NATIONAL ASSOCIATION OF ATTORNEYS GENERAL

PRESIDENT
William Tong
Connecticut
Attorney General

PRESIDENT-ELECT
Marty Jackley
South Dakota
Attorney General

VICE PRESIDENT
Brian Schwalb
District of Columbia
Attorney General

IMMEDIATE PAST PRESIDENT
John Formella
New Hampshire
Attorney General

INTERIM EXECUTIVE DIRECTOR
Dan Schweitzer
Director, Center for
Supreme Court Advocacy

1850 M Street NW
12th Floor
Washington, DC 20036
(202) 326-6000
www.naag.org

July 27, 2026

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

REPLY COMMENTS OF FIFTY (50) STATE ATTORNEYS GENERAL

I. Introduction

The undersigned State Attorneys General ("State AGs") submit these Reply Comments in response to the public notice issued by the Consumer and Governmental Affairs Bureau.[1] The public notice seeks comment on the Federal Communications Commission's ("Commission") proposals to enhance existing "Know-Your-Customer" ("KYC") obligations on originating voice service providers.[2] These proposals recommend implementing more rigorous KYC

[1] *See* Further Notice of Proposed Rulemaking, *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, Adopted Apr. 30, 2026 (hereinafter "KYC Further Notice").

[2] *KYC Further Notice* at ¶ 2 n.1 ("The KYC measures we discuss apply only to originating voice service providers ('originating providers')").

measures to protect consumers, which include collecting specific customer identification requirements for new and renewing customers,[3] requiring providers to verify, retain, and re-verify customer information, and requiring additional information from certain customers including high-volume or high-risk customers.[4]

State AGs support the Commission's efforts to strengthen its mandate that, in order for originating providers to "take affirmative, effective measures" when onboarding and retaining renewing customers, such providers must actually engage in meaningful KYC practices. Because the problem with illegal and fraudulent calls begins with the origination of the call, the undersigned State AGs applaud the Commission's proposals that would provide further guidance on what meaningful KYC and due diligence should look like for originating providers that aim to be good stewards of the ecosystem. These commonsense proposals will further aid all providers that wish to take seriously their obligation to serve as the first line of defense to protect the integrity and safety of the U.S. communications network.

II. Originating Providers are the Principal Gatekeepers of the U.S. Voice Communications Network

State AGs have recognized the importance of meaningful KYC policies—as well as the impact of their absence—in previous filings with the Commission,[5] as well as other collaborative

---

[3] *Id.* at ¶ 6.

[4] *Id.* at ¶ 3.

[5] *See, e.g.*, Reply Comments of Fifty-One (51) State Attorneys General, *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, and *Call Authentication Trust Anchor*, WC Docket No. 17-97, at 6, 11 (filed Jan. 10, 2022) (supporting the Commission's proposals requiring gateway providers to be obligated to engage in meaningful KYC "for all traffic they bring into the U.S. telephone network" from foreign provider customers); Reply Comments of Fifty-One (51) State Attorneys General, *Numbering Policies for Modern Communications*, WC Docket No. 13-97, *Telephone Number Requirements for IP-Enabled Service Providers*, WC Docket No. 07-243, *Implementation of TRACED Act Section 6(a)—Knowledge of Customers by Entities with Access to Numbering Resources*, WC Docket No. 20-67, *Process Reform for*

efforts, like the Anti-Robocall Principles[6] that 51 State AGs and 15 voice service providers[7] agreed to prior to the enactment of the TRACED Act.[8] As the Commission astutely recognizes throughout the KYC Further Notice, knowing a customer's true identity and understanding their business should be of paramount concern to any voice service provider that puts a customer's traffic onto the U.S. communications network.

Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership, IB Docket No. 16-155, at 3–5 (filed November 15, 2021) (emphasizing concerns about companies which lack meaningful KYC policies that allow illegal robocallers to circumvent STIR/SHAKEN call authentication by providing these bad actors with access to telephone numbers without conducting any due diligence on the legitimacy of the companies or their purposes for needing the numbers, thereby allowing these "illegal robocallers . . . the ability to use legitimate phone numbers to place calls with the same degree of anonymity that caller ID spoofing provides").

[6] *See* Anti-Robocall Principles, "Principle #5: Confirm the Identity of Commercial Customers," https://www.ustelecom.org/wp-content/uploads/2019/08/State-AGs-Providers-AntiRobocall-Principles-With-Signatories.pdf. These Anti-Robocall Principles were also included in the Call Authentication Trust Anchor Working Group's 2020 Report on "Best Practices for the Implementation of Call Authentication Frameworks," *see* North American Numbering Council, Call Authentication Trust Anchor Working Group, *Best Practices for the Implementation of Call Authentication Frameworks* at 9–10, 17, 25–26 (Sept. 24, 2020), *available at* https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf, and have been included since their adoption in the USTelecom's Industry Traceback Group Policies and Procedures, *see, e.g.*, USTelecom, *Industry Traceback Group Policies and Procedures*, at 4, 21 (revised Aug. 2025), *available at* https://tracebacks.org/wp-content/uploads/2025/09/ITG_Policies-Procedures_Aug_2025.pdf.

[7] At the time the Anti-Robocall Principles were announced in August 2019, twelve voice service provider joined as signatories: AT&T Services, Inc.; Bandwidth Inc.; CenturyLink; Charter Communications, Inc.; Comcast; Consolidated Communications, Inc.; Frontier Communications Corporation; Sprint; T-Mobile USA; U.S. Cellular; Verizon; and Windstream Services, LLC. In February 2020, the following three additional voice service providers joined as signatories: Shentel; Twilio, Inc.; and Wabash Communications.

[8] Pallone–Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105 (2019) (codified in 47 U.S.C. § 227b).

