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

September 8, 2026

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

In the Matter of	)	
	)	
Call to Authentication Trust Anchor	)	WC Docket No. 17-97
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	

REPLY COMMENTS OF
FORTY-NINE (49) STATE ATTORNEYS GENERAL

I. Introduction

The undersigned State Attorneys General ("State AGs") submit these Reply Comments in response to the further public notice issued by the Wireline Competition Bureau.[1] This Current Further Notice seeks comment on the Federal Communications Commission's ("Commission") proposals that include mandating more rigorous "Know-Your-Upstream-Provider" ("KYUP") obligations on all voice service providers in the ecosystem, expanding KYUP obligations to include entities involved in STIR/SHAKEN implementation and oversight, and raising the standards for

[1] *See* Further Notice of Proposed Rulemaking, *Call Authentication Trust Anchor*, WC Docket No. 17-97; *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59 (adopted May 20, 2026) (hereinafter "Current Further Notice").

how voice service providers apply STIR/SHAKEN attestations to calls so attestations are more trustworthy.[2] These proposals build on the Commission's recent and successive efforts to combat illegal calls.[3]

The Commission correctly recognizes that any measures to stop unlawful and fraudulent calls are "only as effective as the voice service providers that implement them"[4] and, "when voice service providers fail to fulfill these responsibilities, these systems can break down, and illegal calls can find their way to consumers."[5] Because "illegal robocalls will continue so long as those initiating and facilitating them can get away with and profit from it[,]"[6] the State AGs applaud the Commission's efforts in the Current Further Notice to continue its mission to bring consumers meaningful relief from illegal robocalls and to restore trust in America's voice networks by attacking the problem at every point in the call path.[7]

---

[2] *Current Further Notice* at ¶ 2 ("The goals of our proposals are simple . . . cutting voice service providers that enable robocalls out of the voice ecosystem through improvements to know-your-upstream-provider (KYUP) requirements and STIR/SHAKEN oversight[.]").

[3] *Id.* at ¶ 3 ("The STIR/SHAKEN framework deters impermissible number spoofing, supports call traceback efforts, and provides information that informs providers' call analytics engines that are used to make call blocking and labeling decisions. . . . The know-your-customer (KYC) and KYUP rules require providers to conduct due diligence about the end users and voice service providers they serve. . . . STIR/SHAKEN and the KYC and KYUP requirements are critical elements of this multifaceted framework." (footnotes omitted)).

[4] *Id.* at ¶ 10 ("The STIR/SHAKEN framework is built on an expectation that providers will authenticate calls and do so with a proper attestation. . . . KYC requirements are only effective if providers meaningfully vet their customers.").

[5] *Id.*

[6] *See* Further Notice of Proposed Rulemaking, *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59; *Call Authentication Trust Anchor*, WC Docket No. 17-97 (Sept. 30, 2021) (Statement of Comm'r Geoffrey Starks). https://docs.fcc.gov/public/attachments/DOC-376196A3.pdf.

[7] *Current Further Notice* at ¶ 1.

In July 2026, broad bipartisan coalitions of State AGs almost unanimously demonstrated support for the Commission's recent commonsense proposals that sought to constrain access to resources and to the U.S. communications network itself by bad actors, and to obligate those that serve as gatekeepers to those resources and to the U.S. telephone network.[8] The undersigned State AGs build on the advocacy of those recent—as well as prior—filings of State AGs that support commonsense proposals that can and will serve to protect our consumers.

II. More Rigorous Directives on KYUP Obligations are Necessary

The Commission's KYUP rule "requires that all voice service providers '[t]ake reasonable and effective steps to ensure that any originating provider or intermediate provider, foreign or domestic, from which it directly receives traffic is not using the provider to carry or process a high volume of illegal traffic onto the U.S. network.'"[9] The Commission describes this rule as "a flexible KYUP requirement,"[10] since there is limited prescriptive guidance—if any—other than the directive that providers take "reasonable and effective steps" to ensure that their direct upstream customers are not using their network to traffic illegal calls onto the U.S. communications network.

---

[8] *See* Reply Comments of Fifty (50) State Attorneys General, *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 (filed Jul. 27, 2026) (hereinafter "KYC Reply Comments of 50 State AGs"); 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 (filed July. 7, 2026).

[9] *Current Further Notice* at ¶ 9 (quoting 47 C.F.R. § 64.1200(n)(5)).

[10] *Id.* at ¶ 12.

Nevertheless, although the FCC's current rule allowed "flexibility" in *how* providers implemented those requirements, voice service providers have had existing obligations for several years to take effective measures to mitigate illegal calls.[11] Further, even prior to the effective dates of 47 C.F.R. 64.1200(n)(4) and (n)(5), providers were prohibited under the Federal Trade Commission's Telemarketing Sales Rule ("TSR") from providing substantial assistance or support to sellers or telemarketers engaged in acts or practices which violate the certain provisions of the TSR.[12] Similarly, voice service providers may also be held liable under the Telephone Consumer Protection Act ("TCPA")[13]. The FCC's existing rules and obligations under the TSR and TCPA should have been sufficient to prompt voice service providers to take greater action to weed out

---

[11] 47 C.F.R. § 64.1200(n)(4) (eff. May 6, 2021); 47 C.F.R. § 64.1200(n)(5) (eff. Sept. 23, 2022).

[12] 16 C.F.R. § 310.3(b).

[13] *Att'y Gen. of Florida v. Smartbiz Telecom, L.L.C.*, 688 F. Supp. 3d 1230 (S.D. Fla. 2023) (allowing state, acting as *parens patriae* for its citizens in an action under the Telephone Consumer Protection Act, to proceed against telecom provider that continued to transmit fraudulent calls despite repeated notifications through trace-back requests that it was transmitting illegal calls); *Att'y Gen. of Florida v. Smartbiz Telecom, L.L.C.*, 2024 U.S. Dist. LEXIS 169135, at *15 and *20–21, 2024 WL 4251895 (S.D. Fla. Sept 19, 2024) (granting summary judgment against VoIP provider for violations of Telemarketing Sales Rule and Truth in Caller ID Act for knowingly "allow[ing] fraudulent calls to transit its network" and "transmit[ing] call traffic that caused consumers' caller identification services to display inaccurate or misleading information in furtherance of attempts to steal from the call recipients"); *Arizona et al. v. Michael D. Lansky L.L.C. et al.*, 2024 U.S. Dist. LEXIS 83642, at *48, 2024 WL 3657129 (D. Ariz. May 8, 2024) (denying defendants' motion to dismiss as complaint factual allegations "plausibly give rise to an entitlement to relief" for violations of the TSR and TCPA); *Mey v. All Access Telecom, Inc. et al.*, 2021 U.S. Dist. LEXIS 80018, 2021 WL 8892199, at *5 (N.D. W. Va. Apr. 23, 2021) (denying defendant's motion to dismiss claiming common carrier immunity where plaintiff alleged that defendant had transmitted spoofed robocalls to consumers where the complaint alleged that it was obvious to the carriers that they were transmitting illegal calls, they profited from transmitting them, and they could easily have blocked the calls); *Hurley v.* Messer *et al.*, No. CV 3:16-9949, 2018 U.S. Dist. LEXIS 171588, 2018 WL 4854082, at *14 (S.D. W. Va. Oct. 4, 2018) (finding that alleging the ability to stop illegal use of VoIP services and the failure to take action to do so, states a claim under the TCPA); Report & Order, In re Rules & Regulations Implementing the Tel. Consumer Prot. Act of 1991, 7 F.C.C. Rcd. 8752, 8779-80, at ¶ 19 (1992) (providing common carriers may be liable where they have a "high degree of involvement or actual notice of an illegal use and failure to take steps to prevent such transmissions").

end-user or upstream provider customers intent on misusing their services to originate or transit millions of illegal calls. While the State AGs recognize that a likely small percentage of providers are responsible for onboarding the bad actors that send the most significant volumes of illegal calls, the next logical step is to mandate baseline KYUP practices for all providers.

Further, allowing the proposals in the Current Further Notice to be implemented only as "best practices" creates no Commission mandate at all, and merely reiterates the current "flexible" implementation requirements that have not provided sufficient guardrails to obligate providers to act or to protect consumers and the U.S. communications network.[14]

Voice service providers are "the first line of defense" with respect to many robocall mitigation measures.[15] "When bad actor providers are in the ecosystem, those measures often fail, and so we believe it is important to ensure that voice service providers follow robust baseline KYUP practices."[16]

When considering the KYUP-related proposals in the Current Further Notice and the KYC-related proposals in the Commission's recent KYC Further Notice,[17] it may appear that the terms KYUP and KYC have substantive distinctions. And, perhaps, in a way they do, in light of the Commission's use of these terms. For instance, in these Notices, the term "KYC" is used in connection with due diligence practices for onboarding and retaining end user, non-provider, retail customers of originating voice service providers. The term "KYUP" is used in connection with

---

[14] *See Current Further Notice* at ¶ 40.

