APRIL 29, 2026

FCC FACT SHEET*
Enhancing STIR-SHAKEN to Combat Illegal Robocalls
Call Authentication Trust Anchor; Advanced Methods to Target and Eliminate Unlawful Robocalls
Further Notice of Proposed Rulemaking – WC Docket No. 17-97; CG Docket No. 17-59

Background: The Further Notice of Proposed Rulemaking (FNPRM) proposes measures aimed at enhancing STIR/SHAKEN as a tool to combat illegal calls. If adopted, the FNPRM will propose to: (1) improve know-your-upstream-provider (KYUP) requirements and STIR/SHAKEN oversight; (2) raise the standards to make attestations more trustworthy; and (3) close STIR/SHAKEN loopholes. The FNPRM also seeks comment on issues related to foreign-originated calls and proposes to streamline the Commission's STIR/SHAKEN rules. These proposals are aimed at ensuring that *all* voice service providers, at *all* points in the call path, are accountable and actively working to protect consumers from illegal calls.

What the Further Notice of Proposed Rulemaking Would Do:

- Propose baseline measures all voice service providers must follow, including: (1) collecting certain information; (2) evaluating compliance with certain Commission rules; (3) conducting due diligence to verify authenticity; (4) monitoring activities; and (5) refusing or discontinuing service when an upstream provider may be the source of illegal calls.
- Propose improved Governance Authority policies for issuing SPC tokens and selecting Certification Authorities and more assertive steps to enforce those policies.
- Propose to: (1) codify the attestation levels established in the ATIS standards and the criteria that apply to them; (2) set out requirements to satisfy the attestation-level criteria including closing an attestation knowledge gap; and (3) codify prohibitions on improper attestations that are implicit in the STIR/SHAKEN standards.
- Close STIR/SHAKEN loopholes by proposing to: (1) clarify definitions that govern providers' STIR/SHAKEN implementation obligations; (2) repeal the two remaining undue hardship extensions to STIR/SHAKEN implementation; (3) increase the value of STIR/SHAKEN attestations by requiring all providers that serve end users to make attestation-level decisions; and (4) ensure calls arrive at their destination with authentication information by prohibiting intentional call routing to strip such information, requiring blocking of unauthenticated calls, and requiring all intermediate providers to authenticate any unauthenticated calls they receive.
- Seek comment on how the proposals would serve to deter illegal calls that enter the United States from abroad, and whether the Commission should take further actions related to KYUP and caller ID authentication to combat the threat of problematic foreign-originated calls.
- Propose a comprehensive review of the Commission's existing STIR/SHAKEN caller ID authentication rules to simplify and clarify the rules, remove unnecessary redundancy, and ensure consistency, with the goal of enhancing providers' ability to understand their obligations.

* This document is being released as part of a "permit-but-disclose" proceeding. Any presentations or views on the subject expressed to the Commission or its staff, including by email, must be filed in WC Docket No. 17-97 and CG Docket No. 17-59, which may be accessed via the Electronic Comment Filing System (https://www.fcc.gov/ecfs). Before filing, participants should familiarize themselves with the Commission's *ex parted* rules, including the general prohibition on presentations (written and oral) on matters listed on the Sunshine Agenda, which is typically released a week prior to the Commission's meeting. *See* 47 CFR § 1.1200 *et seq*.

Before the
Federal Communications Commission
Washington, D.C. 20554

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

FURTHER NOTICE OF PROPOSED RULEMAKING*

Adopted: [] **Released: []**

Comment Date: (30 days after date of publication in the Federal Register)
Reply Comment Date: (60 days after date of publication in the Federal Register)

By the Commission:

TABLE OF CONTENTS

Heading Paragraph #

* This document has been circulated for tentative consideration by the Commission at its May 20, 2026 open meeting. The issues referenced in this document and the Commission's ultimate resolutions of those issues remain under consideration and subject to change. This document does not constitute any official action by the Commission. However, the Chairman has determined that, in the interest of promoting the public's ability to understand the nature and scope of issues under consideration, the public interest would be served by making this document publicly available. The Commission's *ex parte* rules apply and presentations are subject to "permit-but-disclose" *ex parte* rules. *See, e.g.*, 47 CFR §§ 1.1206, 1.1200(a). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules, including the general prohibition on presentations (written and oral) on matters listed on the Sunshine Agenda, which is typically released a week prior to the Commission's meeting. *See* 47 CFR §§ 1.1200(a), 1.1203.

I. INTRODUCTION

1. The Federal Communications Commission (Commission) is on a mission to bring consumers meaningful relief from illegal robocalls and restore trust in America's voice networks, and we have been attacking the problem at every point in the call path. Today's effort is the latest act in this undertaking.

2. The Commission has long promoted a competitive marketplace that gives new and innovative providers the power to bring people together through the voice network. But with great power comes great responsibility, and some voice service providers are not living up to the task. We propose an ambitious set of measures aimed at enhancing STIR/SHAKEN to ensure that all voice service providers[1] are taking action and fulfilling obligations to protect consumers from illegal calls. The goals of our proposals are simple: (1) 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; (2) raising the standards for how voice service providers apply STIR/SHAKEN attestations to calls so attestations are more trustworthy; and (3) closing STIR/SHAKEN implementation loopholes. We believe this approach, which is informed by input from industry stakeholders, is necessary to ensure that any baseline rules we adopt will measurably reduce illegal calls while also giving voice service providers the flexibility to address bad actors' evolving tactics. We believe these changes will not only improve the utility of STIR/SHAKEN, but will enhance the foundation for several Commission and private sector anti-robocall tools as well as support federal and state enforcement efforts, ultimately serving to restore trust in voice communications.

II. BACKGROUND

3. The Commission's rules work in concert to combat illegal calls at every point in the call path. Its numbering administration rules set the conditions under which providers may access telephone numbers and tracks their usage.[2] The STIR/SHAKEN framework deters impermissible number spoofing,[3] supports call traceback efforts, and provides information that informs providers' call analytics

[1] We use the term "voice service provider" and "provider," interchangeably, to refer to all initiating, originating, intermediate, and terminating providers, including facilities-based providers and non-facilities-based providers (inclusive of interconnected Voice over Internet Protocol (VoIP) resellers and Mobile Virtual Network Operators (MVNOs)). We propose to address these definitions herein.

[2] *See* 47 CFR § 52.13.