The Commission's unequivocal remarks bear repeating: "[t]he most effective way to prevent illegal calls from reaching American consumers is by ensuring they never enter the network[;]"[9] "[o]riginating voice service providers are best positioned to do that by screening new or renewing customers before they make calls[,]"[10] but "some originating providers do not do enough."[11] The undersigned State AGs and the Commission have a shared belief that, when an originating voice service provider gives the figurative and literal keys to the U.S. communications network to a customer without conducting sufficient—or, in some cases, any—meaningful KYC as to the legitimacy of that customer's business, that provider is shirking its responsibility to its competitors and industry colleagues in the ecosystem, to the U.S. communications network as a whole, and to our nation's consumers.

Further, "[b]eyond allowing illegal calling, this lack of diligence on the part of some originating providers can make it difficult for law enforcement to identify criminals that use the telephone network to perpetrate drug deals, violent crimes, and human trafficking."[12] State AGs agree that "[e]nhanced KYC information can assist law enforcement to more easily identify callers that use the network to perpetuate crimes by ensuring that voice providers have accurate and complete customer information."[13] The Commission rightfully recognizes that "[t]he KYC

---

[9] *KYC Further Notice* at ¶ 2.

[10] *Id.*

[11] *Id.*

[12] *Id.*

[13] *Id.* at ¶ 28; *cf.* Reply Comments of Forty-Seven (47) State Attorneys General, *Improving the Effectiveness of the Robocall Mitigation Database*, WC Docket No. 24-213, and *Amendment of Part 1 of the Commission's Rules, Concerning Practice and Procedure, Amendment of CORES Registration System*, MD Docket No. 10-234 at 5 (filed Nov. 12, 2024) (supporting the Commission's proposals to adopt rules requiring that voice service providers' entries in the FCC's Robocall Mitigation Database ("RMD") be accurate and current, because law enforcement agencies "rely on the RMD to identify potential bad actors using, or attempting to use, United

information gathered and verified would help ensure that law enforcement gets accurate information in response to subpoenas when investigating crimes."[14] And State AGs agree that, "[w]hen an originating provider fails to meet its obligations to properly scrutinize its customers before they commence using the provider's services to originate calls, it [further] creates a risk that malicious actors will gain access to those services to make illegal calls and opens the door for foreign actors to exploit U.S. networks for fraud, espionage, or influence operations that undermine national security."[15]

Moreover, there is precedent for mandating that an industry engage in commonsense due diligence in its customer onboarding and retention practices and procedures in order to protect against rampant abuse, as the Commission recounts by referencing the statutes and rules enacted in the financial sector to address money laundering.[16]

The State AGs appreciate that some industry members may oppose rigorous—or any—clarifying mandates concerning meaningful KYC requirements. However, to those members, we ask: What is the legitimate business use case for originating providers—or any member of this industry's ecosystem—that would be served by rejecting a set of industry-wide, commonsense KYC practices when onboarding and retaining customers? What argument can an originating provider make, whether large or small, global or mom-and-pop, that a provider does not have a legitimate business interest in making certain that its customers are each demonstrably legitimate businesses engaged in legitimate business practices?

States communications networks for illegal purposes").

[14] *KYC Further Notice* at ¶ 28; *see id.* at ¶ 36 (recognizing that a lack of accurate and complete customer information hinders the abilities of the Commission—as well as law enforcement generally—to identify and locate parties responsible for making illegal calls).

[15] *KYC Further Notice* at ¶ 36.

[16] *Id.* at ¶¶ 4–5, 9.

To the question of whether enhanced KYC requirements would prevent or mitigate misuses of U.S. communications networks and numbering resources and cut down on illegal calls,[17] the indisputable answer must be "Yes." As the Commission recognizes, and State AGs agree, when bad actors are allowed to leverage anonymity and are permitted to operate in the shadows by the very providers who are gatekeepers to this ubiquitous infrastructure,[18] "[t]he result is more illegal calls that defraud American consumers and open our communications network to vulnerabilities."[19] However, if all originating providers were held to the same KYC standards, and there were consequences for failing to do one's part in implementing them, the resulting industry-wide spotlight would both prevent bad actors from continuing to hide and make it much easier to identify those providers that help to keep these nefarious businesses going.

The proposals in this KYC Further Notice are measured and reasonable. The Commission, at its core, seeks to mandate that originating providers conduct business only with those entities that they know are legitimate and are engaged in legitimate business practices. As principal gatekeepers to the U.S. communications network, originating providers are best positioned to scrutinize those who seek entry to the network primarily to profit from harm caused to the network and our constituent consumers. The U.S. communications network should be a place for efficiency, but not for shortcuts. As described herein, the State AGs support the Commission's proposals to require KYC practices that will reduce available points of entry for bad actors that seek to use the U.S. communications network only as a pathway for abuse, rather than a pathway for connections.

---

[17] *Id.* at ¶ 10.

[18] *Id.* at ¶ 8.

[19] *Id.* at ¶ 2 (footnote omitted).

III. Articulating More Rigorous and Specific KYC Practices Does Not Need to Start from a Blank Page

A good starting place to address the proposals in the KYC Further Notice may be with the Commission's inquiry regarding whether there are "any existing industry best practices to set baseline KYC compliance standards, including for smaller providers."[20] Numeracle's public-facing enhanced KYC practices are a useful reference. Those practices accompany a 2023 *ex parte* filing[21] by Numeracle.[22] While the State AGs are not aware that these KYC Model Standards[23] have been formally adopted by any particular segment of industry to date, these comprehensive standards from 2023 provide a reasonable starting place for this discussion.

What is particularly notable about Numeracle's KYC Model Standards is that they regard the KYC process, not as a static, one-time, checklist-based activity, but as an inquiry on a continuum that contemplates a provider's obligations to verify a customer's business, that business's identity and its history, and the intended use of the originating provider's services by that business. Further, and importantly, Numeracle's KYC Model Standards contemplate the provider's post-activation obligations to monitor the customer's call activity, to conduct further KYC reviews and audits, and to undertake enhanced due diligence for customers that are part of

---

[20] *Id.* at ¶ 16.