[15] *Id.* at ¶ 17.

[16] *Id.*

[17] *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").

due diligence practices by wholesale voice service providers for onboarding and retaining other voice service providers from which the wholesale provider receives call traffic. Yet, the purpose of both Notices and the accompanying proposals therein is the same: establishing and mandating practices for voice service providers that will ensure that their customers—be they retail end users or upstream providers—are legitimate and responsible entities that do not regularly, either actively or passively, initiate or traffic illegal calls.[18]

Additionally, in support of the proposals set out in the KYC Further Notice, 50 State AGs urged that "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."[19] The same can be said of providers that accept and route their upstream customers' call traffic through the U.S. communications network: knowing an upstream customer's true identity and understanding their business should be of paramount concern. Indeed, as the Current Further Notice recognizes, "robust KYUP practices are more feasible for providers to follow . . . because there are far fewer providers than there are end users."[20]

---

[18] *See, e.g.*, *Current Further Notice* at ¶¶ 14, 15 ("The existing KYUP rule gives voice service providers the flexibility to use the best methods to know their upstream providers and prevent them from transmitting illegal calls. But those benefits will only materialize if providers actually take accountability and adopt meaningful measures to know their upstream providers and act on that knowledge. . . . [W]e now believe it is necessary to establish certain baseline measures that all voice service providers must follow to help ensure the upstream providers they serve are legitimate and responsible entities that are unlikely to be the source of illegal calls."); *KYC Further Notice* at ¶ 8 ("To bring illegal callers out of the shadows, we seek comment on making our KYC rules more robust by specifying information originating providers must obtain from customers before they are granted access to its service to make calls, how they should verify that information, and how we can assess enforcement penalties that are proportionate to the harms that unwanted and illegal calls cause. Through this proceeding, the FCC aims to make it more difficult for scammers to originate illegal calls . . . .").

[19] *KYC Reply Comments of 50 State AGs* at 3.

[20] *Current Further Notice* at ¶ 17.

For these reasons, and to the extent that it is feasible to do so, the State AGs incorporate by reference those arguments and illustrative examples set out in the KYC Reply Comments of 50 State AGs that were advanced in support of the Commission's similarly focused KYC proposals.[21]

A. <u>The KYUP requirements must be strengthened to be effective</u>

Because providers have not effectively implemented KYUP practices despite their existing obligation to do so,[22] the potential benefits of KYUP have not materialized. The Current Further Notice proposes mandating five categories of baseline KYUP measures—the types of KYUP practices that "responsible voice service providers" have already adopted.[23] Since some providers have shown their willingness to exploit the current flexibility in implementation of the existing KYUP rule, the State AGs generally support the more rigorous stance advanced by the Commission in this Current Further Notice and offer the following additional comments on each of the five proposed measures.

1. *The State AGs support KYUP information collection (KYUP Category 1 Measures)*

The State AGs support the Commission's proposal to provide more concrete guidance about the information that voice service providers are expected to collect from their upstream provider customers. The State AGs agree that "it is beneficial to require providers to obtain this information directly from upstream providers because upstream providers are in the best position

[21] *See, e.g.*, *KYC Reply Comments of 50 State AGs* at 2–6, 8–22, 24–27.

[22] *See Current Further Notice* at ¶ 14 ("Indeed, record evidence suggests that some providers are failing to take action to cut off bad actor providers even though the universe of bad actor providers appears identifiable and even when the evidence against a particular provider is clear." (citations omitted)).

[23] *Id.* at ¶ 15.

to supply this information."[24] Consistent with the KYC Reply Comments of 50 State AGs supporting the Commission's efforts to strengthen KYC processes on originating traffic, the State AGs support this effort in part because of obstacles State Attorneys General Offices ("State AGOs") have encountered when attempting to contact some providers, and because issues concerning the accuracy and completeness of this information are not isolated to the customers of originating or gateway providers.[25] Rather, in conjunction with the KYC obligations on originating providers, specific obligations for all providers to collect true, complete, and accurate information from and about their upstream providers customers will only better protect the U.S. telephone network and the consumers that rely on that network.

Specifically, the State AGs enthusiastically support requiring providers to collect a physical address that is a real place of business for their upstream providers. Efforts to obtain information from upstream providers sometimes proves to be difficult or impossible because the addresses providers share are either not legitimate or are not monitored by the provider.[26] For these reasons, State AGs support the proposal that neither a shared office location nor the address of a registered agent would suffice to meet the requirement to collect a valid business address.[27]

The State AGs further support the Commission's proposal to require providers to collect information about the identities of the "human principals, owners, and company leadership . . .

---

[24] *Id.* at ¶ 20.

[25] *See, e.g.*, *KYC Reply Comments of 50 State AGs* at 9 (citing the 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)).

[26] *Id.* at 9–10.

[27] *Current Further Notice* at ¶ 20.

[and] information about the company's parents, affiliates, and subsidiaries."[28] Specifically, given the uptick in the use of "shelf" or "aged" companies,[29] the State AGs support the Commission's proposal that providers look deeper than the corporate formation paperwork filed with a Secretary of State when evaluating the risk an upstream provider might present. In addition, some of the undersigned were plaintiffs in a multistate case where the injunctive relief they obtained prohibited an individual defendant from being involved in the business of robocalling. The defendant was nonetheless capable of subsequently forming at least two additional businesses that transmitted illegal robocalls and, more importantly, found voice service providers to transmit his traffic. He accomplished this by putting his stepfather—a man who had a career as a home inspector with no previous experience in telecommunications—on the corporation's filings as the CEO while the defendant quietly ran the newly-formed businesses himself. That the defendant's inexperienced stepfather was purportedly the head of a voice service provider should have led to more careful vetting by downstream providers, but apparently did not.[30] The Commission's proposal that providers look deeper at a provider's credentials than merely the existence of corporate formation paperwork and consider whether the information in those corporate filings makes sense should reduce bad actors' ability to transmit illegal calls.

The Commission is also correct to require that voice service providers conduct KYUP on upstream providers by not only collecting information, but also by making reasonable judgments about whether the upstream provider's information presents a heightened risk. Providers should make these judgments and follow up, if necessary, before agreeing to take traffic from an upstream

---

[28] *Id.*

[29] *KYC Reply Comments of 50 State AGs* at 11.

[30] *See, e.g.*, *id.* at 13 n.33.

provider. The State AGs support this approach as a reasonable corollary to requiring KYC by an originating provider before allowing retail customers to access the U.S. communications network.[31]

2. *The State AGs support KYUP compliance review (KYUP Category 2 Measures)*

The State AGs further support a requirement that providers conduct due diligence of an upstream provider's compliance with Commission rules. The types of data the Commission suggests collecting are appropriate to determine whether voice service providers comply with the bare minimum of the Commission's rules. However, the State AGs caution that the required filings are not always carefully vetted, and the existence of these filings alone should not constitute sufficient compliance review.

For instance, the robocall mitigation plans ("RMPs") in the FCC's Robocall Mitigation Database ("RMD") do not always include accurate information. As recently as October 2025, State AGOs have found that relying on the address, email, or phone number that a voice service provider uses in its RMD filing or in its accompanying RMP can be fruitless. The addresses in those plans sometimes lead to unmonitored, fake, or abandoned locations; calls to the numbers are not answered; and email addresses are either unmonitored or also fake.[32]

---

[31] *See id.* at 12.

[32] For example, while conducting discovery in the matter of *State of Arizona, et al. v. Michael Lansky, dba Avid Telecom, et al.*, No. 4:23-cv-00233 (D. Ariz. 2023), the plaintiffs attempted to serve many of the corporate defendant's upstream providers with subpoenas for records, relying on the addresses for the upstream providers listed in the RMD. Many of those subpoenas were returned as undeliverable. Some were delivered to people or companies who had no relationship to any voice service provider, had never heard of the upstream provider, and had been at their address for many years. Examples of difficulties with phone numbers and email addresses listed in the RMD abound and tend to turn up early in investigations when investigators seek informal contact with voice service providers.