[3] Impermissible caller ID spoofing occurs when bad actors falsify caller ID information to deceive call recipients into believing the caller is someone they trust, exposing consumers to fraudulent and malicious activity. *See* FCC, *Caller ID Spoofing*, https://www.fcc.gov/spoofing (last updated Nov. 13, 2024); *Call Authentication Trust Anchor, Implementation of TRACED Act Section 6(a) — Knowledge of Customers by Entities with Access to Numbering Resources*, WC Docket Nos. 17-97 and 20-67, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3241, 3263, para. 48 (2020) (*First Caller ID Authentication Order and Further Notice of Proposed*

(continued….)

engines that are used to make call blocking and labeling decisions.[4] The Robocall Mitigation Database (RMD) rules serve as an important accountability and enforcement tool, as providers must submit filings to the RMD that include a STIR/SHAKEN implementation certification and robocall mitigation plan, and they may only accept traffic from other providers that have a filing in the RMD.[5] The traceback rules establish Commission oversight of a private-sector mechanism that relies in part on STIR/SHAKEN information and RMD filings to trace back suspected illegal calls to the source.[6] The know-your-customer (KYC) and KYUP rules require providers to conduct due diligence about the end users and voice service providers they serve.[7] And the call blocking rules establish mandatory and permissive call blocking requirements for illegal calls when they are discovered by using numbers that are impermissible for origination, by call analytics, and by traceback results.[8] STIR/SHAKEN and the KYC and KYUP requirements are critical elements of this multifaceted framework.[9]

4. *STIR/SHAKEN authentication framework.* The STIR/SHAKEN framework[10] is a set of technical standards and protocols that deter spoofing by enabling providers to authenticate and verify that the caller ID information transmitted with Session Initiation Protocol (SIP) calls matches the caller's number.[11] The framework involves two components: (1) the technical requirements for authenticating

---

Rulemaking). Telephone numbers may be spoofed permissibly in certain circumstances, such as when a business chooses to present its main contact number instead of a number it uses only to make outbound calls. *See*, *e.g.*, TransNexus, *Understanding STIR/SHAKEN*, https://transnexus.com/whitepapers/understanding-stir-shaken (last visited Apr. 27, 2026).

[4] *See* FCC, Wireline Competition Bureau, Triennial Report on the Efficacy of the Technologies Used in the STIR/SHAKEN Caller ID Authentication Framework at 17 (2025), https://docs.fcc.gov/public/attachments/DOC-416732A1.pdf (Second Triennial STIR/SHAKEN Report).

[5] *See* 47 CFR § 64.6305(g)(1)-(4); *Improving the Effectiveness of the Robocall Mitigation Database*; *Amendment of Part 1 of the Commission's Rules, Concerning Practice and Procedure, Amendment of CORES Registration System*, WC Docket No. 24-213, MD Docket No. 10-234, Report and Order, 40 FCC Rcd 599, 600-01, paras. 4-5 (2025) (*RMD Order*).

[6] 47 CFR § 64.1200(n)(1); *Advanced Methods to Target and Eliminate Unlawful Robocalls*; *Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Seventh Report and Order in CG Docket 17-59 and WC Docket 17- 97, Eighth Further Notice of Proposed Rulemaking in CG Docket 17-59, and Third Notice of Inquiry in CG Docket 17-59, 38 FCC Rcd 5404, 5412, para. 21 (2023) (*Seventh Call Blocking Order*); *see also* Industry Traceback Group, Policies and Procedures at 5 (Aug. 2025), https://tracebacks.org/wp-content/uploads/2025/09/ITG_Policies-Procedures_Aug_2025.pdf.

[7] *See* 47 CFR § 64.1200(n)(4)-(5).

[8] *See* 47 CFR § 64.1200(k), (n), (o). Providers that block calls consistent with the Commission's rules must make all reasonable efforts to avoid blocking calls from PSAPs and government outbound emergency numbers and never block emergency calls to 911 unless the provider knows without a doubt that the calls are unlawful. *See* 47 CFR § 64.1200(k)(5)-(6).

[9] Commission rules also govern end users that make calls using artificial and prerecorded voice messages, which are not relevant to the discussion here. 47 CFR § 64.1200(a)-(h).

[10] A working group of the Internet Engineering Task Force (IETF) called Secure Telephone Identity Revisited (STIR) developed several protocols for authenticating caller ID information. *See Call Authentication Trust Anchor*, WC Docket No. 17-97, Report and Order, 36 FCC Rcd 1859, 1862-63, para. 7 (2020) (*Second Caller ID Authentication Order*). The Alliance for Telecommunications Industry Solutions (ATIS), in conjunction with the SIP Forum, produced the Signature-based Handling of Asserted information using toKENs (SHAKEN) specification, which standardizes how the protocols produced by STIR are implemented across the industry. *Id.*

[11] *Id.* at 1862, paras. 6-7. The Session Initiation Protocol (SIP) is "an application-layer control protocol" "for creating, modifying, and terminating sessions" such as IP telephone calls. IETF, SIP: Session Initiation Protocol, RFC 3261 at 1 (2002), https://tools.ietf.org/html/rfc3261. The STIR/SHAKEN caller ID authentication framework only works on IP networks—that is, those networks with technology that is able to initiate, maintain, and terminate SIP calls. *First Caller ID Authentication Order and Further Notice*, 35 FCC Rcd at 3245, para. 7.

and verifying caller ID information, and (2) the governance system designed to maintain trust in the authentication information transmitted with a call.[12] The two components are set out in three standards that are published and periodically amended by the Alliance for Telecommunications Industry Solutions (ATIS):[13] ATIS-1000074 stipulates the technical requirements,[14] and ATIS-1000080 and ATIS-1000084 define the STIR/SHAKEN governance system.[15] Under Commission rules, all voice service providers,[16] including gateway providers[17] and non-gateway intermediate providers,[18] must implement STIR/SHAKEN in their IP networks, unless subject to an implementation exemption,[19] by complying with, *at a minimum*, the three ATIS standards and all of the documents referenced therein.[20]

[12] *Call Authentication Trust Anchor*, WC Docket No. 17-97, Eighth Report and Order, 39 FCC Rcd 12894, 12897, para. 6 (2024) (*Eighth Caller ID Authentication Order*).

[13] *Id.* at 12900, para. 9.

[14] *See* ATIS & SIP Forum, Signature-based Handling of Asserted information using toKENs (SHAKEN), ATIS-1000074.v003 (2022), https://access.atis.org/higherlogic/ws/public/download/67436/ATIS-1000074.v003.pdf/latestATIS-1000074 (ATIS-1000074).

[15] *See* ATIS & SIP Forum, Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management, ATIS-1000080.v006 at 1 (2025), https://access.atis.org/higherlogic/ws/public/download/82892/ATIS-1000080.v006.pdf (ATIS-1000080); ATIS & SIP Forum, Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators, ATIS-1000084.v003 at 1 (2023), https://access.atis.org/higherlogic/ws/public/download/70989/ATIS-1000084.v003.pdf (ATIS-1000084).

[16] 47 CFR § 64.6300(o) (defining "voice service" as "any service that is interconnected with the public switched telephone network and that furnishes voice communications to an end user using resources from the North American Numbering Plan or any successor to the North American Numbering Plan," and includes "[t]ransmissions from a telephone facsimile machine, computer, or other device to a telephone facsimile machine" and "[w]ithout limitation, any service that enables real-time, two-way voice communications, including any service that requires internet Protocol-compatible customer premises equipment and permits out-bound calling, whether or not the service is one-way or two-way voice over internet Protocol"). The Commission has interpreted the definition of "voice service" in section 64.6300(o) to only apply to the service provided by originating and terminating providers, and not intermediate providers. However, we propose to interpret "voice service" to now include the service provided by intermediate providers, and we use that broader interpretation here and throughout for clarity. *See infra* Section III.C.1.a.

[17] 47 CFR § 64.6300(d) (defining "gateway provider" as "a U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider" and further defining for the purpose of the rule "U.S.-based" and "receives a call directly").