[21] Letter from Rebekah Johnson, Founder and CEO, Numeracle, Inc., to Marlene Dortch, Secretary, FCC, CG Docket No. 17-59 and WC Docket No. 17-97, at 5 (dated Apr. 27, 2023) (hereinafter "Numeracle 2023 *Ex Parte*"), *available at* https://www.fcc.gov/ecfs/search/search-filings/filing/1042778647719.

[22] *Numeracle 2023 Ex Parte* at 2 ("While Numeracle is not a voice service provider, we face many of the same challenges. Numeracle's mission is to verify the identities of entities that seek to communicate lawfully with their customers and to facilitate those communications across all channels.").

[23] Numeracle, Inc., *Model Standards for Know Your Customer "KYC,"* Attachment to *Numeracle 2023 Ex Parte*, https://www.fcc.gov/ecfs/document/1042778647719/2 (hereinafter "Numeracle's KYC Model Standards").

potentially high-risk categories or exhibit red flag behaviors that require further scrutiny.

The Numeracle KYC Model Standards contemplate and provide methodology for a fulsome inquiry into the legitimacy of a business entity and that business's services and practices as that business first presents itself at the time of onboarding and as it later grows, changes, expands, and adapts over time. The State AGs support standards that address the ways that companies change over time and believe the Commission could identify portions of the Numeracle KYC Model Standards that advance the Commission's goals while further articulating reasonable baseline KYC compliance standards. We encourage the Commission to consider mandating that these KYC practices be implemented by all originating providers and, frankly, by all providers so that they take seriously their responsibility and obligation to safeguard the U.S. communications network.

IV. KYC Should Require More Than Merely Knowing the Customer's Business Name; It Should Require Understanding the Customer's Business

State AGs would not presume to articulate an exhaustive or comprehensive list of KYC policies that would make the U.S. communications network impenetrable to every incursion by bad actors or by those that enable bad actors for an easy profit. However, as a result of our individual and collective investigations, litigation, and engagement with industry partners and associations, the State AGs have a solid understanding of the questions that originating providers should ask to onboard or retain only those customers that limit the origination of suspicious call traffic from the providers' networks. The State AGs further advise that originating providers should be required to verify the information they obtain during the onboarding process before allowing a customer to access the U.S. communications network.

For instance, to start, the Commission proposes that originating providers, "at a minimum, obtain and retain the name, physical address, government issued identification number, and an alternate telephone number of any new and renewing customer before granting access to its services."[24] State AGs agree. But, as to the Commission's inquiry as to whether this information is "sufficient to enable originating providers to identify malicious actors before they originate illegal calls,"[25] we think it is not.

In order to begin to know a prospective or renewing customer, an originating provider must ask for, receive, and verify information that will help the provider understand the true nature of the customer's business. This means that, in addition to verifying the identity, formation, and actual existence of the business entity and its ownership, the originating provider should be obligated to examine and understand the customer's services and business practices, the reputation and history of all principals in the customer's business, the customer's intended use of the provider's services, and the customer's compliance with state and federal laws.

For example, over the years, the State AGs have encountered obstacles contacting businesses using information that the businesses themselves provided, including information that businesses have provided to the Commission.[26] The contact information was inaccurate. For this

---

[24] *KYC Further Notice* at ¶ 9.

[25] *Id.* at ¶ 10.

[26] *See, e.g.*, Reply Comments of Forty-Seven (47) State Attorneys General, *Improving the Effectiveness of the Robocall Mitigation Database*, WC Docket No. 24-213, and *Amendment of Part 1 of the Commission's Rules, Concerning Practice and Procedure, Amendment of CORES Registration System*, MD Docket No. 10-234 at 2 (filed Nov. 12, 2024) ("The [Commission's Robocall Mitigation Database] is an essential resource in State AGs' efforts to combat illegal robocalls. However, too often the information submitted by providers to the RMD is clearly false or inaccurate and demonstrates contempt for the Commission's requirements and the consumers those requirements protect. In our investigative and enforcement efforts, State AGs have encountered facially deficient RMD entries and mitigation plans. . . . These deficiencies include false, incomplete, or misleading contact information, blank or inapplicable mitigation plans, and

reason, ensuring that contact information provided by the prospective customer is complete and accurate should be the first priority. This may include the collection and validation of contact email addresses with a domain name that exactly matches that of the entity website provided, or a domain verified as controlled by the entity.[27] This could also include the collection and validation of the name, physical address, email address, and telephone number for the customer's business owner(s), and if the business is not directly owned by a natural person, then the name, physical address, email address, and telephone number for the natural person(s) who indirectly own(s) the business.

After collecting and verifying the perfunctory business information about a prospective business customer, an originating provider should inquire about a business's ownership, including the legal name(s) of any parent company(ies), as well as its state/province/country of business incorporation, the business's website(s), and the name(s) of all individuals with 10% or more direct or indirect ownership of the entity.[28] The prospective customer should also be required to provide a list of all business and trade names, fictitious names, and other "dbas" under which the customer or its principal owners and operators have transacted business for the previous several years. The customer should also provide a Taxpayer Identification Number, the business's articles of organization or incorporation and other formation documents, as well as proof that the entity is in good standing with the Secretary of State for the state in which the business is organized.

representations which are contradicted by other FCC filings or publicly available sources.").

[27] *See Numeracle's KYC Model Standards* at 5.

[28] *See id.*

Once the legitimacy of the entity, ownership, and contact information are verified, the originating provider should further inquire about the timespan and circumstances of the customer's organization and its history in the industry. State AGs have recently been finding inconsistencies concerning company longevity and seeing an uptick in the use of "shelf" or "aged" companies. These are shell companies that were pre-registered with a state corporation commission (or comparable regulatory authority) but left inactive for a period of time to allow the company to age but were later acquired and made active to give a newly formed company the illusion of company longevity.