Furthermore, the State AGs caution that some voice service providers submit RMPs with insufficient, incorrect, or overtly improper content. As one U.S. Senator observed: "[S]o many are thumbing their nose at a requirement with the mitigation plan. Submitting blank documents, documents that are intended to be rude or menus or whatever nonsense is also being submitted shows that it's not working, that there's a loophole somewhere that's been created, that there's no attention to the prosecution side if you will or the requirements for the mitigation plan[.]"[33]

Moreover, it is not clear that other sources of publicly filed information are more accurate. The State AGs believe that there are similar issues with the veracity of information in Form 499 filings. As the corporate representative for the Industry Traceback Group said under oath during a deposition, "the form 4-99 is . . . not that hard to get."[34]

Because of these experiences concerning inaccuracies and deficiencies in entries in both the FCC's RMD and with Form 499 filings, the State AGs urge the Commission to consider requiring voice service providers to verify information in legally required filings in at least two circumstances. First, when the provider determines that the information provided by the upstream provider customer conflicts with the information filed with the FCC, and second, when the compliance review reveals a facially defective filing. Facially defective filings by an upstream can include, but should not limited to, leaving required information blank, certifying that it has fully or partially implemented STIR/SHAKEN but is not an authorized SPC token holder, or submitting an RMP that is in some way defective or presents cause for concern.

---

[33] *Protecting Americans from Robocalls, Hearing Before the Subcomm. on Commc'ns, Media, & Broadband of the S. Comm. on Com., Sci., and Transp.*, 118th Cong. at 1:48:36 (Oct. 24, 2023) https://www.commerce.senate.gov/2023/10/protecting-americans-from-robocalls (statement of Sen. Ben Ray Luján).

[34] Bercu Dep., 157:25-158:2, Aug. 9, 2023, *Florida v. SmartBiz Telecom, LLC*, No. 1:22-cv-23945-JEM (S.D. Fla. 2022).

In addition, the State AGs applaud the Commission for its proposal to require voice service providers to consider an upstream provider's traceback history when evaluating compliance. In particular, the State AGs welcome the Commission's proposal that voice service providers consider both the volume of tracebacks and the number of tracebacks with a non-responsive provider in the call path in evaluating compliance.[35] To ensure that this is feasible, the State AGs encourage the Commission to continue publishing traceback data in its annual report to Congress[36] and its Traceback Transparency Report.[37] The State AGs are aware that it will soon be possible for voice service providers to request an upstream provider's traceback history directly through ITG Insights as part of the onboarding or ongoing monitoring of the upstream provider.[38] Given the resources that are or will soon be available to voice service providers to evaluate an upstream provider's traceback history, the State AGs support this effort by the Commission to require providers to more thoroughly vet their upstream providers.

Finally, the State AGs suggest that the Commission consider adding public actions by state attorneys general and/or the State AG Anti-Robocall Multistate Litigation Task Force[39] to the list

---

[35] *Current Further Notice* at 84 (referencing proposed 47 C.F.R. § 64.6305(a)(2)(i)).

[36] *See, e.g.*, Fed. Commc'n Comm'n, Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information (Dec. 23, 2025), *available at* https://www.fcc.gov/document/fcc-submits-traced-act-2024-annual-report-congress.

[37] *See, e.g.*, Fed. Commc'n Comm'n, Report on Traceback Data for the Period of April 1, 2023 Through June 30, 2023 (Sep. 29, 2023), *available at* https://www.fcc.gov/document/fcc-releases-traceback-transparency-report.

[38] Comments of Industry Traceback Group, *Enhancing Know-Your-Upstream-Provider Requirements and Strengthening STIR/SHAKEN (Call Authentication Trust Anchor; Advanced Methods to Target and Eliminate Unlawful Robocalls)*, WC Docket No. 17-97; CG Docket No. 17-59; at 4–5 (filed Aug. 7, 2026).

[39] The State AG Anti-Robocall Multistate Litigation Task Force (alternatively "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

of data points a voice service provider should consider when reviewing an upstream provider's compliance with state and federal laws.[40]

3. *The State AGs support KYUP information verification (KYUP Category 3 Measures)*

The State AGs enthusiastically support the Commission's proposal that voice service providers verify the information they collect about their upstream provider customers. Although it should go without saying, requiring basic due diligence will prevent upstream providers that are either not legitimate businesses themselves or are connected with principals or businesses with histories of questionable conduct and business practices from accessing the U.S. communications network.

Voice service providers should manually verify the phone numbers and emails that upstream provider customers furnish to the provider during the onboarding process. The voice service provider should also confirm the accuracy of this contact information on an ongoing basis as it engages in required KYUP monitoring. Voice service providers should further manually verify the contact information an upstream customer provides in public filings to the FCC when that information differs from that which the upstream provider customer furnishes to the voice service provider.

The State AGs also strongly support requiring verification of an upstream provider's physical place of business. As discussed in Sections II(A)(1) and (2) above, State AGOs have had difficulty establishing contact with some providers using phone numbers, emails, and physical

---

messaging traffic routed into and across the country.

[40] State AG Anti-Robocall Multistate Litigation Task Force, Warning Notices, https://ncdoj.gov/protecting-consumers/telephones-telemarketing/fighting-robocalls/warning-notices/.

addresses in the RMD. Requiring voice service providers to verify information furnished by upstream provider customers, including checking the information furnished against that which is in public filings with the FCC, will improve the accuracy of the information available to law enforcement and others.

It is important that State AGOs and our federal law enforcement counterparts have the ability to serve voice service providers registered in the FCC's RMD with court documents and other formal demands. For this reason and others, it is imperative that the addresses upstream providers use be actual places of business. The State AGs suggest that, when there are indications that an upstream provider is using "a virtual address, shared office location without a dedicated suite or floor, P.O. Box, mail forwarding service, hosted server location, or an address shared by multiple unrelated or purportedly unrelated businesses,"[41] the voice service provider manually verify the address by sending certified mail, return receipt requested, to confirm that the upstream provider can be reached at that location.

Finally, the State AGs encourage the Commission to apply these same KYUP information verification requirements to all domestic service providers. The Commission advances a proposal that voice service providers be deemed either "foreign" or "domestic" based solely on where they are "created, incorporated, or organized."[42] The State AGs are wary of these proposed definitions, as making the location of incorporation the sole measure of whether a voice service provider is foreign or domestic has the potential to encourage foreign bad actors to set up artificial U.S.-based corporations. Should this happen, it would lead to the widespread circumvention of gateway

---

[41] *Current Further Notice* at ¶ 23 (suggesting that "a registered agent's address," which the Current Further Notice acknowledges cannot be "a physical address that is a real place of business"—*see id.* at ¶ 20—be added to this list of addresses that constitute a risk factor).

[42] *Id.* at ¶ 80.

provider obligations by moving the first legitimate US-based provider down in the call path. Gateway providers will be nothing other than disposable corporate entities created by foreign service providers by filing articles of incorporation with a Secretary of State.

The risk of foreign providers falsely manufacturing a U.S. presence is not hypothetical. In a 2023 deposition, Josh Bercu, the Executive Director of the Industry Traceback Group, testified about the ease with which foreign providers could set up a U.S. presence without having offices or staff in the country: "[W]e see a lot of providers that claim they're in the US and probably have no US presence. . . they register in Delaware or Wyoming . . . there's more entities . . . in the middle that are from a legal perspective in the US but . . . they have no presence in the US. . . . [T]hey would basically be there to enable some of the international traffic to get in to the US."[43]

KYUP conducted by domestic voice service providers will only be meaningful if, in addition to scrutinizing the location in an upstream provider's incorporation paperwork, they take additional steps to "deter bad actor foreign voice service providers from attempting to nominally establish themselves as domestic voice service providers."[44] KYUP should include verifying that the upstream provider customer maintains a physical office and staff in the United States, conducts business from a U.S. IP addresses, and uses U.S. bank accounts to pay for services rendered by the provider.

4. *The State AGs support KYUP monitoring (KYUP Category 4 Measures)*

In anticipation of the possibility that bad actors may circumvent initial KYUP vetting or start to transmit illegal traffic after the initial KYUP is complete, the Commission proposes

---

[43] Bercu Dep., 158:19-159:14, Aug. 9, 2023, *Florida v. SmartBiz Telecom, LLC*, No. 1:22-cv-23945-JEM (S.D. Fla. 2022).

[44] *Current Further Notice* at ¶ 80.

requiring voice service providers to implement several "baseline KYUP monitoring obligations."[45] The State AGs appreciate this realistic acknowledgement and support ongoing KYUP monitoring, both as a mechanism for identifying bad actor upstream providers that have circumvented initial KYUP procedures and as a method of responding to upstream providers whose business practices, although upstanding at the time of initial vetting, deteriorate into disrepute.