[18] 47 CFR §§ 64.6300(i) (defining "non-gateway intermediate provider" as "any entity that is an intermediate provider as that term is defined by paragraph (g) of this section that is not a gateway provider as that term is defined by paragraph (d) of this section"), 64.6300(g) (defining "intermediate provider" as "any entity that carries or processes traffic that traverses or will traverse the public switched telephone network at any point insofar as that entity neither originates nor terminates that traffic").

[19] We use the term "exemption" here and elsewhere to refer both to exemptions from implementing STIR/SHAKEN and any applicable implementation extension granted by our rules.

[20] *First Caller ID Authentication Order and Further Notice of Proposed Rulemaking*, 35 FCC Rcd at 3258-59, para. 36 (finding that "[c]ompliance with the most current versions of these three standards as of March 31, 2020, including any errata as of that date or earlier, represents the minimum requirement to satisfy our rules"); *Advanced Methods to Target and Eliminate Unlawful Robocalls*; *Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Sixth Report and Order in CG Docket No. 17-59, Fifth Report and Order in WC Docket No. 17-97, Order on Reconsideration in WC Docket No. 17-97, Seventh Further Notice of Proposed Rulemaking in CG Docket No. 17-59, Fifth Further Notice of Proposed Rulemaking in WC Docket No. 17-97, 37 FCC Rcd 6865, 6887-88, para. 53 (2022) (*Gateway Provider Order*) ("Compliance by [gateway providers] with the most current

(continued….)

5. Under the STIR/SHAKEN technical requirements, voice service providers that are responsible for placing a call onto the IP network must authenticate calls by encrypting certain information about the call into a "PASSporT" and inserting the PASSporT and the location of a public key used to decrypt it into the "Identity header" of the SIP INVITE that travels with the call.[21] This information includes the authenticating provider's name and digital signature, the originating telephone number (i.e., the caller ID), and an attestation—A, B, or C—regarding the level of knowledge the authenticating provider asserts it has about its direct customer's identity and that customer's right to use the number transmitted.[22] In a typical scenario, the Identity header, inclusive of the encrypted PASSporT and public key location, travels with the call from the originating provider, through any intermediate providers, to the terminating provider. The terminating provider then uses the public key to decrypt the PASSporT, verifies the information, and can use the information in its efforts to prevent illegal calls.[23]

6. The STIR/SHAKEN governance system establishes how voice service providers may obtain the digital certificates necessary to authenticate calls. The certificates are designed to affirm that a voice service provider is the entity it claims to be, that it is authorized to authenticate the caller ID information, and that the caller ID information it is transmitting is trustworthy.[24] The governance system consists of: (1) a Governance Authority, which sets policies and procedures governing the application of the STIR/SHAKEN standards, including the conditions for the issuance and revocation of both certificates and the Service Provider Code (SPC) token necessary to obtain them, and selects the Policy Administrator;[25] (2) a Policy Administrator, which applies and enforces the policies set by the Governance Authority, including issuance of SPC tokens to voice service providers and approval of Certification Authorities authorized to issue certificates;[26] and (3) Certification Authorities, which issue the certificates used for caller ID authentication to voice service providers with SPC tokens.[27] Under the system, certificates expire after a certain time, so providers must periodically present their SPC token to the Certification Authority to get new certificates, thereby revalidating their authorization to participate in

versions of these standards as of the compliance deadline, along with any errata to the standards as of that date or earlier, represents the minimum requirement to satisfy our rules."); *Call Authentication Trust Anchor*, WC Docket No. 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd 2573, 2586, para. 22 (2023) (*Sixth Caller ID Authentication Order*) ("We adopt our proposal that non-gateway intermediate providers subject to the authentication obligation described above must comply with, at a minimum, the versions of the standards in effect at the time of their authentication compliance deadline. . . along with any errata."). Prior and current versions of the standards are available on the ATIS website. *See* ATIS, *Public Workspace, Documents* (last visited Apr. 27, 2026), https://access.atis.org/higherlogic/ws/public/documents?view=.

[21] *See Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12897, para. 6; IETF, Authenticated Identity Management in the Session Initiation Protocol, RFC 8224 at 5 (2018), https://datatracker.ietf.org/doc/rfc8224.

[22] ATIS-1000074 at 12-13.

[23] *Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12897, para. 6; *see also* ATIS-1000074 at 8-9; 47 CFR §§ 64.6300(n) (defining "verify caller identification information"), 64.6301(a)(3) (requiring terminating providers to verify caller identification information).

[24] *Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12897-98, para. 7.

[25] *Id.* The role of Governance Authority is currently held by the Secure Telephone Identity Governance Authority. *Id.*; *see also* Secure Telephone Identity Governance Authority, *STI Governance Authority*, https://sti-ga.atis.org (last visited Apr. 27, 2026).

[26] *Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12897-98, para. 7. The role of Policy Administrator is currently held by iconectiv. *See* iconectiv, *Industry Players*, https://authenticate.iconectiv.com/industry-players (last visited Apr. 27, 2026).

[27] *Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12898, para. 7. There are currently 11 Certification Authorities approved by the Policy Administrator. *See* iconectiv, *Approved Certification Authorities*, https://authenticate.iconectiv.com/approved-certification-authorities (last visited Apr. 27, 2026).

the STIR/SHAKEN ecosystem.[28]

7. The Commission permits voice service providers with a STIR/SHAKEN implementation obligation to engage third parties to perform the technological act of signing calls so long as the voice service provider with the STIR/SHAKEN implementation obligation: (1) makes all attestation-level decisions, consistent with the STIR/SHAKEN technical standards; and (2) ensures that all calls are signed using its own certificate obtained from a STIR/SHAKEN Certification Authority—not the certificate of a third party.[29]

8. *Know Your Customer (KYC).* The Commission's KYC rule requires that each originating provider "[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."[30] In April 2026, the Commission adopted a *KYC FNPRM* seeking comment on customer identification requirements for new and renewing customers and requirements for originating providers to verify, retain, and re-verify customer information.[31] This followed an October 2025 *Call Branding FNPRM* in which the Commission proposed to require voice service providers to transmit verified caller identity information to a consumer's device in instances when the provider chooses to transmit an A-level attestation to the consumer's device.[32]

9. *Know Your Upstream Provider (KYUP).* 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."[33] Voice service providers also must describe the measures they use to know their upstream providers in the robocall mitigation plans they must submit as part of their RMD filings.[34]

III. DISCUSSION

10. Commission measures to stop unlawful and fraudulent calls are only as effective as the voice service providers that implement them.[35] Numbering rules assume providers will use telephone numbers responsibly. The STIR/SHAKEN framework is built on an expectation that providers will authenticate calls and do so with a proper attestation. The value of the RMD is reliant on providers following their described robocall mitigation programs and only accepting traffic from providers with a filing that appears in the RMD. Tracebacks only work if providers respond to traceback requests. KYC requirements are only effective if providers meaningfully vet their customers. The call blocking rules depend on providers actually blocking calls when permitted or required. And the utility of some

[28] ATIS-1000080 at 28.

[29] *Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12903-04, para. 14.