State AGs are seeing this tactic used more frequently by entities entering and participating in the communications industry, almost as much as shell companies have historically been used to obscure true ownership of a company. For this reason, State AGs would recommend that any inquiry into a business include its history in the industry, which could be verified with information showing the organization has indicia of legitimacy, possibly including but not limited to participation in trade shows, membership in industry associations, possession of a unique website, use of social media accounts, advertisements or other documentation evidencing effort to recruit or retain customers. These or other indicia of legitimacy give an originating provider useful context to corroborate the legitimacy of any claimed company history or longevity.

Next, a legitimate business should be able to provide an originating provider with information about the business's services and business practices, including a description of the intended use of the provider's services, the business's website and public-facing materials, a description of the types of calls to be made, a description of consent collection practices, sample scripts that the callers will be using, and information about whether the business currently, or intends to originate robocalls or engage in telemarketing.[29]

The originating provider should further inquire about information that will help give context to the reputation of that customer in its industry. For example, the provider should learn whether the customer—or other businesses operated by its principals—have previously been put on probation, suspended, or terminated as a customer from another originating provider's network, as well as the reasons given for that action. If a provider knows the principals of a business, the provider can further ascertain whether the business or its owners have been subject to any prior federal or state enforcements or adverse judgments for alleged illegal activity related to illegal robocalls or unlawful telemarketing or solicitations.

In sum, State AGs support proposals that will help inform the originating provider about the true identity of a prospective or renewing customer. Further, any information requested and collected during any KYC process *must* be verified, and, in order to protect the integrity of the U.S. communications network, it should go without saying that such verifications would have to be completed *prior to* allowing any customer to use the originating provider's network.

As the Commission recognizes, "[a]n effective KYC regime must confirm the accuracy of the information customers provide" because—as State AGs have seen firsthand—"[b]ad actors may submit fake or stolen information to conceal their identity to gain access to the network and avoid accountability for making illegal calls.[30] Yet, originating providers that "conduct a thorough verification of their customers' information can discover the use of such fake information before allowing bad actors to originate calls and stop illegal calls before they occur."[31]

[29] *See id.* at 5–6.

[30] *KYC Further Notice* at ¶ 18.

[31] *Id.*

By requiring that verification of any prospective customer's information be completed before accepting its call traffic, originating providers will further minimize opportunities for potential bad actors to exploit loopholes in KYC processes that may be bypassed by, for example, "trial" periods or accounts, concerns about which were highlighted in a recent filing by State AGs on numbering resources.[32]

Additionally, mandating that an originating provider take reasonable steps to review and assess the accuracy of the information provided by any customer should not be overly costly or burdensome when compared to the cost to consumers—as well as, quite possibly, to the offending originating provider—for not doing so. The State AGs believe that it would not be necessary for originating providers to retain a third-party vendor to provide the verification services that the State AGs advocate; rather, often the legitimacy of a business can be tested and verified by reviewing publicly available information.[33]

[32] Reply Comments of Forty-Nine State Attorneys General, *Combatting Illegal Robocalls Through FCC Numbering Policies*, WC Docket No. 26-49, *Implementation of TRACED Act Section 6(a) — Knowledge of Customers by Entities with Access to Numbering Resources*, WC Docket No. 20-67, *Numbering Policies for Modern Communications*, WC Docket No. 13-97, and *Telephone Number Requirements for IP-Enabled Service Providers*, WC Docket No. 07-243, at 14 (filed July. 7, 2026).

[33] As an analogous example, in *State of Texas, et al. v. Rising Eagle Capital Group, LLC, et al.*, No. 4:20-cv-2021 (S.D. Tex. 2020), eight state attorneys general—Arkansas, Indiana, Michigan, Missouri, North Carolina, North Dakota, Ohio, Texas—filed a complaint against four individual defendants and several business entities for violations of the Telephone Consumer Protection Act, the Telemarketing Sales Rule, and state statutes involving allegations of billions of illegal robocalls to U.S. consumers. The parties agreed to entry of stipulated judgments that included injunctive relief barring certain of the individual defendants from involvement in the business of robocalling. The Plaintiff States were forced to initiate contempt proceedings after they determined that the principal individual defendant—John Spiller, II—who was subject to the injunctive relief, had started no fewer than four additional business entities, at least two of which were involved in the sending and/or routing illegal robocalls to consumers after the entry of the stipulated judgment against him. Further, at least one of those companies named as its officer and owner Mr. Spiller's stepfather, a man with no previous experience in the telecom industry. Mr. Spiller was the de facto owner and beneficiary of that company, was involved in its daily operation, and was a signor on its bank account. Were more rigorous KYC required of other voice service providers, Mr. Spiller's

For instance, an originating provider can manually call all contact telephone numbers provided by the customer to ensure that responsible parties are reachable. A provider can check the customer's online presence through its internet website(s) and social media page(s), and through Internet searches to see if the business relies heavily on other websites' stock language and images. A provider can review public databases hosted by relevant state and/or federal government agencies that contain information about the registration or licensing of business entities to verify any business registration or licensing information provided. A provider can review the physical location(s) of the customer to ensure that one exists and that it is a reasonable business address. A provider can review the domain name for all contact email addresses provided to ensure they are operational, that they correspond with the potential customer's business, and that they are not readily available to any end user that is not associated with the customer's business (e.g., the email provided should generally not end in @gmail, @hotmail, @outlook, @protonmail, etc.).