The Commission's proposed monitoring obligations include "checking the upstream provider's compliance with Commission rules related to the provision of service;" analyzing call analytics "to identify illegal or suspect calls or call patterns from each upstream provider;" evaluating information that an "upstream provider is transmitting illegal calls, failing to authenticate calls, or authenticating calls with improper attestations;" evaluating information that "presents inconsistencies with other KYUP information" associated with the upstream provider; and evaluating information "concerning the upstream provider's reputation."[46]

The State AGs support these proposed monitoring requirements as reasonable, commonsense measures to ensure that voice service providers are engaged in a continuing conversation with their upstream provider customers. Additionally, and so that providers are more likely to monitor their upstream provider customers, the State AGs encourage the Commission to set "specific monitoring timelines"—such as annually—"rather than the 'regularly,' 'ongoing,' and 'timely basis' proposed requirements."[47]

However, some updates should not be left for an annual review. Connected to the discussion of ongoing monitoring, the Commission asks if it should "direct providers to require,

---

[45] *Id.* at ¶ 24.

[46] *Id.*

[47] *Id.*

such as through interconnection agreements, that upstream providers update any information the upstream provider supplied within a certain amount of time of any change."[48] The State AGs approve of this proposed directive and think that the Commission's suggested 10-day time frame is appropriate.

Further, the State AGs encourage the Commission to mandate that providers require notification from their upstream provider customers of enforcement actions, formal and informal notice letters, and demands for information. Providers could incorporate this as a provision in their contracts with upstream provider customers. Although law enforcement sometimes advises providers of actions taken against upstream provider customers,[49] providers should expect proactive and prompt notification from their legitimate upstream provider customers of any such law enforcement requests or actions.

5. *The State AGs support KYUP responsive action (KYUP Category 5 Measures)*

The Commission's fifth category of baseline KYUP measures—responsive action—mandates voice service providers "to refuse or discontinue services to upstream providers who have not fulfilled compliance obligations."[50] The success of KYUP in combatting illegal calls depends upon providers' identification and removal of bad actors,[51] and the State AGs support the Commission's proposal for an "objectively reasonable standard to prevent subjective

---

[48] *Id.*

[49] *See, e.g.,* State AG Anti-Robocall Multistate Litigation Task Force, Warning Notices, Aug. 7, 2025 Notice Letters, *List of Downstream Providers Carrying Noticed Target Call Traffic*, https://ncdoj.gov/wp-content/uploads/2025/08/List-of-Downstreams-Providers-Carrying-Noticed-Target-Call-Traffic.pdf.

[50] *Current Further Notice* at ¶ 25 n.72.

[51] *See id.* at ¶ 14.

applications," especially those "where a provider fails to refuse or discontinue service when a reasonable provider would do so."[52] The Commission acknowledges that, "for some providers, the incentive to enter into business with other providers to drive revenue growth deters them from instituting even the most basic practices,"[53] and examples of such profit-focused behavior can be found in enforcement actions.[54]

To spur providers to eschew profit in favor of integrity, the State AGs support the Commission's proposed objective responsive action requirement and similarly support the proposed safe harbor specifically and for the limited purpose of affording some protection to providers that make "objectively reasonably decisions to refuse or discontinue service."[55] However, even given the proposed strengthening of the SPC token access policy, the State AGs do not support the creation of a "safe harbor from Commission enforcement of KYUP requirements if a provider provides service to an upstream provider that has and maintains an SPC token with specific regard to the KYUP requirements that would duplicate the token access policy requirements."[56] Given the possibility for bad actors' tactics to change, the State AGs believe that such a safe harbor would erode accountability. Since the barriers to obtaining the required KYUP information are minimal,[57] the costs of duplication would be minimal; accordingly, the State AGs discourage the creation of such a safe harbor.

---

[52] *Id.* at ¶ 25.

[53] *Id.* at ¶ 14.

[54] *See, e.g.,* Complaint at 52, *Indiana v. Startel Commc'n LLC et al.*, No. 3:21-cv-00150-RLY-MJD (S.D. Ind. Oct. 14, 2021) (alleging that, on the same day, a downstream provider sent (1) a notice to the upstream provider of scam calls being transmitted by the upstream and (2) a demand for payment of $10,000.00).

[55] *Current Further Notice* at ¶ 25.

[56] *Id.* at ¶ 39.

[57] *See id.* at ¶ 30.

The State AGs further note that the Commission's proposal to strengthen information verification, discussed in Section II(A)(3) above, demands that voice service providers meaningfully and thoroughly check the information furnished by upstream provider customers. Given the potential for conflict between profit and best practices, the State AGs have concerns about the level of due diligence some providers will bring to the task. Many examples exist of upstream providers changing names, addresses, and corporate owners when they receive negative attention due to tracebacks—sometimes with the knowledge and support of their downstream providers.[58]

For these reasons, the State AGs encourage the Commission to enforce strong KYUP standards and authorize other entities like the STIR/SHAKEN Governance Authority, the STIR/SHAKEN Policy Administrator, and the State AG Anti-Robocall Multistate Litigation Task Force to also take action to enforce KYUP practices as appropriate.

B. The State AGs support additional proposals related to KYUP

The Commission proposes three "triggers for when a voice service provider must perform these KYUP requirements":

(a) before entering into a service agreement with a new upstream provider;

(b) before renewing or renegotiating an agreement with an upstream provider that has an existing service agreement; and

(c) at any other time the voice service provider finds, receives, or is made

---

[58] *See, e.g.*, Robocall Enforcement Notice to All U.S.-Based Voice Serv. Providers: FCC Enforcement Bureau Notifies all U.S.-Based Providers of Rules Permitting Them to Block Robocalls Transmitting from One Owl Telecom Inc., 38 FCC Rcd. 6711, 6713 n.23 (Aug. 1, 2023) (referencing Skype chat in which the CEO of One Owl Telcom tells its downstream, Great Choice Telecom, to expect a new sign up under the name "One Eye" that day); FCC Enforcement Bureau Notifies All U.S.-Based Providers of Rules Permitting Them to Block Robocalls Transmitting from Lingo Telecom, LLC, 39 FCC Rcd. 1013,1013 (Feb. 6, 2024) (listing the myriad names Lingo had previously used, including Matrix Telecom, LLC, under which name it was issued a Cease and Desist Demand by the FCC).

> aware of information or evidence concerning an upstream provider.[59]

The State AGs endorse these proposed triggers but also, as discussed above,[60] encourage the Commission to "set more specific triggers for performing the KYUP requirements."[61] The repetition of regular review and monitoring would maximize the effectiveness of KYUP measures and reduce the likelihood of a bad actor upstream provider escaping notice.

The State AGs further support the requirement of a "one-time information collection, compliance review, and information verification KYUP review" for all of a provider's upstream customers, and the State AGs agree with the Commission's proposal to require such a one-time review within 6 months after the effective date of any rules arising out of this Current Further Notice.[62] As to the effective date of those rules, the State AGs believe that implementation should begin as soon as is feasible. If twelve months after *Federal Register* publication of a Report and Order or 30 days after OMB approval, whichever is later,[63] is as soon as is practicable for implementation, the State AGs support that timeline.

The State AGs concur with the Commission that there are not "meaningful barriers to voice service providers performing the proposed KYUP requirements."[64] As the Commission recognizes, providers are able to obtain the required information directly from their upstream provider customers, necessitating no more than a phone call or email in most cases.[65] And the State

---

[59] *Current Further Notice* at ¶ 16.

[60] *See supra* Section II(A)(4).

[61] *Current Further Notice* at ¶ 16.

[62] *See id.* at ¶ 16.

[63] *Id.*

[64] *Id.* at ¶ 30.

[65] *Id.*

AGs are confident that meaningful compliance reviews and monitoring can be conducted using "information from readily available public sources . . . [or] its own call analytics tools and monitoring practices, the ITG, the Governance Authority, the Commission and other federal agencies, state entities [], and other voice service providers."[66] The ITG's recently-launched Insights tool, which provides structured traceback history metrics on upstream providers along with a proprietary risk score, is just one example of a monitoring means available to providers. Additionally, given the lack of any significant barriers to the implementation of these KYUP requirements, the State AGs do not believe that small providers will face unique challenges to implementation and, consequently, the State AGs would not support any sort of exception for small providers.

Where compliance with these KYUP requirements would impose costs on voice service providers, the State AGs agree that "the greatest cost would be incurred by providers that have not implemented the most basic KYUP practices to comply with that existing obligation," and further agree that such a cost would be warranted.[67] Moreover, providers that "seek to enter into business with a number of upstream providers will also incur greater costs," again, the State AGs agree that "those costs are warranted as they will ensure that wholesale providers are employing proper measures to deter bad actor providers."[68] Similarly, although upstream providers will bear the costs of compiling the requested KYUP information, the State AGs agree with the Commission's assessment that those costs are warranted as, "the fact that they will have to provide information will . . . spur all voice service providers in the ecosystem to be more responsible actors."[69]

---

[66] *Id.*

[67] *See id.* at ¶ 36.