[30] 47 CFR § 64.1200(n)(4).

[31] *See Advanced Methods to Target and Eliminate Unlawful Robocalls et al.*, CG Docket Nos. 17-59 et al., Further Notice of Proposed Rulemaking, FCC-CIRC2604-02, at 4, 16, paras. 9, 18 (rel. Apr. 9, 2026) (*KYC FNPRM*).

[32] *See Advanced Methods to Target and Eliminate Unlawful Robocalls et al.*, CG Docket No. 17-59 et al., Ninth Further Notice of Proposed Rulemaking in CG Docket No. 17-59; Seventh Further Notice of Proposed Rulemaking in WC Docket No. 17-97; Further Notice of Proposed Rulemaking in CG Docket No. 02-278; Public Notice in CG Docket No. 25-307, FCC 25-76, at 11, para. 30 (Oct. 29, 2025) (*Call Branding FNPRM*).

[33] 47 CFR § 64.1200(n)(5).

[34] *See* 47 CFR § 64.6305(d)(2)(ii), (e)(2)(ii), (f)(2)(ii).

[35] *See* Transaction Network Services Call Branding Comments at 3-4 ("[I]t is important for the Commission to remember that a chain is only as strong as its weakest link. Experience with the STIR/SHAKEN authentication framework and robocall mitigation practices have demonstrated that bad actors will exploit call origination points with the weakest protections.").

burgeoning call-branding solutions can be dependent on the effectiveness of STIR/SHAKEN and on the role providers play in verifying the identity of callers.[36] But when voice service providers fail to fulfill these responsibilities, these systems can break down, and illegal calls can find their way to consumers.

11. We propose a number of actions designed to increase voice service providers' accountability in fulfilling these obligations. First, we propose steps aimed at removing voice service providers that enable illegal calls from the voice ecosystem. Second, we propose to raise the bar for STIR/SHAKEN attestations to ensure that voice service providers are applying the correct attestations to calls. Third, we propose to close certain STIR/SHAKEN implementation loopholes to ensure ubiquitous and consistent deployment of STIR/SHAKEN on IP networks. Fourth, we address special circumstances related to TRS providers, foreign-originated calls, and public safety. We also propose and seek comment on related implementation considerations. We believe these proposed actions will not only enhance the effectiveness of STIR/SHAKEN, but will directly and indirectly improve the efficacy of the other Commission anti-robocall measures, thereby advancing the Commission's ultimate goal to restore trust in voice communications.

A. Cutting Off Providers That Enable Illegal Calls

12. 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 our rules undermine trust in the voice network and the effectiveness of tools designed to combat illegal calls.[37] Providers and other industry stakeholders have been well positioned to identify "bad actor providers" and take rapid action to address them.[38] The Commission established a flexible KYUP requirement that both empowers and obligates providers to identify bad actor providers and keep them from getting illegal calls onto the U.S. voice network. Similarly, the STIR/SHAKEN Governance Authority was designed to maintain trust in the STIR/SHAKEN framework by setting policies and procedures that govern which providers may be a part of the voice ecosystem. Despite these mechanisms, many bad actor providers remain.

13. We propose and seek comment on measures designed to improve how providers' KYUP obligation and the STIR/SHAKEN Governance Authority serve to excise bad actor providers from the voice network and deter them from establishing new operations to get back in. Although we are aware that bad actors will continue to look for new ways to commit fraud, we believe these actions will create friction that substantially undercuts the ability of bad actor providers to profit off of transmitting illegal calls. Specifically, we believe our proposals will disincentivize bad actor providers from attempting to gain access to the U.S. voice network by increasing both the costs they must incur to appear legitimate,

---

[36] *See, e.g.*, Letter from Keith Buell, General Counsel and Head of Global Public Policy, Numeracle, to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59 and WC Docket No. 17-97, at 1 (filed Mar. 24, 2025) (Numeracle *Ex Parte*) ("STIR/SHAKEN can be the foundation of a Rich Call Data-based ecosystem where identity information is inserted by originating service providers with meaningful standards and enforcement, and that information is passed to the terminating service provider for display on the device of the call recipient.").

[37] *See* Cloud Communications Alliance Call Branding Comments at 4 ("It is an unfortunate fact that some voice providers fail to undertake rigorous KYC processes or worse, proactively make their networks available to scammers and fraudsters."); ACA International Call Branding Comments at 7 ("We are concerned that relying on originating providers to apply rigorous KYC due diligence will not ensure trusted information. Unfortunately, bad actor originating providers may not apply a rigorous KYC approach, even if the Commission provides more guidance on KYC requirements (which it should) or, worse, they may turn a blind eye to fake information or affirmatively agree to include it."); *cf.* Transaction Network Services Call Branding Comments at ii-iii ("With fewer bad actors in the call ecosystem, any caller identity information that is transmitted would be more trustworthy, and TSPs could deliver more of this information to consumers.").

[38] Letter from David Frankel, CEO, ZipDX, to Marlene H. Dortch, Secretary, FCC, CG Docket Nos. 17-59, 02-278, and 25-307; WC Docket No. 17-97, at 1 (filed Oct. 19, 2025) (ZipDX Oct. 19, 2025 *Ex Parte*) ("We know from experience that enforcement cannot be left to the FCC alone; the problem is potentially overwhelming . . . .").

and the chances that their deceptive schemes will be discovered through ongoing monitoring practices that may result in their expulsion from the U.S. voice network. We seek comment on this assessment and on the potential impact of the requirements we propose.

1. Establishing Specific KYUP Requirements

14. 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.[39] Thus far, the Commission has declined to require that providers adopt specific KYUP measures,[40] opting to allow them to determine the best means to fulfill that responsibility.[41] However, we believe 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 to evaluate their upstream providers.[42] Other providers may not have implemented baseline practices because they do not take their KYUP obligations seriously. 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[43] and even when the evidence against a particular provider is clear.[44] Although stakeholders disagree on exactly what should be done to address providers' lax KYUP practices, many agree that better practices—and Commission action to achieve them—is needed.[45]

---

[39] AT&T Call Branding Reply at 6 ("Continuing efforts to restore trust in the complex communications marketplace that serves vastly different categories of customers requires providers to know their customer/upstream provider so that untrustworthy callers and entities are not allowed to place calls on the network.").

[40] Below we propose to define "upstream" and "downstream" to codify the relationships between providers, particularly as it relates to the application of any existing and future KYUP requirements. *See infra* Section III.C.1.g. Consistent with our description there, a non-facilities-based provider on the origination side of a call path is responsible for conducting KYUP regarding the providers to which it resells service, while a non-facilities-based provider on the termination side of a call path is responsible for conducting KYUP regarding the providers from which it purchases service.

[41] *See Gateway Provider Order*, 37 FCC Rcd at 6905, para. 98; *see also Seventh Call Blocking Order*, 38 FCC Rcd at 5421, para. 50.

[42] Numeracle Call Branding Comments at 6 ("Even if the Commission develops and enforces specific KYC practices, originating service providers still cannot be trusted as the entity to carry out those KYC practices because of a fundamental conflict of interest as those entities are financially incentivized to originate the calls. Originating carriers are compensated based on traffic volume, not traffic integrity."); ZipDX Triennial Report Comments at 3 ("Some token holders flaunt or ignore the rules and accept any customer that pays their bill.").