Additionally, the State AGs agree that "[p]eriodic review or ongoing re-verification of KYC information is essential to ensure that bad actors have not gained access to the network," and to enable the Commission and other law enforcement agencies to hold them accountable.[34] For this reason, State AGs support the proposals that originating providers should be required to collect

---

entities likely would not have been able to start (or continue) sending illegal robocall call traffic. While the KYC Further Notice contemplates only mandating rigorous KYC by originating providers for its customers, we provide this example to show how providers that continued to do business with Mr. Spiller's later-formed entities had, within their reach, the ability to know that Mr. Spiller was court-ordered not to be involved in the telecom industry before doing business with him, which could have resulted in less illegal call traffic reaching consumers through the U.S. communications network.

[34] *KYC Further Notice* at ¶ 18.

and verify all KYC information "before allowing the customer to use its network,"[35] and that originating providers should be required to "periodically re-verify" certain customer information "on an ongoing basis."[36] While an annual reassessment may be a reasonable baseline, further scrutiny may be necessary "in response to changes in traffic patterns or other red flags that may suggest illegal calls."[37]

Originating providers that seek to safeguard our nation's communications network should also responsibly monitor and assess all call traffic of their respective customers to determine whether there are patterns consistent with illegal or suspicious call traffic, whether such monitoring and assessments are conducted by the provider itself or by a third party. Since at least 2020, the Commission has been clear that all originating providers are required "to implement KYC obligations and exercise due diligence to ensure their services are not used to originate unlawful and illegal calls."[38] The current KYC Further Notice does nothing to disturb the Commission's prior directive. The Commission previously tasked originating providers to ask sufficient questions of their customers to mitigate the problem of illegal robocalls. Those providers, as a whole, failed to meet that directive. So, while the Commission has returned to seek further input to provide more specific direction, the Commission's mandate has been consistent, clear, and has the State AGs' support.

---

[35] *Id.* at ¶ 20.

[36] *Id.* at ¶ 12, 23.

[37] *Id.* at ¶ 22.

[38] *Id.* at ¶ 37.

V. KYC Obligations Should Be Shouldered by the Entire Ecosystem, Including Small Originating Providers

The Commission expressed concern about whether "enhanced KYC requirements impose burdens on smaller providers."[39] The State AGs are of the opinion that the burden of ensuring the safety and security of the U.S. communications network and our consumers is one that must be shouldered by all originating providers without exception. The proliferation of illegal and fraudulent calls reaching our nation's consumers and weaponizing the U.S. communications network has been achieved through the entry points provided by originating providers. This has happened regardless of the size of those providers, and, in fact, the State AGs have observed that illegal call traffic has often been facilitated by smaller voice service providers.[40] Some originating providers have failed to engage in meaningful KYC and due diligence when onboarding customers, failed to sufficiently monitor and/or intervene when a customer's traffic has indicated red flags that the provider received and chose to ignore, or were complicit in—and profited from—the conduct either knowingly or by looking the other way.

While State AGs understand that there are real costs associated with conducting meaningful KYC and due diligence when onboarding and retaining customers, whether those responsibilities are carried out by in-house resources or by a retained third party, it cannot be said that there is a legitimate use case to shroud or exempt smaller originating providers from the obligation that they, too, should know that their customers and their customer's business practices

---

[39] *KYC Further Notice* at ¶ 10.

[40] *See, e.g.*, *State of Arizona, et al. v. Michael Lansky, dba Avid Telecom, et al.*, No. 4:23-cv-00233 (D. Ariz. 2023); *State of Florida v. Smartbiz Telecom LLC,* No. 1:22-cv-23945 (S.D. Fla. 2022); *State of Ohio v. Aaron Michael Jones, et al.*, No. 2:22-cv-2700 (S.D. Ohio 2022); *State of Vermont v. TCA VOIP, et al.* No. 5:22-cv-00069 (D. Vt. 2022); *State of North Carolina v. Articul8 LLC, et al.,* No. 1:22-cv-00058 (M.D.N.C. 2022); *State of Indiana v Startel Commc'ns LLC, et al.*, No. 3:21-cv-00150 (S.D. Ind. 2021); *State of Texas, et al., v Rising Eagle Capital Grp., LLC, et al.*, No. 4:20-cv-02021 (S.D. Tex. 2020).

are legitimate. In fact, not holding small originating providers to the same standards will cause them to be more attractive to bad actors seeking a less rigorous entry ramp for illegal traffic. It is reasonable to demand that all entities that enjoy the privilege of offering access to the U.S. communications network incorporate funds and resources into their business plans to do the work that best ensures that their networks are secure for their customers and are not being used to originate illegal calls that abuse and perpetrate fraud on the public.

VI. Do High-Risk Customers Require Additional KYC? Yes, As Part of Required Post-Activation Monitoring.

The Commission asks whether it should require originating providers "to collect more information about customers that are more likely to make illegal calls, e.g., those subscribing to high volume services or those that may be difficult to locate based on being foreign based, or other factors,"[41] such as 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."[42] The State AGs believe that initial, information-collection KYC requirements should be universal for all customers; however, the State AGs would support additional, long-term monitoring of customers with identified risk factors.

[41] *KYC Further Notice* at ¶ 13.

[42] *Id.*

Some "red flags,"[43] or a determination that a customer is "high risk,"[44] appear in any basic

[43] State AGs agree—and have encountered—most, if not all of the red flags identified in the KYC Further Notice, *KYC Further Notice* at ¶ 21 (identifying red flags that "should raise concerns for closer verification such as providing a registered agent or virtual office as a physical address; registering a corporate address using a residential address or random commercial location that is unaffiliated with the customer; lacking a commercial presence or operating a suspicious website (e.g., a newly created website); using a suspicious email address (e.g., a recently created email address, template website with little information unique to the company); not being registered in the state in which it purports to be located or incorporated; or paying for service in non-traceable ways such as the use of cryptocurrency.") There are many other examples. *See, e.g.*, *Numeracle's KYC Model Standards* at 10–11 ("The following behaviors should be considered red flags and prompt enhanced due diligence or potential rejection of the account.