[68] *See id.*

[69] *Id.* at ¶ 37.

Like the Commission, the State AGs "remain concerned that certain providers may seek to circumvent [their KYUP] obligations."[70] Accordingly, the State AGs support the Commission's proposed liability standard: a provider should be held accountable if it "knew or should have known that an upstream provider is using its network or services to transmit illegal calls."[71] Further, the State AGs believe that a provider's failure to meet any KYUP rules arising out of this Current Further Notice should be taken as evidence—or even rise to the level of a presumption—that a provider knew or should have known that its upstream provider was transmitting illegal robocall traffic.

Finally, while the State AGs agree with the Commission's belief that "KYUP obligations will require gateway providers to scrutinize the foreign voice service providers from which they accept calls,"[72] additional obligations on gateway providers would not be out of place, given the prevalence of illegal calls that enter the U.S. telecommunications network from abroad.

III. The Policies Set by the STIR/SHAKEN Governance Authority Should Incorporate KYUP Obligations

As recognized in the Current Further Notice, the STIR/SHAKEN framework is "predicated on trust," and its Governance Authority, including its Policy Administrator and Certification Authorities, together "establish[] and enforce[] the policies and procedures that determine which voice service providers can participate in the STIR/SHAKEN ecosystem so that authentication information is applied by *trusted entities*."[73]

---

[70] *Id.* at ¶ 41.

[71] *Id.*

[72] *See id.* at ¶ 126.

[73] *Id.* at ¶ 42 (emphasis added).

However, as the Commission appreciates, the STIR/SHAKEN Governance Authority's current policies and practices are not "sufficiently preventing bad actor providers from entering the STIR/SHAKEN ecosystem."[74] Thus, in order to remedy the current breakdown of trust in the STIR/SHAKEN framework resulting from "bad actor providers in the ecosystem that are not implementing the framework consistently or correctly[,]"[75] the State AGs agree that the designated STIR/SHAKEN Governance Authority—currently the STI-GA[76]—is most credibly positioned to restore that trust.[77]

The Current Further Notice proposes to mandate that the Governance Authority adopt improved policies to require voice service providers and Certification Authorities to comply with the STIR/SHAKEN framework and rules. As the Commission acknowledged, the Current Further Notice proposes a "more directed oversight approach with the Governance Authority" than was originally set forth by the Commission when the Governance Authority was established.[78] However, the Commission determined that oversight is now necessary to restore trust in the STIR/SHAKEN framework, and because it has identified problems that the Commission can address by requiring updated policies and procedures.

A. <u>Helpful Takeaways from Candid Conversations Between the Leadership Teams of the STI-GA and the State AG Anti-Robocall Multistate Litigation Task Force</u>

For more than two years, representatives from leadership of the Task Force have met

[74] *See id.* at ¶ 43.

[75] *See id.* at ¶ 42.

[76] *Id.* at ¶ 6 n.25 ("The role of Governance Authority is currently held by the Secure Telephone Identity Governance Authority.").

[77] *See id.* at ¶ 44 (acknowledging that "Commission intervention now is necessary to restore trust in the STIR/SHAKEN framework" and that the Commission believes it has the authority to "apply[] a more directed oversight approach with the Governance Authority").

[78] *See id.*

regularly with leadership from the STI-GA to discuss issues of concern and to identify where our collectives can work together to address illegal robocalling. These conversations have been helpful and frank. One issue that has been revisited since these meetings began precisely aligns with proposals in the Current Further Notice that would direct the Governance Authority "to revise its SPC token access policy to include baseline vetting requirements prior to the issuance of SPC tokens that are modeled off the KYUP requirements," and further proposes that these requirements "should also be applied to existing SPC token holders."[79]

The Task Force leads have repeatedly voiced their concern—a concern that is echoed in the Current Further Notice—that the policies and practices set forth by the STI-GA do not "sufficiently prevent[] bad actor providers from entering the STIR/SHAKEN ecosystem."[80] As the Commission articulates, the existing SPC token access policy "does not include an evaluation of whether a provider is a legitimate entity or provide the gatekeeping necessary to keep potential bad actor providers out of the STIR/SHAKEN ecosystem."[81] Rather, as it has been explained to the Task Force leads, in order for a voice service provider to be issued an SPC token and, ultimately, a certificate that will be used for caller ID authentication, the provider must only have completed three tasks,[82] none of which currently entail vetting, verification, or due diligence

---

[79] *Id.* at ¶ 45.

[80] *See id.* at ¶ 43.

[81] *Id.* at ¶ 45.

[82] These three tasks consist of: (1) filing an FCC Form 499-A with the Universal Service Administrative Company ("USAC"); (2) having been issued an Operating Company Number ("OCN") by the National Exchange Carrier Association ("NECA"); and (3) filing an entry in the RMD. *See* iconectiv, SHAKEN Policy Administrator, Secure Telephone Identity (STI) Service Provider Methods and Procedures, STI-PA Release 2.7, at 3–4 (released May 2026), https://authenticate.iconectiv.com/sites/authenticate/files/2026-06/STI-PA-US-METHODPROCSP-001-Rel-2.7-Issue-8-Onboarding-Guide-for-SP.pdf.; *see also* STI-GA Policy Decisions Binder v10.1, Policy 001: SPC Token Access Policy Version 1.2 (adopted May 2021), https://cdn.atis.org/sti-ga.atis.org/2024/05/03194346/210518-Policy-001-SPC-token-Access-v1-

concerning the legitimacy or validity of the filer or requesting entity.

However, before addressing the proposals set forth in the Current Further Notice on this issue, it may be helpful to first address some feedback that the STI-GA provided to the Task Force leadership representatives in conversations regarding STI-GA's involvement in scrutinizing providers that seek to gain access to the STIR/SHAKEN ecosystem.

STI-GA's position about the sufficiency of its policies and obligations, as reflected in conversations with the Task Force leadership, has primarily been two-fold. First, in its current form, the STI-GA is exclusively an industry collective, and STI-GA has asserted that asking the industry members that comprise the STI-GA to "police" or exclude fellow industry competitors from engaging in STIR/SHAKEN call authentication may be viewed as an anti-competitive tactic to put or keep their competitors out of business. Second, the STI-GA points out that the three requirements for issuance of an SPC token and certificate—a Form 499-A filing, a filing in the RMD, and an issued OCN—are only accessible from repositories administered either by the Commission itself or by an organization designated by the Commission. Thus, it has been STI-GA's position that, since the information upon which the STI-GA, the Policy Administrator, or the Certification Authorities rely to adjudge the legitimacy and identity of a provider is both submitted to, and subsequently made public by, law enforcement—in this case, the Commission or its designees—then why should industry be tasked with the responsibility of further scrutinizing the legitimacy and identity of providers?

On the first point, the State AGs appreciate the complexities and challenges facing industry members who make critical—and possibly negative—assessments about the legitimacy of their industry brethren, particularly when the denial of a request for an SPC token and certificate would

2-FINAL.pdf.

likely prevent a provider from routing call traffic onto or through the U.S. communications network and would likely put the provider out of business.

One proposal to address this first concern may be to broaden the membership base of the STI-GA—or any entity that is subsequently designated by the Commission to serve in the role of Governance Authority—to include non-industry members, such as state, local, and/or Tribal government regulators and telecommunications officials; consumer and community organizations; and other non-industry stakeholders or interested parties with relevant experience.[83] If the Commission endeavored to set guidelines to counter industry's anticompetitive concerns, it could mandate that the designated Governance Authority follow the model of the Commission's own recently disbanded North American Numbering Council ("NANC") and its working groups when considering its membership composition.[84] Further, the Commission could mandate that, regardless of the membership structure of the Governance Authority, the issuance and revocation processes for both certificates and SPC tokens expressly include non-industry representatives.

---

[83] *See, e.g.*, Public Notice, FCC, FCC Solicits Nominations for Rechartered North American Numbering Council Working Group Membership, at 2 (Jun. 1, 2023), https://docs.fcc.gov/public/attachments/DA-23-468A1.pdf ("The Commission will select members to balance the expertise and viewpoints that are necessary to effectively address the issues to be considered by the working groups.").