[43] Letter from David Frankel, CEO, ZipDX, to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59 and WC Docket No. 17-97, at 10-11 (filed Dec. 9, 2025) (ZipDX Dec. 9, 2025 *Ex Parte*) (showing that based on calls analyzed by ZipDX, "25 Carriers cover 80% of the illegal/unlawful calls" and "90% of the problematic calls come from 45 carriers"); TransUnion Call Branding Comments at 9 (noting that "89.4 percent of calls originated by the ten providers considered the most prolific generators of robocalls by TransNexus were signed with A-level attestation").

[44] *See, e.g.*, NCLC Call Branding Comments at 8 ("The Commission's SK Telco order illustrates that even where a provider has earned a bad reputation, that fact does nothing to prevent that provider from continuing to bombard consumers with scams and other illegal calls."); *id.* at 7 ("Downstream providers were continuously apprised of SK Teleco's role in originating scam robocalls through the numerous tracebacks conducted on these calls, yet downstream providers continued to allow SK Telco's scam calls through their networks.").

[45] *See, e.g.*, *id.* at 8 ("A better approach to solving the robocall problem would be to focus on promulgating strong rules requiring providers at all points in the call path to know their traffic and block calls of unknown legality. The Commission should direct its attention to rulemakings that will strengthen call blocking requirements and stop illegal calls before they ever reach consumers."); Letter from Joel Bernstein, Vice President, Head of U.S. Public Policy and Government Affairs, Somos, Inc., to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59 and WC

(continued….)

15. In light of this evidence, we 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. Specifically, we propose five categories of baseline measures that providers must follow to fulfill their obligation to know their upstream provider: information collection, compliance review, information verification, monitoring, and responsive action. We developed these categories and the included baseline measures using a variety of Commission and private-sector resources[46] and believe this framework is the logical outgrowth of the types of KYUP practices that responsible voice service providers use today. We seek comment on these categories and baseline measures. We also propose and seek comment on related issues, including appeals, barriers to performing KYUP responsibilities, use of third parties, compliance and recordkeeping responsibilities, implementation costs and cost recovery, and alternative approaches to various aspects of our proposed KYUP scheme.

16. We further propose triggers for when a voice service provider must perform these KYUP requirements. Specifically, we propose that they must do so: (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 aware of information or evidence concerning an upstream provider, such as through the monitoring practices we propose. We seek comment on these triggers, including whether we should set more specific triggers for performing the KYUP requirements.[47] Below we propose to require that the KYUP rules go into effect the later of 12 months after *Federal Register* publication of a Report and Order adopting the rules or 30 days after approval by the Office of Management and Budget (OMB) for rules that contain new or modified information collections subject to review under the Paperwork Reduction Act (PRA).[48] Accordingly, by the time the rules go into effect, providers would need to have processes and procedures in place to perform the KYUP requirements in accordance with the triggers. Additionally,

---

Docket No. 17-97, Attach. B (White Paper) at 8 (filed Nov. 19, 2024) ("A robust vetting process that determines the legitimacy of a party before any communication happens is key—and even if there are issues, an immediate ability to revoke privileges will reduce the incentive to use telephone identity to commit fraud."); Transaction Network Services Call Branding Comments at 6 ("TNS supports the Commission releasing clearer guidance on what practices will satisfy the Commission's KYC/KYUP requirements under its rules."); Verizon Call Branding Reply at 9 (supporting a Commission role in developing best practices).

[46] The resources include the proposals in the *KYC FNPRM*, prior enforcement determinations, the caller ID authentication best practices released by the Wireline Competition Bureau (Bureau) and the associated best practices adopted by the North American Numbering Council (NANC) Call Authentication Trust Anchor (CATA) Working Group, the i3 Forum Know Your Customer/Know Your Traffic Code of Conduct, and best practices identified by stakeholders in the Call Branding FNPRM record. *See, e.g.*, *KYC FNPRM*, FCC-CIRC2604-02, at 4, para. 9; *Lingo Telecom, LLC*, EB-TCD-24-00036425 NAL/Acct. No.: 202432170004, Order, 39 FCC Rcd 9304, 9318, para. 4 (EB Aug. 21, 2024) (*Lingo Order*); *Wireline Competition Bureau Issues Caller ID Authentication Best Practices*, WC Docket Nos. 17-97 and 20-324, Public Notice, DA 25-1526, at Appendices A, B (WCB Dec. 22, 2020); I3Forum KYC/KYT Code of Conduct; BCID Call Branding Comments at 10; NCLC Call Branding Comments at 11; American Bankers Association et al. Call Branding Comments at 23.

[47] *See, e.g.*, I3Forum, Know Your Customer/Know Your Traffic Code of Conduct at 9 (Oct. 2024), https://i3forum.org/wp-content/uploads/2025/09/i3Forum_KYC-KYT_CoC_24042025.pdf ("Customer accounts should regularly be reviewed for compliance with the KYC and KYT policies and with the compliance obligations of each pertinent jurisdiction. Scheduled reviews that confirm all information is up to date and the extent to which risk profiles may have altered can occur on a quarterly or annual basis, or according to the contract renewal cycle. Reviews may also be triggered by the following circumstances.

- The customer advises a change to the KYC information provided previously.
- The customer seeks approval for higher-risk products, higher capacity, a nonstandard use case etc.
- The traffic exceeds or nears a threshold or limit for the service being provided.
- There have been complaints about a customer or their traffic.").

[48] *See infra* Section III.E.4.

we propose to require that, within six (6) months *after* the rules go into effect, a provider must perform a one-time KYUP review for all upstream providers with which it has a service agreement at the time the rules we adopt go into effect if the provider has not already performed the KYUP requirements for a provider under the proposed triggers above.

17. We acknowledge that the KYUP requirements we propose above may be considered more prescriptive than the approach suggested in our recent *KYC FNPRM*, and we believe this is warranted. As we noted above, voice service providers are the first line of defense with respect to many of the Commission and private-sector robocall mitigation measures. 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. We also believe robust KYUP practices are more feasible for providers to follow than more stringent KYC practices for retail, small business, and enterprise end users because there are far fewer providers than there are end users.[49] Additionally, we believe that voice service providers will have a heightened awareness of the importance of responding to KYUP requests to ensure their calls go through than would retail and small businesses end users that may be unfamiliar with KYC and KYUP requirements that apply in the communications industry.

18. We believe these measures will realign provider incentives and further empower them to be another "cop on the beat" stopping bad actor providers from getting illegal calls onto the voice network.[50] The measures are meant to target upstream providers to which no reasonable voice service provider would provision service and ensure that all voice service providers are held to that same standard. We also believe that specifying KYUP requirements will provide a clearer foundation on which to hold providers accountable; providers that fail to take these obligations seriously may be subject to enforcement action. The measures we propose are not intended to be exhaustive, and if adopted, voice service providers would continue to have both the flexibility and an obligation to implement additional practices to respond to new tactics by bad actor providers in order to satisfy their obligation to prevent their networks and services from being used to transmit illegal calls.