- Unwillingness or expressions of hardship to provide requested information (or an unexpected eagerness to provide information)
- Aggressive, hostile behavior or over-escalation
- Claiming very large amounts of traffic with no clear basis (very few employees, brand new business entity, no web presence outside of a company website, etc.)
- Vague or incomplete answers to questions
- Unsolicited, notable interest in specific KYC processes and criteria
- Creating pressure to complete an agreement as soon as possible
- Customer's business entity is associated with a large number of related businesses or a complex structure of ownership without a clear reason
- Communication using email domains associated with multiple businesses or using public email domains (gmail, hotmail, etc.)
- Provided information, website, or documentation is unclear, incomplete, unprofessional, or appears to have been created very recently
- Customer is unwilling to speak over the phone or repeatedly avoids, cancels, or postpones meetings
- Customer presents as operating in one location but all customer contacts and operations seem to be located elsewhere or contacts claim to be traveling elsewhere").

[44] *See, e.g.*, Stipulated Order for Permanent Injunction and Monetary Judgment Against John C. Spiller, II at 5–6, *State of Texas, et al. v. Rising Eagle Capital Group, LLC, et al.* (S.D. Tex. 2020) No. 4:20-cv-2021) (defining "High Risk Customer" as any customer that: (1) "Engages in Telemarketing and/or generates or initiates Robocalls;" (2) "Is a Person domiciled outside of the United States;" (3) "Pays for Telephony Services via stored-value cards (e.g. gift cards), cryptocurrency, or money-transfer businesses (e.g. Venmo®, Zelle®, Cash App®, Paypal®, Western Union®, etc.);" (4) "Is, at any point, determined by the Industry Traceback Group, in its sole discretion, to be 'Non-Responsive' or equivalent term as defined in its 'Policies and Procedures' or any amendment, restatement, or subsequent update thereof;" or, (5) "Is blocked from another

KYC screening. Originating voice service providers have information early in the KYC process about the type of traffic a business customer anticipates sending. As a result of their investigations, the State AGs are aware that originating voice service providers often offer "dialer" rate decks that are billed at higher price points for high volume, short duration calls. The acceptable use terms of "dialer" rate decks vary from "conversational" rate decks in that they allow call traffic with lower average call duration and lower answer rates, which are metrics that can be associated with suspicious traffic. [45] A business customer who warrants this type of rate deck should be subject to

---

voice service provider's network after being determined to be a 'bad-actor upstream voice service provider' pursuant to a notice to the Federal Communications Commission in a process more formally described in Paragraphs 35-45 of the Federal Communication Commission's Third Report and Order, Order On Reconsideration, and Fourth Further Notice of Proposed Rulemaking in CG Docket No. 17-59 and adopted July 16, 2020"); *Numeracle's KYC Model Standards* at 10 ("Accounts associated with the following industries or business models have a higher risk of carrying highly regulated, unsolicited, or potentially illegal communications. While many legitimate operators may be in these categories, many have been subject to enforcement actions. Customers in these categories or who serve businesses in these categories require a higher standard of KYC review.

- Affiliate marketing/lead generation
- High-risk financial services (payday loans, debt relief, credit repair, auto/home warranties, loan offers by non-direct lenders, etc.)
- Third-party debt collections
- Political communications, fundraising (political or nonprofit), surveys
- IT support call centers not directly staffed and operated by the device or software manufacturer
- Highly marketed services (solar power, for-profit colleges, etc.)
- Businesses seeking US-based communications services that have a physical location in the United States but whose headquarters, staff, or leadership are located primarily outside of the United States." (footnotes omitted)).

[45] *See* Further Notice of Proposed Rulemaking, *Call Authentication Trust Ancho*, WC Docket No. 17-97; *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Adopted May. 20, 2026 (citing I3Forum, *Know Your Customer/Know Your Traffic Code of Conduct* at 9 (2025), https://i3forum.org/wp-content/uploads/2025/09/i3Forum_KYC_KYT_CoC_202509.pdf); *see also Appropriate measures for robocall mitigation*, TransNexus Blog (Oct. 12, 2020),

more careful vetting from the start.

However, other "red flags" or determinations that a business customer is "high risk" may not become clear until an originating provider is in the midst of, or has completed, the KYC process. It is also possible that the level of risk a customer presents to an originating provider, the U.S. communications network, and consumers may change over time. For these reasons, the State AGs would support a mandate that all business customers be subject to the same ongoing KYC requirements, regardless of their call volume or risk categorization. A universal set of KYC obligations would be more straightforward to implement and enforce for all originating providers and, perhaps ultimately, for all providers in the call path. It would also take the guesswork out of identifying which customers should be subject to a more thorough KYC process at the initiation of service.

For instance, although the definitions of "high risk" or "high volume" callers seem fairly straightforward, State AGs and service providers have not always agreed on what constitutes these types of customers. This is puzzling, particularly because providers appear to know when to offer customers higher priced rate decks for services that originate or route "high volume, short duration" call traffic. A universally applicable initial KYC process for all customers would remove the opportunity for originating providers to claim any perceived ambiguity about when to apply a more rigorous KYC process. All customers, regardless of services offered, size classification, or categorization, would be equally scrutinized, vetted, and known before they are given access to the U.S. communications network.

---

https://transnexus.com/blog/2020/robocall-mitigation-appropriate-measures/.

Specifically, State AGs support requirements that, for instance, obligate originating providers to "collect the intended use of the service (e.g., marketing, education, political campaign) and the customer's IP address from which each call will be placed (if applicable)"[46] from *all* customers, and not merely for high-volume customers, including business and foreign customers. While the State AGs understand that imposing higher obligations only on higher risk customers may be a reasonable allocation of the burden on an originating provider's willingness to carry that customer's call traffic,[47] every business customer has the potential to make changes to its business that would negatively impact the U.S. communications network.

