessary to share fraud-related intelligence with each other or with a neutral, trusted third party that can then make relevant information available across the ecosystem as appropriate. Stopping fraud requires full ecosystem cooperation, and the Commission should establish a governance framework that empowers sharing in a manner that is legally protected, competitively neutral, and operationally effective.

B. The Commission Should Adopt a Simplified, Technology-Neutral Definition of "Voice Service Provider"

The *Further Notice* uses the definition of "voice service provider" from the *Fourth Call Blocking Order*.[22] While INCOMPAS appreciates the Commission's effort to provide clarity, the existing definition creates inconsistency in the application of KYC and related obligations across different provider types and enables regulatory gaps that bad actors can exploit by structuring their operations to fall outside the scope of current definitions.

The Commission should 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 that may not reflect the realities of modern voice network architecture. A functional, technology-neutral definition would close the gaps that bad actors currently exploit, ensure that obligations apply consistently across equivalent functions

[22] *See Further Notice* at n. 1.

regardless of technology, and provide greater regulatory certainty for providers operating across multiple service categories.

VII. ADEQUATE IMPLEMENTATION TIME FOR NEW KYC RULES SHOULD BE PROVIDED

INCOMPAS urges the Commission to extend its proposal on when new KYC rules should take effect to at least twelve months following OMB approval.[23] Changes to existing KYC processes require time to plan and execute necessary engineering changes, update customer-facing interfaces and documentation, train staff, and educate customers on new requirements. Six months is insufficient for many providers, particularly smaller competitive providers with more constrained engineering resources. The Commission should consider a tiered implementation schedule that provides additional time for smaller providers.

INCOMPAS also supports the *Further Notice's* proposal to apply new rules primarily to new and renewing customers acquired after the effective date.[24] Applying enhanced KYC requirements retroactively to existing customers would impose enormous compliance burdens without commensurate consumer protection benefits, as existing customers have already been vetted under the provider's current KYC framework. For existing high-volume customers, any enhanced requirements should apply only at service renewal.

VIII. 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*.

---

[23] *See id.* at para. 29 (the item proposes a six-month post-OMB effective date, while INCOMPAS urges the Commission to extend this to at least twelve months to allow sufficient time for engineering changes, customer education, and compliance planning).

[24] *See id.* at para. 29.

Respectfully submitted,

/s/ Christopher L. Shipley

Christopher L. Shipley
Executive Director of Public Policy
INCOMPAS
1100 G Street, NW, Suite 800
Washington, DC 20005
(202) 872-5746
cshipley@incompas.org

June 25, 2026