19. *Strengthening the general KYUP requirement.* As the foundation for our proposed KYUP requirements, we propose to revise the baseline KYUP requirement in section 64.1200(n)(5) of our rules to establish an even more stringent obligation on voice service providers to prevent the transmission of illegal calls from upstream providers. Specifically, we propose to require that each voice service provider takes affirmative, effective measures to prevent an upstream provider from using its network or services to transmit illegal calls, including knowing its upstream provider. The proposed revised language focuses on the illegality of calls rather than traffic (consistent with how our rules typically apply) and cuts the "high volume of illegal traffic" limitation in the current rule to require that providers prevent all illegal calls. We also believe our proposed changes make clear our intent to apply this rule to all voice service providers, including both facilities-based providers and non-facilities-based providers.[51] We seek comment on this proposal and analysis.

[49] In May 2025, the Commission's Office of Economics and Analytics reported that as of June 2024, "there were 18 million end-user switched access lines in service, 65 million interconnected VoIP subscriptions, and 388 million mobile subscriptions, for a total of 471 million retail voice telephone service connections in the United States." FCC, Voice Telephone Services: Status as of June 30, 2024, at 2, https://docs.fcc.gov/public/attachments/DOC-411462A1.pdf. Conversely, as of April 21, 2026 there are only 10,872 voice providers with filings in the Commission's Robocall Mitigation Database, and we believe each provider only directly accepts traffic from a relatively small subset of these providers. *But see* Letter from Keith Buell, General Counsel and Head of Global Public Policy, Numeracle, to Marlene H. Dortch, Secretary, FCC, CG Docket Nos. 17-59, 02-278, and 25-307; WC Docket No. 17-97, at 3 (filed Apr. 9, 2026) (advocating that the Commission "establish robust KYC standards").

[50] Letter from David Frankel, CEO, ZipDX, to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59 and WC Docket No. 17-97, Attach. at 6 (filed Feb. 17, 2026) (ZipDX Feb. 17, 2026 Non-IP Authentication *Ex Parte*) (advocating for deputizing providers to combat illegal calls).

[51] We seek comment on definitions of "facilities-based provider" and "non-facilities-based provider" below. *See infra* Section III.C.1.f.

20. *KYUP information collection.* We propose to require that voice service providers collect directly from upstream providers, using mechanisms of their own choosing, the following information or an explanation for why the upstream provider cannot produce this information:

- General business information, including:
  - legal business name and supporting records (e.g., government record, government identification, lease, utility statement, search result from a government website, or report from a legitimate private database that validates company information);
  - any prior business names or trade names (DBAs) the company has used in the last three years;
  - a physical address that is a real place of business for the upstream provider and is not a virtual address, shared office location without a dedicated suite or floor, P.O. Box, mail forwarding service, hosted server location, registered agent, or address shared by multiple unrelated or purportedly unrelated businesses; and
  - contact information, including a business telephone number and email address;
- Financial information, including: billing address, forms of payment, financial institution, and account information;
- Internet commercial presence information, such as website, social media, or apps;
- Ownership and affiliate information, including:
  - information about human principals, owners, and company leadership (including ultimate beneficial owners and authorized business representatives), including their name, title, business telephone number, business email address, work address, country of residence, citizenship, and copies of government issued identification;
  - information about the company's parents, affiliates, and subsidiaries, including their business names, trade names (DBAs), place of incorporation, and principal places of business;
  - names, addresses (including country), email addresses, and ownership stake for all individuals with 10% or more direct or indirect ownership of the company; and
  - whether or not the provider or its parents, affiliates, subsidiaries, principals, owners, or leadership, and other companies where any such persons have served as a principal, owner, or leader, have been the subject of any criminal or regulatory investigations or actions in the past five years and the nature of such investigations or actions;
- Operational information, including:
  - place of formation and corporate formation records, including proof of good standing;
  - location of its principal operations, how long the company has been operating, and whether the company has any foreign ownership or management;
  - business registration number in its jurisdiction (such as federal or state Employer Identification Numbers (EINs) for United States providers and the foreign-equivalents for foreign providers); and
  - registered U.S. agent (if the provider has one);
- Service information, including:
  - information about the nature of the upstream provider's operations, including the types of services it offers, the types of customers it serves or intends to serve, and whether it relies

on non-Internet Protocol (IP) technology;[52] and

- o whether another voice service provider has refused or discontinued service to the upstream provider.

We believe that this is the basic amount of information necessary for a provider to be able to know their upstream providers. We also believe this information will help providers determine if an upstream provider is a foreign entity.[53] Are these views correct? Is there additional information we should require providers to obtain? For instance, should we require that providers obtain photos of certain individuals the upstream provider identifies with their government-issued identification? Is there any information listed above that providers should not be required to obtain? If not, why not? We believe it is beneficial to require providers to obtain this information directly from upstream providers because upstream providers are in the best position to supply this information. It may also serve to spur upstream providers to complete necessary steps to establish their business while deterring bad actor providers that may be disincentivized from taking the steps necessary to appear legitimate. Do commenters agree? We recognize that some of this information may be duplicative of information voice service providers must submit in the RMD, but to the extent providers would not collect this information directly from new upstream providers anyway, we think requiring providers to obtain this information will allow them to cross-check the information with the RMD to identify any inconsistencies.[54]

21. *KYUP compliance review.* We propose to require that voice service providers perform due diligence of upstream providers' compliance with Commission rules related to the provision of service by:

- confirming the upstream provider has a filing in the RMD[55] and reviewing the filing (including the robocall mitigation plan) to generally assess whether it is complete and compliant with Commission rules;[56]

[52] Below, we propose to prohibit voice service providers from accepting unauthenticated SIP calls, and to support that proposal, we believe voice service providers should know whether an upstream provider uses non-IP technology. *See infra* Section III.C.4. The TRACED Act—and the Commission's rules implementing it—use the general term "non-internet protocol" to capture networks that use types of technology other than IP. *See* 47 U.S.C. § 227b(b)(1)(B); 47 CFR § 64.6303. Such technology includes time-division multiplexing (TDM) technology, which often uses the Signaling System No. 7 (SS7) protocol instead of SIP. *See Second Caller ID Authentication Order*, 36 FCC Rcd at 1895, para. 69.

[53] NCLC Call Branding Comments at 11 ("Providers generally know when they are dealing with foreign upstream customers, as payments from these customers will often come through foreign financial institutions and the IP-address(es) the upstream provider uses to interconnect with the provider are suggestive of whether the customer is foreign or domestic.").

[54] We are exploring whether some entities are establishing dummy filings in the RMD that bad actors can use to quickly start transmitting unlawful traffic, and which may contain false or unverifiable information and are not properly updated. We intend to evaluate potential improvements to the RMD in a future proceeding.

[55] Providers can check the RMD in three ways: (1) searching the database by filer or keyword; (2) downloading a .csv file that lists the filings in the database; or (3) accessing the database using the application program interface (API). *See* FCC, Robocall Mitigation Database External Filing Instructions at 2-4 (Jan. 2026), https://www.fcc.gov/sites/default/files/rmd-instructions.pdf.