Requiring the same KYC processes for all business customers would allow all originating providers to be fully informed about each of their customers. Accordingly, State AGs see no reason why questions about whether, for instance, a potential or existing customer will use, or is using, lead generators or dialing platforms should be asked only of a limited subset of customers, when such information is needed to inform a provider's assessments about each customer's risk level.

However, while *some* "high risk" characteristics or "red flags" arguably may not, in and of themselves, be determinative that a customer is a bad actor or impute nefarious conduct, it should go without saying that the existence of any of these characteristics or flags should always compel an originating provider to ask questions and hold the customer to account for the provider's concerns. If an originating provider makes a business decision to onboard or retain a business customer that is "high risk," or exhibits or accumulates any number of "red flags," the State AGs

---

[46] *KYC Further Notice* at ¶ 9.

[47] *See id.*

recommend requiring further enhanced activity monitoring and ongoing KYC review.[48]

KYC requirements already include an expectation that "originating providers will monitor traffic on their networks to determine if there are customer information inconsistencies."[49] While this monitoring is vitally important for *all* customers, the State AGs would support a requirement for more stringent monitoring of high-risk customers. Additionally, the State AGs support risk -based reverification, or requiring high-risk customers to re-verify on a more frequent basis than customers without the same risk factors.[50]

VII. MNOs, MVNOs, and all SIM-Engaging Entities May Require Different KYC Processes, But Definitely Should Require Rigorous KYC Processes

Almost a year ago, the leadership of the Anti-Robocall Multistate Litigation Task Force[51] began speaking with members of industry that could inform the Task Force further about players in, and practices of, the mobile ecosystem, with a particular focus on two aspects: understanding more about the role of Mobile Virtual Network Operators ("MVNOs"), and understanding more about the proliferation of SIM-based fraud. The State AGs applaud and support the Commission's invitation for commenters to provide public input on the steps that Mobile Network Operators ("MNOs") and MVNOs have taken to address bulk purchases of SIM cards or bulk account

[48] *See, e.g.*, *Numeracle's KYC Model Standards* at 7–8.

[49] *KYC Further Notice* at ¶ 22.

[50] *See id.* at ¶¶ 22–23.

[51] The Anti-Robocall Multistate Litigation Task Force is a 51-member bipartisan collective of State Attorneys General, led by the Attorneys General of Indiana, North Carolina, and Ohio, which is focused on actively investigating and pursuing enforcement actions against various entities in the robocall and robotext ecosystems that are identified as being responsible for significant volumes of illegal and fraudulent robocall and messaging traffic routed into and across the country.

activation,[52] to validate KYC for prepaid and postpaid services purchased at third-party retailers,[53] as well as its inquiry about what, if any, customer information wireless providers obtain from customers who purchase prepaid SIM cards.[54]

The State AGs have observed that KYC processes for individual consumers in the mobile ecosystem and KYC processes for business customers of originating voice service providers are markedly different. For example, while business customers typically negotiate contracts with their originating providers for services, individual consumers can purchase prepaid SIMs or postpaid service at an MVNO's retail location, online, or at a stand-alone reseller, such as Walmart. We also have learned that the processes for conducting KYC on individual consumers vary widely from location to location and provider to provider. The level of KYC to which an individual consumer is subject depends on, among other things, requirements of each individual MVNO and the diligence of the stand-alone reseller. We agree that this area of the ecosystem could benefit from the Commission's attention. Nonetheless, because this KYC Further Notice focuses on the KYC processes for business customers of originating voice service providers and not concerns raised by inconsistent KYC processes for individual consumers, the State AGs look forward to addressing those concerns at another time.

---

[52] *KYC Further Notice* at ¶ 15.

[53] *Id.* at ¶ 14.

[54] *Id.*

VIII. Proposals Concerning Implementation, Record Retention, and Enforcement are Necessary to Ensure Compliance with Enhanced KYC Processes

Because illegal robocalls continue to be among the top complaints received by all State AGs, implementation of any rules arising out of this KYC Further Notice should begin as soon as feasible, and if six months after OMB approval[55] is as soon as is practicable for implementation, State AGs support that timeline.

Additionally, State AGs support the application of these enhanced KYC requirements to both new and renewing customers that originating providers "acquire after the effective date of any new rules and to any customers that renew service with such providers after the effective date."[56] Again, because illegal robocalls persist in harming our constituents, there are clearly customers for which providers are currently originating illegal calls. For this reason, the obligation to engage in more rigorous KYC processes should apply to *all* current and prospective customers of *all* originating providers.

Further, the State AGs support the proposal that the Commission modify its downstream provider blocking requirements so that any provider downstream of an originating provider that fails to comply with the KYC requirements must block that originating provider's traffic.[57] This is common sense, since the absence of any consequence for failure to comply with these enhanced requirements may not compel any real action.

Similarly, to better encourage compliance, State AGs also support the proposed base forfeiture amount for violations and support the proposal that violations be on a per call basis "to best correlate penalties to the volume of illegal calls made, and thus the harm caused by any

---

[55] *KYC Further Notice* at ¶ 29.