[84] For instance, in addition to industry members and associations, the NANC and/or its working groups included representatives of several state public utilities commissions; representatives from the National Association of State Utility Consumer Advocates ("NASUCA"); the Electronic Privacy Information Center ("EPIC"), a public interest research center; and representatives from several offices of state attorneys general designated on behalf of the National Association of Attorneys General. *See, e.g.*, Membership Directory, North American Numbering Council 2023–2025, https://www.fcc.gov/sites/default/files/NANC-Membership-Directory-for-Website-4-15-2025.pdf; Membership Directory, Call Authentication Trust Anchor (CATA) Working Group 2023-2025, https://www.fcc.gov/sites/default/files/CATA%20Membership%20Directory%20for%20website%205%2015%202024.pdf; Membership Directory, Numbering Administration Oversight Working Group (NAOWG) 2023–2025, https://www.fcc.gov/sites/default/files/NAOWG%20Membership%20Directory%20for%20website%209%2030%202024.pdf.

As to the second point, the Task Force leadership representatives regularly debated with the STI-GA regarding whether industry—in this case, specifically, the STIR/SHAKEN Governance Authority, the Policy Administrator, and the Certification Authorities—should be responsible for scrutinizing the legitimacy and identity of providers in some way other than the mere passive collection of the provider's OCN and its Form 499 and RMD filings. This brings us back to the Current Further Notice. As the Commission has set out quite plainly, the Commission does not believe—and State AGs agree—that the STIR/SHAKEN Governance Authority's current policies and practices are sufficiently preventing bad actor providers from entering the STIR/SHAKEN ecosystem.[85]

The State AGs support the Commission's efforts to "enhance the Governance Authority's role in serving as a gatekeeper to the ecosystem" by "requir[ing] that the Governance Authority adopt improved policies that include affirmative, effective measures to prevent voice service providers that are issued SPC tokens from transmitting calls that are not in compliance…and to prevent Certification Authorities from failing to comply" with a variety of regulatory frameworks.[86] The State AGs support the Commission's proposal that these policies include "enhancements for the issuance and revocation of SPC tokens and the selection and removal of Certification Authorities."[87] Applying more rigorous criteria to existing and prospective SPC token holders, as well as to Certification Authorities, along with the Commission's call for the Governance Authority to "tak[e] greater action to enforce those policies" will all serve to restore trust to the STIR/SHAKEN framework.[88]

---

[85] *See Current Further Notice* at ¶ 43.

[86] *Id.*

[87] *Id.*

[88] *See id.* at ¶¶ 43, 44

B. <u>The Governance Authority Should Mandate and Oversee the Implementation of KYUP Requirements for Providers Seeking SPC Token Access and Certificates, as well as for the Certification Authorities that Issue those Certificates</u>

As referenced above, in order to be issued an SPC token by the Policy Administrator, and thus, the digital certificate necessary to authenticate calls within the STIR/SHAKEN framework, a voice service provider need only have been issued an OCN, have filed a Form 499-A, and have an entry in the RMD. The State AGs have previously opined on concerns regarding the deficiencies and insufficiencies of filings in the RMD.[89] Additionally, the processes for filing Forms 499-A and requesting OCNs are pro forma, conducted without verification impediments or scrutiny as to the legitimacy of the filing or requesting entities. Therefore, if the STIR/SHAKEN framework is to be truly predicated on trust,[90] it should almost go without saying that allowing a provider the ability to authenticate calls in this trusted framework must only be a privilege bestowed upon those voice service providers that can—and have—first authenticated themselves.

Accordingly, the State AGs applaud and support the proposal requiring the Governance Authority to modify its policies to include KYUP information collection, compliance review, and verification requirements, as those KYUP categories are recognized, further supplemented, and illustrated herein.[91]

---

[89] *See, e.g.*, *supra* Section II(A)(2); Reply Comments of Forty-Seven (47) State Attorneys General, *Improving the Effectiveness of the Robocall Mitigation Database*, WC Docket No. 24-213; *Amendment of Part I 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 RMD 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. . . . These deficiencies include false, incomplete, or misleading contact information, blank or inapplicable mitigation plans, and representations which are contradicted by other FCC filings or publicly available sources.").

[90] *See id.* at ¶ 42.

[91] *See id.* at ¶ 45.

The State AGs further endorse the proposal that the Governance Authority should rely on these same meaningful and applicable KYUP collection, compliance, and verification processes to undertake some due diligence and vet entities seeking to become Certification Authorities prior to their selection, and should undertake this same due diligence on existing Certification Authorities.[92] In recent months, Task Force leadership has found that certain Certification Authorities ("CAs") are repeatedly identified as the issuing CAs for significant volumes of illegal calls. Task Force members do not know why certain CAs have a nexus of higher volumes of illegal or suspicious calls; it could possibly be because those CAs have lower price points, apply less scrutiny during the contracting process, enter into more favorable contracts with providers, or if there are other reasons altogether. Regardless, as the Commission recognizes, some CAs may be enabling illegal calls, and the State AGs support the proposals directing the Governance Authority to "take steps to identify bad actors before they are selected as CAs," ultimately "denying selection of an entity as a Certification Authority when there is a reasonable basis for believing the entity is unlikely to comply with the STIR/SHAKEN authentication framework, the Commission's STIR/SHAKEN rules, and/or the Governance Authority's policies."[93]

For these same reasons, the State AGs support requiring the Governance Authority "to establish a conflict of interest policy governing Certification Authorities' relationships with voice service providers,"[94] including and *particularly* when the CAs are also acting as voice service providers or have common ownership with providers for which the CA issues certificates. The State AGs appreciate the Commission's recognition that the issuance or revocation of certificates

[92] *See id.* at ¶ 46.

[93] *See id.*

[94] *See id.* at ¶ 47.

should be conducted at arm's length, ensuring the foundational trustworthiness of the parties given access to this framework intended to be one of trust. A conflict-of-interest policy currently exists with regard to common management and ownership between various entities including the STI-PA and CAs, as well as the STI-PA and service providers; that policy appears to be easily modified to add conflict of interest provisions regarding CAs and service providers.[95]

C. The Governance Authority Should Play a More Active Role in Collecting and Sharing Information that Should Result in Revocation of SPC Tokens or Removal of Certification Authorities

The State AGs further endorse the proposals that would require the STIR/SHAKEN Governance Authority to, as the Commission characterizes it, "play an active role" both in obtaining information about providers misusing their SPC tokens and take appropriate action on any information the Governance Authority receives or obtains,[96] and in seeking information, and taking action on information it receives, about Certification Authorities failing to follow the STIR/SHAKEN authentication framework, the Commission's STIR/SHAKEN rules, and/or the Governance Authority's policies.[97]

As the Commission recognizes, SPC token revocations by the Governance Authority in 2024 and 2025 were primarily due to nonpayment of required fees—fees which are determined by a contribution factor of .00002705%, where the maximum payment for the largest providers is $97,500, and the minimum payment for the smallest providers is only $450—and numbered less than one or two handfuls for failing to supply the required FCC Form 499 data or for subsequent

---

[95] STI-GA Policy Decision 007: Conflict of Interest Policy https://cdn.atis.org/sti-ga.atis.org/2025/08/27174200/SHAKEN-Framework-Conflict-Policy-Final.pdf.

[96] *Current Further Notice* at ¶ 48.

[97] *Id.* at ¶ 49.

removal from the RMD.[98] Further, the Governance Authority has not suspended or removed any CAs, despite certain CAs, as described above, issuing a disproportionate number of certificates to providers responsible for high volumes of illegal calls and/or applying improper attestations to their calls.[99] The State AGs urge the Commission to adopt those proposals that would mandate a hands-on approach by the STIR/SHAKEN Governance Authority to take action to do all that is required to govern this strata of, and framework in, the voice ecosystem, which includes setting more rigorous policies, overseeing and monitoring all authorized participants, and, when necessary, removing entities or revoking credentials that allow then access to, and authority in, this trusted framework.

Policies and procedures already exist that STI-GA and the Commission can actively utilize to oversee and monitor authorized participants and, when necessary, revoke access to and authority in the STIR/SHAKEN framework. Currently, policies and procedures have been adopted by the STI-GA to address how and why SPC tokens may be revoked, including compromised credentials of either the token holder or the Certificate Authority, or where the voice service provider has exited the ecosystem and closes its account with the STI-PA. In addition, the STI-GA "managed revocation process" takes effect in several situations, for example, when the voice service provider fails to adhere to STIR/SHAKEN policy or technical requirements, when the service provider demonstrates inappropriate use of a delegate certificate, falsification of information linked to the signing of a STI-GA recognized SHAKEN PASSport extension, or when directed by a court, the FCC or another body with relevant legal authority due to a violation of caller ID authentication

---

[98] *See id.* at ¶ 48 nn.100–01; *see, e.g.*, STI Governance Authority, *2025 STI-GA SHAKEN Report* at 2, 5–6, https://cdn.atis.org/sti-ga.atis.org/2026/02/20165621/2025-STIGA-Public-Report-Final.pdf; STI Governance Authority, *2024 STI-GA SHAKEN Report* at 2, 4, https://cdn.atis.org/sti-ga.atis.org/2025/02/19165205/2024-STIGA-Public-Report-Final.pdf.