[56] Although we do not propose to specify exact requirements for this assessment, we believe providers should check whether a filing includes all required information, such as: principals, parents, affiliates, and subsidiaries, including, at a minimum, at least one natural person principal; operating company number (OCN) if the upstream provider has certified to complete or partial STIR/SHAKEN implementation (as an OCN is required to get an SPC token to implement STIR/SHAKEN); a valid exemption and a detailed basis for claiming the exemption if the upstream provider certifies to less than complete STIR/SHAKEN implementation; and a robocall mitigation plan that describes the upstream provider's robocall mitigation program, including KYC and KYUP measures. *See* 47 CFR § 64.6305(d)-(f) (listing the information providers must include in their RMD filings).

- confirming the upstream provider has obtained an SPC token if it certified in its RMD filing that it has fully or partially implemented STIR/SHAKEN;[57]
- determining whether the upstream provider appears on the Foreign Adversary Control System[58] or the Covered List;[59]
- determining whether the upstream provider has been subject to a Commission action revoking a Commission license; and
- determining whether the upstream provider has been the subject of any other final or preliminary Commission enforcement actions;[60]

In addition to these mechanisms, we believe that providers should evaluate an upstream provider's traceback history, including whether the upstream provider was the source of any tracebacks or failed to respond to any traceback requests, and we seek comment on how easily providers can obtain this information. Additionally, we believe that providers should try to ascertain, beyond just a general provision in a contract, whether an upstream provider actually has mechanisms in place to ensure its own customers, upstream providers, clients, employees, and contractors comply with federal and state laws and regulations concerning unlawful calls, including any KYC and KYUP requirements established by the Commission, and we seek comment on how and the extent to which providers can do this. We also seek comment on whether and how providers may determine whether a provider has been subject to numbering restrictions by the North American Numbering Plan Administrator (NANPA).[61]

22. We believe this compliance review is a sufficient baseline that providers can use to evaluate whether upstream providers are following Commission regulatory obligations without unnecessarily burdening providers with obligations that are inflexible or require comprehensive compliance reviews. We seek comment on these requirements and this assessment. Should voice service providers be required to perform more or less detailed compliance reviews? Should they confirm that upstream providers have an FCC Form 499 on file with the Commission? Should we require that contracts between voice service providers and upstream providers specifically address that the upstream providers will follow KYUP and KYC requirements established by the Commission, rather than just generic statements that the upstream providers will comply with all laws and regulations?

23. *KYUP information verification.* We propose to require that voice service providers conduct at least a basic level of due diligence to verify the validity and authenticity of an upstream provider, the information voice service providers obtain from or about an upstream provider, and the upstream provider's explanation for any information it could not produce, including:

---

[57] The STIR/SHAKEN Policy Administrator, iconectiv, maintains a list of providers with SPC tokens. *See* iconectiv, *Authorized Providers*, https://authenticate.iconectiv.com/authorized-service-providers-authenticate (last visited Apr. 27, 2026).

[58] *See Protecting Our Communications Networks by Promoting Transparency Regarding Foreign Adversary Control*, GN Docket No. 25-166, Report and Order, FCC 26-2, at 48-49, para. 75 (rel. Jan. 30, 2026).

[59] *See* FCC, *List of Equipment and Services Covered By Section 2 of The Secure Networks Act*, https://www.fcc.gov/supplychain/coveredlist (last updated Mar. 23, 2026). The Commission recently adopted a *Notice of Proposed Rulemaking* that proposes to exclude entities identified on the Covered List from providing domestic interstate telecommunications services pursuant to blanket authority under section 214 of the Act. *See Protecting Against National Security Threats in Domestic Telecommunications Service*, WC Docket No. 26-82, Notice of Proposed Rulemaking, FCC-CIRC2604-04, at 1, para. 1 (Apr. 9, 2026).

[60] This includes Forfeiture Orders, Consent Decrees, Final Determination Orders, Final RMD Removal Orders, Cease-and-Desist Letters, and Notices of Apparent Liability. *See* FCC, *Enforcement Actions*, https://www.fcc.gov/enforcement/orders (last visited Apr. 27, 2026).

[61] By numbering restrictions, we mean that the upstream provider has been prohibited from accessing numbers directly from the NANPA, has had its access to numbers suspended, or has had numbers reclaimed.

- confirming any telephone numbers and email addresses are active;
- participating in a verbal communication with one or more natural person principals, owners, or company leaders;
- conducting general research to identify risk factors or contradictory information, such as:
  - whether the physical address provided by the upstream provider represents a real place of business associated with the provider and is not 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;
  - whether there is contradictory information concerning the upstream provider's place of business, such as evidence the company is based outside the United States, including whether the company's IP address is associated with a foreign country or otherwise does not match the location information provided;
  - whether the principals, owners, and leadership of the upstream provider exist as natural persons;
  - whether there is any information that contradicts an upstream provider's claims about prior criminal or regulatory investigations or actions;
  - whether there is other evidence that raises questions about the upstream provider's legitimacy or reputation, such as a lack of digital presence for a purportedly established company; and
  - whether the upstream provider is owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary;[62]
- reviewing the upstream provider's Internet commercial presence information to identify risk factors or contradictory information, such as:
  - excessive spelling and grammatical errors, being created recently, apparent copying of another company's website, apparently fake customer reviews, or use of fake photos for leadership and listed employees (e.g., stock photos, potentially AI-generated photos, or photos of persons with no relationship to the provider); and
  - whether it contains information that contradicts the information supplied to the provider, including, but not limited to, different contact information, different leadership, or an inconsistent description of the nature of the services and types of customers served;
- conducting a basic comparative analysis of the information to identify inconsistencies in the information or consistencies with information concerning other upstream providers, such as:
  - different business names, addresses, contact information, email addresses or website domains, and individuals involved with the company;
  - similarities with other current or former upstream providers purportedly operating as unrelated entities, which may indicate the upstream provider is replacing a provider whose traffic was being scrutinized or blocked;[63] and

[62] *See Protecting Our Communications Networks by Promoting Transparency Regarding Foreign Adversary Control*, GN Docket No. 25-166, Report and Order, FCC 26-2, at 10, para. 15 (Jan. 30, 2026) (defining "owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary"); *id.* at 16-17, para. 22 (defining "foreign adversary" and "foreign adversary country").

[63] ACA International Triennial Report Comments at 14 ("A recurring problem undermining trust in the network is the practice of sanctioned bad actors simply reappearing as new companies."); Letter from Joshua M. Bercu,

(continued….)

- evaluating an upstream provider's financial information to identify risk factors, such as untraceable forms of payment (e.g., cryptocurrency or prepaid credit cards).

We believe that this level of due diligence sufficiently balances the need for providers to evaluate the information the upstream provider supplied without placing unreasonably burdensome or inflexible baseline requirements for that evaluation. We seek comment on these requirements and this assessment. Should we require providers to conduct more or less due diligence? Should we require providers to take additional steps to verify the identities of natural person principals, owners, and/or leadership, such as checking identity verification or reputation databases?[64] Should we require credit checks?