[56] *Id.*

[57] *Id.* at ¶ 27.

one caller."[58]

Finally, on the issue of record retention, State AGs roundly support the proposal requiring originating providers to "retain KYC information and supporting records for the entirety of any potential statute of limitation period relating to misuse of their services to make illegal calls."[59] In August 2022, 43 State AGs filed Comments in support of the Federal Trade Commission's ("FTC") proposed amendments to the Telemarketing Sales Rule, 16 C.F.R. Part 310, that included amendments to section 310.5(a)(2), which obligates sellers and telemarketers to retain—for a period of five years—various records that would substantiate the telemarketing campaigns in which each was engaged, as well as call detail records of each telemarketing call.[60]

The State AGs' position in those Comments still applies today:

> "[T]echnological advancements have . . . reduced the burden and costs of recordkeeping," with electronic storage costing no more than a fraction of a dollar per gigabyte. The small cost of retaining this information is more than offset by its value to law enforcement. The representations in telemarketers' or sellers' advertisements are often at the heart of enforcement actions alleging deceptive and unfair trade practices. Requiring that these materials be preserved for five years from the date they are no longer in use is necessary to ensure that essential evidence remains available to law enforcement.
>
> The State Attorneys General share the same frustrations as those experienced by the FTC in investigating and bringing enforcement actions against those engaged in illegal telemarketing.
>
> . . . .
>
> The State Attorneys General agree with the FTC's conclusion that sellers and telemarketers "are in the best position to have information about their

---

[58] *Id.* at ¶¶ 25, 38.

[59] *Id.* at ¶ 24.

[60] Forty-Three State Attorneys General, Comment Letter on Proposed Amendments to the Telemarketing Sales Rule, 16 C.F.R. Part 310 at 5 (Aug. 2, 2022), https://www.regulations.gov/comment/FTC-2022-0034-0020 (hereinafter "FTC Recordkeeping Comments").

telemarketing calls."[61]

The obstacles that State AGs face when investigating those that originate illegal calls are no different today than they were when we filed those comments four years ago. Information is still fleeting, and the burden and cost to retain records is still minimal. Without affirmative obligations to engage in KYC processes, to certify the findings of those processes,[62] to retain records reflecting compliance with these KYC processes, and to be subject to consequences for failing to meet those obligations, the problem of illegal robocalls will not abate.

IX. Conclusion

In its mandate requiring originating providers to "[t]ake affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal traffic,"[63] the Commission exercised restraint and deferred to industry to identify those threshold practices that would satisfy the mandate.[64] However, as evidenced by the continued prevalence of illegal and fraudulent robocalls, originating providers as a whole have failed to meet the moment with meaningful and/or consistent onboarding and retention KYC requirements for their customers.[65]

---

[61] *FTC Recordkeeping Comments* at 4.

[62] *KYC Further Notice* at ¶ 27.

[63] *See* 47 C.F.R. § 64.1200(n)(4).

[64] *KYC Further Notice* at ¶ 6.

[65] *See, e.g.*, Letter from Keith Buell, General Counsel and Head of Global Public Policy, Numeracle, Inc., to Marlene Dortch, Secretary, FCC, CG Docket Nos. 17-59, 02-278, and 25-307 and WC Docket No. 17-97, at 5 (dated Mar. 25, 2026) ("Since the FCC Robocall Strike Force was convened in 2016, carriers have consistently argued that a light-touch approach would allow industry to self-determine the most effective solutions. That approach has failed.").

For these reasons, the State AGs support the Commission's commonsense proposals mandating that originating providers engage in specific and robust KYC processes for both their new and renewing customers. These measures are necessary to combat the anonymity leveraged by bad actors that have been permitted to operate in the shadows, and State AGs applaud the Commission for its willingness to push for accountability and improvements to protect the safety and security of this nation's consumers and its communications network.

BY [50] STATE ATTORNEYS GENERAL:

Kwame Raoul Illinois Attorney General	**Todd Rokita** Indiana Attorney General
Jennifer Davenport New Jersey Attorney General	**Jeff Jackson** North Carolina Attorney General
Andy Wilson Ohio Attorney General	**Dave Sunday** Pennsylvania Attorney General
Steve Marshall Alabama Attorney General	**Cori Mills** Alaska Attorney General

Gwen Tauiliili-Langkilde
American Samoa Attorney General

Kris Mayes
Arizona Attorney General

Tim Griffin
Arkansas Attorney General

Rob Bonta
California Attorney General

Phil Weiser
Colorado Attorney General

William Tong
Connecticut Attorney General

Kathy Jennings
Delaware Attorney General

Brian Schwalb
District of Columbia Attorney General

Chris Carr
Georgia Attorney General

Anne E. Lopez
Hawaii Attorney General

Raúl Labrador
Idaho Attorney General

Brenna Bird
Iowa Attorney General

Kris Kobach
Kansas Attorney General

Russell Coleman
Kentucky Attorney General

Liz Murrill

Liz Murrill
Louisiana Attorney General

Aaron M. Frey

Aaron Frey
Maine Attorney General

Anthony G. Brown
Maryland Attorney General

Andrea Campbell
Massachusetts Attorney General

Dana Nessel

Dana Nessel
Michigan Attorney General

Keith Ellison

Keith Ellison
Minnesota Attorney General

Lynn Fitch

Lynn Fitch
Mississippi Attorney General

Catherine L. Hanaway

Catherine Hanaway
Missouri Attorney General

Mike Hilgers

Mike Hilgers
Nebraska Attorney General

Aaron D. Ford
Nevada Attorney General

John Formella
New Hampshire Attorney General

Raúl Torrez
New Mexico Attorney General

Letitia James

Letitia A. James
New York Attorney General

Drew H. Wrigley

Drew Wrigley
North Dakota Attorney General

Gentner Drummond
Oklahoma Attorney General

Dan Rayfield
Oregon Attorney General

Peter F. Neronha
Rhode Island Attorney General

Alan Wilson
South Carolina Attorney General

Marty Jackley
South Dakota Attorney General

Jonathan Skrmetti
Tennessee Attorney General

Gordon C. Rhea
U.S. Virgin Islands Attorney General

Derek Brown
Utah Attorney General

Charity R. Clark
Vermont Attorney General

Jay Jones
Virginia Attorney General

Nick Brown
Washington Attorney General

John B. McCuskey
West Virginia Attorney General

Josh Kaul
Wisconsin Attorney General

Keith Kautz
Wyoming Attorney General