[99] *Current Further Notice* at ¶ 49.

laws.[100] The revocation policy also includes a detailed process to be followed to enforce the policy including opportunities for appeal.

Additionally, the STI-GA currently has a policy to address Certification Authority Suspension and Revocation that also includes a detailed process aimed to enforce the policy.[101] The policy provides that a CA may have its authority revoked for violations of the Certification Policy, violations of the STI-CA Agreement, or security incidents. Rule 64.6308 of the Commission's rules then provides an opportunity for the parties aggrieved by STI-GA decisions to appeal to the Commission. Therefore, rather than creating new processes and procedures to address the issues regarding violations by service providers or Certification Authorities of the Commission's policies, rules and regulations, the Commission may require the Governance Authority and the Policy Administrator to more proactively pursue entities that appear to be violating their policies or the Commission's rules and utilize the processes currently in place. Moreover, the State AGs urge the Commission to expand the scope of these policies and procedures to cover additional issues, such as those associated with any new KYUP requirements for obtaining tokens or becoming a Certification Authority.

Further, the State AGs would support a more open reporting system regarding the Governance Authority's oversight and/or enforcement activity.[102] Currently the STI-GA token

---

[100] STI-GA Policy Decision 002: Certificate Policy, version 1.4.3 (adopted June 16, 2026) https://cdn.atis.org/sti-ga.atis.org/2026/06/30120552/260423-Policy-002-CP-v1-4-3-clean.pdf.

STI-GA Policy Decision 003: SPC token Revocation Policy, version 2.3 (adopted Oct. 1, 2024) https://cdn.atis.org/sti-ga.atis.org/2026/01/14133624/241004-Policy-003-SPC-token-Revocation-Policy-Final-v2.pdf;

[101] STI-GA Policy Decision: 006: CA Suspension and Revocation Policy, version 3 (adopted March 25, 2026). https://cdn.atis.org/sti-ga.atis.org/2026/03/26132149/260325-Policy-006-CA-Sus-and-Revoc-Policy-v3-0-Final.pdf.

[102] *See Current Further Notice* at ¶ 53.

Revocation policy provides that if the Board ultimately grants a complaint against a token holder, the STI-GA will post public notice of the revocation for cause.[103] The Revocation policy for Certification Authorities provides for notifications to external parties regarding violations to include the FCC, other federal or state agencies and STI Participants, as necessary, after the Initial Investigation Report as well as after the STI-GA Board's decision.[104] The State AGs do not have suggested modifications to these processes and instead, as otherwise discussed in these comments, look forward to the STI-GA's utilization of these processes and would like to be included as an entity that is provided with the notices described in the policies.

Accordingly, and in order to restore the trust that the STIR/SHAKEN framework set out to build and nurture, the State AGs support the proposals in the Current Further Notice that would mandate the adoption and active utilization of policies by the Governance Authority incorporating the commonsense due diligence KYUP information collection, compliance review, verification requirements and enforcement processes set out in the Current Further Notice as discussed herein.[105]

IV. STIR/SHAKEN Attestations Would Benefit from the Application of KYUP Requirements

State AGs agree that "[i]mproper attestations undermine the trust in and integrity of the STIR/SHAKEN framework, and its value in supporting efforts to combat illegal robocalls."[106] State AGs further agree that "the primary cause for improper attestations is a lack of specificity on

[103] STI-GA SPC Token Revocation Policy at ¶ 15.

[104] STI-GA CA Suspension and Revocation Policy at Steps 8 and 13.

[105] *Current Further Notice* at ¶ 12.

[106] *Id.* at ¶ 56.

what practices are permissible for satisfying each of the attestation-level criteria."[107] For these reasons, the State AGs support further action by the Commission to connect KYC and KYUP requirements to the practice of signing calls.

The Commission lays out the required relationship between an end user, the telephone number the end user is using to make the call, and the signer of the call. Representatives of the Task Force leadership have noticed that not all signers understand how to properly and consistently apply attestations. In conversations with signers who have improperly signed calls with, for instance, B level attestations on behalf of long-time customers where the signer does not know if the call is coming from the long-time customer or a reseller.

In at least one instance, in conversation with Task Force leadership, signers have admitted to signing calls for upstream providers that claim to have complete STIR/SHAKEN implementation but stopped signing their own calls due to a "problem." Task Force leadership has also discovered instances where signers are using C attestations when they originate the call and provide the phone numbers to the end user. These conversations cause Task Force leadership to believe that signers receive insufficient training to sign calls consistently and accurately.

As a first step to address the problem of improper attestation, the State AGs support the Commission's proposal to provide additional and express guidance about the attestation levels.[108] In doing so, the Commission will begin to remove any perceived ambiguity about the meaning of the attestation levels. However, further defining the attestation levels will not be sufficient to address the confusion that some signers still have about who is responsible for signing calls, and what information a signer has about the end user and their right to use the calling telephone

---

[107] *Id.* at ¶ 57.

[108] *Id.* at ¶ 59.

number. For this reason, the State AGs propose that the STI-GA or STI-PA develop training and rules that require signers to demonstrate familiarity with the attestation levels and their proper use, and that the STI-PA implement those rules before issuing an SPC token to any signer.

To further bolster efforts to ensure consistent and proper attestations, the State AGs support the Commission's proposal that a direct relationship with the customer must be established using the KYC or KYUP requirements.[109] State AGs wrote extensively in their KYC Reply Comments of 50 State AGs about their support for Commission proposals to establish clear and robust requirements for information collection and verification before a voice service provider establishes a relationship placing calls on the U.S. communications network for an end-user.[110] Throughout these Reply Comments, the State AGs have articulated support for similar information and verification requirements when the signing voice service provider's customer is an upstream provider.

The State AGs support the mechanisms the Commission proposes for establishing an end user's relationship with a phone number.[111] The State AGs support the Commission's clear, positive statement that a relationship between the customer and the calling number exists only in two situations. First, when the voice service provider signing the call itself assigned the telephone number to the customer either as an individual number or as part of a range of numbers. Or, second, when a customer presents the signing provider with a delegate certificate from the telephone number service provider that demonstrates the entity's authority to use the calling number.[112]

---

[109] *Id.* at ¶ 62.

[110] *See generally KYC Reply Comments of 50 State AGs.*

[111] *Current Further Notice* at ¶ 64.

[112] *Id.*

The State AGs appreciate and agree with the Commission's statement that a contractual agreement is *not* sufficient to establish the necessary relationship between an end user, the signing provider and a telephone number. The State AGs are acutely aware that Lingo Telecom, LLC, was the originating provider for thousands of deep fake robocalls, all of which it assigned A-level attestations.[113] Lingo assigned those calls A-level attestations because it assigned the customer some phone numbers, but not the ones used in this deep fake campaign.[114] The calls to which Lingo assigned A-level attestations were spoofed telephone numbers.[115]

Given this experience, the State AG applaud the Commission's strong statement rejecting as insufficient a contractual relationship in which the upstream or initiating provider certifies that it will only use numbers with which it has a verified association.[116] The State AGs likewise agree with the Commission that no association between the end user or signing provider and the phone number exists when the phone number is unallocated, unassigned or on a do not originate list.

V. Additional Observations About Improper STIR/SHAKEN Attestations

The State AGs support the Commission's proposal "to prohibit voice service providers from willfully assigning attestations that are higher or lower than permissible under the STIR/SHAKEN standards."[117] In communications between representatives of Task Force leadership and at least one originating provider, it has become clear that in some instances, originating providers are applying C-level attestations when the originating provider has a relationship with the initiating customer.

---

[113] *In the Matter of Lingo Telecom, LLC,* 39 FCC Rcd 9304, 9309 (2024).

[114] *Id.*

[115] *Id.*

[116] *Current Further Notice* at ¶ 65.

[117] *See id.* at ¶ 69.

Applying a lower than permissible attestation in an effort to ensure calls are transmitted with less scrutiny is not a proper use of STIR/SHAKEN attestations and should not be permitted. Representatives of Task Force leadership are also aware of situations when a voice service provider is affixing C-level attestations to calls that its upstream provider customer should have signed itself. These are calls originated by that upstream provider, where that provider has completely implemented STIR/SHAKEN and yet has not signed its own calls with an A-level attestation. The State AGs support the Commission's efforts to reduce or eliminate this misuse of STIR/SHAKEN in these ways.

VI. Closing Loopholes for Universal Implementation of STIR/SHAKEN

The State AGs also support the Commission's efforts to close the loopholes that may exist for implementation of STIR/SHAKEN and agree with the Commission's determination that the Commission's caller ID authentication rules apply to all voice service providers in a call path, including those providers that serve the end user initiating the call, those that place the calls onto the public network, non-gateway intermediate providers, gateway providers that receive calls from foreign originating or intermediate providers at their United States facilities and transmit them downstream, and the providers that terminate the calls.[118] The Commission notes that certain providers mistakenly "do not consider themselves subject to the caller ID authentication rules."[119] To the extent those providers exist, the State AGs agree that the Commission should take action to ensure that those providers recognize their obligations and comply with the Commission's rules.

For the STIR/SHAKEN process effectively and accurately to identify the calling party to those providers all along the call stream, all voice service providers involved in the transmission

---

[118] *Id.* at ¶ 71.

[119] *Id.*

of a call from the calling party to the called party must be STIR/SHAKEN compliant. On that basis, the State AGs agree that the Commission should ensure that its rules utilize consistent definitions of key terms, including the definitions of "voice service provider." [120] Use of consistent definitions of key terms across all Commission rules eliminates any efforts to profess confusion and better ensures compliance as well as enforcement of Commission rules. Therefore, the State AGs agree that the definition of "voice service provider," if not already, should be made consistent across the caller ID authentication, telemarketing, Truth in Caller ID and all other Commission rules apply to "voice service providers."[121]

Lack of consistency across Commission rules is a key reason, however, that the State AGs disagree with the Commission's proposed new definitions of "origination" or "originating provider."[122] For purposes of the caller ID authentication rules, the Commission proposes to change the definition of "origination" to "the technological act of placing a customer's outgoing call onto the network using the voice service provider's own facilities," and "originating provider" to "the voice service provider whose network performs the origination of a given call."[123] These new definitions would impose a limitation to the current application of the Commission's STIR/SHAKEN obligations to only a facilities-based provider that technically places the call on the public network instead of the voice service provider that directly serves the non-provider person or entity that initiated the call. These narrowed definitions of "origination" and "originating provider" conflict with the Commission's use of the term in the current caller ID authentication rules and other rules governing communications services.

---

[120] *Id.* at ¶¶ 75–76.

[121] *Id.* at ¶ 78.

[122] *Id.* at ¶¶ 85–88.

[123] *Id.* at ¶ 88.

For instance, Rule 64.1200, the Commission's rule embodying the KYC and KYUP requirements, uses the terms "originate" or some form of the word to refer to the act of a person or entity initiating a call or that person or entity's voice service provider initiating a call, not the act of a facilities based voice service provider placing the call on the public network. Some form of the word "originate" is further used in the broader sense 27 times in this consumer protection rule, including the provisions addressing call blocking by voice service providers. Using inconsistent meanings for origination in the KYC/KYUP rules vis-a-vis the STIR/SHAKEN rules —particularly as related as they are—would wreak havoc for service providers, the Commission and law enforcement authorities to determine compliance obligations and enforcement parameters.

The Commission's privacy rules also use the term "originate" in the broader sense to apply to the voice service provider that serves the end user directly, regardless of whether the service provider uses its own facilities to technically place the ongoing call onto the public network. For example, Rule 64.1601 (a)(1) reads, "Telecommunications carriers and providers of interconnected Voice over Internet Protocol (VoIP) services, in originating interstate or intrastate traffic on the on the public switched telephone network (PSTN) *or originating interstate or intrastate traffic that is destined for the PSTN (collectively "PSTN Traffic")* are required to transmit for all PSTN Traffic, the telephone number received from or assigned to or otherwise associated with the calling party to the next provider in the path from the originating provider to the terminating provider."[124] This example demonstrates clearly that "originate" is not limited only to the facilities based provider that technically places the call on the PSTN. The "originating provider" also includes a VoIP provider that initiates a call destined to the PSTN.

[124] (Emphasis added).

These are just two examples of potential inconsistencies demonstrating that modifying the definition of "originate" to exclude non-facilities based providers in one section of the Commission rules would be inconsistent with the Commission's use of the term in other rules and thereby introduce confusion for both voice service providers and those engaged in enforcement, which would hamper proper compliance with and enforcement of several Commission's rules.

VII. Proposals Concerning Implementation, Record Retention, and Enforcement Penalties are All Necessary to Ensure Compliance with the KYUP Processes

As 50 State AGs recently addressed in Reply Comments supporting the Commission's proposals set out in the KYC Further Notice, implementation of any rules that will help to mitigate the onslaught of illegal robocalls reaching our nation's consumers should be implemented as soon as is practicable.[125]

As is also reflected in the 50 State AGs recently filed Reply Comments, in order to better encourage compliance with the Commission's mandates, the State AGs further support the proposed base forfeiture amounts for violations concerning failures to follow KYUP requirements, improper attestations and unauthenticated calls, and for continuing violations for providers that have failed to implement STIR/SHAKEN.[126] As the Commission rightfully proposes, these violations should be on a per call basis in order to "better encourage compliance and thereby enhance consumer protections against illegal calls."[127]

And, lastly, on the issue of record retention, as 50 State AGs recently wrote recently:

> 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 [to the Federal Trade Commission] four years ago. Information

---

[125] *See, e.g.*, *KYC Reply Comments of 50 State AGs* at 24.

[126] *See Current Further Notice* at ¶ 131; *see also KYC Reply Comments of 50 State AGs* at 24–25.

[127] *Current Further Notice* at ¶ 131.

> 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, 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.[128]

This is also indistinguishably true of, and applicable to, the KYUP requirements at issue in the Current Further Notice. For these reasons, the State AGs roundly support the proposals requiring the retention of all KYUP information voice service providers collect "for each upstream provider for the entirety of any potential statute of limitations relating to the use of its network or services to transmit illegal calls."[129] Again, "[t]he small cost of retaining this information is more than offset by its value to law enforcement[,]"[130] and, ultimately, to our nation's consumers.

VIII. Conclusion

About six weeks ago, 50 State AGs filed Reply Comments with the Commission in support of commonsense proposals mandating that originating providers engage in specific and robust KYC processes for both their new and renewing customers.[131] The undersigned State AGs applaud and endorse the Commission's continued efforts to attack the problem of illegal robocalls at every point in the call path by proposing actions in the Current Further Notice designed to increase *all* voice service providers' accountability in fulfilling similar obligations.[132] As discussed herein,

---

[128] *KYC Reply Comments of 50 State AGs* at 25–26 (citing 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/conmient/FTC-2022-0034-002Q (internal footnote omitted)).

[129] *Current Further Notice* at ¶ 34.

[130] *KYC Reply Comments of 50 State AGs* at 25 (quoting 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)) (internal quotation marks omitted).

[131] *Id.* at 26.

[132] *Current Further Notice* at ¶¶ 1, 10–11.

the proposals in the Current Further Notice seek to do what industry, as a whole, has failed to accomplish—to set policies and processes requiring all providers to be accountable for, and meaningfully informed about, the providers that are given the privilege of accessing the nation's communications network.

The problem could not be more plainly stated: "Whether they actively collaborate with fraudsters, turn the other way when bad actors use their networks or services to transmit illegal calls or defraud consumers, or simply fail to implement policies and procedures to fulfill their regulatory obligations to stop such nefarious activity," voice service providers that "evade or ignore [the Commission's] rules undermine trust in the voice network and the effectiveness of tools designed to combat illegal calls."[133] Thus, the answer to this problem has been within the reach of providers and other industry stakeholders all along, since they have all been "well positioned to identify 'bad actor providers' and take rapid action to address them."[134] They have altogether failed to do so. For these reasons, the State AGs endorse the commonsense measures described herein that do no more than to put responsibility and accountability for diligence in the hands of those best positioned to safeguard our nation's consumers and the U.S. communications network.

BY FORTY-NINE (49) STATE ATTORNEYS GENERAL:

[133] *Id.* at ¶ 12.

[134] *Id.*

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

Kwame Raoul
Illinois Attorney General

Brenna Bird
Iowa Attorney General

Kris Kobach
Kansas Attorney General

Russell Coleman
Kentucky Attorney General

Liz Murrill
Louisiana Attorney General

Aaron Frey
Maine Attorney General

Anthony G. Brown
Maryland Attorney General

Andrea Campbell
Massachusetts Attorney General

Dana Nessel
Michigan Attorney General

Keith Ellison
Minnesota Attorney General

Lynn Fitch
Mississippi Attorney General

Catherine Hanaway
Missouri Attorney General

Mike Hilgers
Nebraska Attorney General

Aaron D. Ford
Nevada Attorney General

John Formella
New Hampshire Attorney General

Raúl Torrez
New Mexico Attorney General

Letitia A. James
New York Attorney General

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

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