24. *KYUP monitoring.* To protect against bad actor providers who successfully circumvent initial KYUP vetting, we propose to require that voice service providers implement the following baseline KYUP monitoring obligations:

- regularly checking the upstream provider's compliance with Commission rules related to the provision of service, consisting of whether the upstream provider no longer has a filing in the RMD, has had its SPC token revoked, has been added to the Foreign Adversary Control System or the Covered List, has had a Commission license revoked, or has become the subject of any other Commission enforcement actions;
- using call analytics on an ongoing basis to identify illegal or suspect calls or call patterns from each upstream provider, including whether the upstream provider is transmitting traffic from a further upstream provider that the voice service provider knows no longer has a filing in the RMD, has had its SPC token revoked, appears on the Foreign Adversary Control System or Covered List, has had a Commission license revoked, or has been subject of a Commission enforcement action that denies its ability to provision voice service;
- evaluating on a timely basis information or evidence it finds, receives, or is made aware of that an upstream provider is transmitting illegal calls, failing to authenticate calls, or authenticating calls with improper attestations;
- evaluating on a timely basis whether any information or evidence it finds, receives, or is made aware of presents inconsistencies with other KYUP information obtained from or about the upstream provider, such as that:
    - the upstream provider or its employees are operating outside the United States, or its calls are originating outside the United States when it claimed it is a domestic provider;
    - the upstream provider's calls are originating in the United States when it claimed it is a foreign provider;
    - the upstream provider is providing different types of service or serving different types of customers than what was described;
    - the upstream provider's calls are sent over non-IP technology when the upstream

Executive Director, Industry Traceback Group, to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59 and WC Docket No. 17-97, Attach. at 10 (filed Jan. 14, 2026) (Industry Traceback Group *Ex Parte*) (noting that "[p]atterns of repeated and overlapping relationships may indicate intentional strategic obfuscation rather than isolated incidents" and that "[t]racebacks have identified groups of providers that appear to operate as alter egos of same entity" based on "indicators suggesting common control and operation").

[64] *See, e.g.*, Dun & Bradstreet, *Business Directory*, https://www.dnb.com/business-directory.html (last visited Apr. 27, 2026) (providing a database "covering hundreds of millions of business records to discover insights about companies").

provider did not specify it uses such technology;[65] and

- evaluating on a timely basis any other new information or evidence it finds, receives, or is made aware of concerning the upstream provider's reputation, such as a refusal or discontinuance of service by another provider.

We seek comment on each of these proposed requirements and whether we should specify additional KYUP monitoring obligations. For instance, should we specify the type of call analytics information providers must implement and evaluate?[66] Should we require that providers monitor when certificates have been revoked and not just SPC tokens?[67] Should we direct providers to require, such as through interconnection agreements, that upstream providers update any information the upstream provider supplied within a certain amount of time of any change, such as 10 business days?[68] Are there any obligations listed above that we should not require providers to follow? We also seek comment on whether we should set specific monitoring timelines, rather than the regularly, ongoing, and timely basis requirements.

25. *KYUP responsive action.* We propose to require that voice service providers perform a holistic, totality-of-the-circumstances evaluation of each upstream provider based on the information collection, information verification, compliance review, and monitoring measures described above and implement measures to refuse or discontinue service:

- when the results do not form an objectively reasonable basis for concluding that the upstream provider is a valid and authentic entity;
- when the results form an objectively reasonable basis for concluding that an upstream provider is likely to use or is using the network or services of the provider with the KYUP obligation to transmit illegal calls or enable the transmission of illegal calls;
- when the upstream provider does not have a filing in the RMD, transmits calls in IP but does not have an SPC token,[69] appears on the Foreign Adversary Control System or Covered List, has had a Commission license revoked, or has been the subject of any other Commission enforcement actions that deny its ability to provision voice service;[70] and

[65] Below, we propose to prohibit providers from intentionally initiating or routing a call over networks that do not support the transmission of STIR/SHAKEN authentication information, and we believe this proposed evaluation will support that proposal. *See infra* Section III.C.4.

[66] For example, the I3 Forum suggests that providers should implement the following call analytics measures: short call duration percentage; average call duration; answer seizure ratio (ASR); the percentage of call attempts blocked due to an improper CLI (invalid, unallocated, on a DNO list etc.); delivery receipt ratio (DLR); ratio of long code Sender IDs relative to short code Sender IDs; and ratio of long code Sender IDs relative to alphanumeric Sender IDs. *See* I3Forum, Know Your Customer/Know Your Traffic Code of Conduct at 9 (2025) (I3Forum KYC/KYT Code of Conduct), https://i3forum.org/wp-content/uploads/2025/09/i3Forum_KYC_KYT_CoC_202509.pdf. We note that Commission rules require providers to describe any call analytics they use to identify and block illegal traffic, including whether they use any third-party call analytics providers and the names of those providers. *See* 47 CFR § 64.6305(d)(2)(ii), (e)(2)(ii), (f)(2)(ii).

[67] Industry Traceback Group *Ex Parte*, Attach. at 7 (filed Jan. 14, 2026) ("A small number of providers continued to sign calls post-certificate revocation.").

[68] This would mirror providers' requirement to update the information they submit in the RMD within 10 business days. 47 CFR § 64.6305(d)(5), (e)(5), (f)(5).

[69] This relates to our proposal, below, to prohibit providers from accepting any SIP calls that are not authenticated with STIR/SHAKEN, as providers with a STIR/SHAKEN implementation obligation cannot authenticate calls without an SPC token. *See infra* Section III.C.4.

[70] We believe that providers are already obligated to refuse or discontinue services to upstream providers who have not fulfilled compliance obligations necessary to provision service or whose authority to provide service by

(continued….)

- when the provider finds, receives, or is made aware that an upstream provider does not have mechanisms in place to ensure its customers, upstream providers, clients, employees, and contractors comply with federal and state laws and regulations concerning unlawful calls, including any KYC and KYUP requirements established by the Commission.

We propose an objectively reasonable standard to prevent subjective applications where a provider refuses or discontinues service for anticompetitive purposes and where a provider fails to refuse or discontinue service when a reasonable provider would do so. To support providers taking responsive action, we propose that providers will not be subject to liability under the Act or Commission rules for objectively reasonable decisions to refuse or discontinue service. We seek comment on our proposal and whether it would serve our goal to remove bad actor providers from the voice network. What is the risk that providers would abuse their KYUP obligations for anticompetitive purposes? Are there other reasons we should require providers to refuse or discontinue service? Should we permit targeted call blocking based on providers' evaluations in certain circumstances, and if so, what circumstances? We also seek comment on potential economic or operational costs that could result if a provider refuses or discontinues service to valid and authentic upstream providers that are not in fact an actual or likely source of illegal calls due to a misapplication of the KYUP requirements.

26. We seek comment on whether our proposed approach will deter upstream providers from evading these requirements. Should we set a specific standard for when an upstream provider is using or likely to use the network or services of the provider with the KYUP obligation to transmit illegal calls or enable the transmission of illegal calls? Will these requirements successfully deter situations where bad actor providers create multiple shell providers, sometimes in multi-level arrangements, to try to avoid scrutiny by downstream providers? Will it address upstream providers that use traffic management techniques, such as mixing legal traffic with illegal traffic or transmitting illegal traffic for short periods of time on a repeated but occasional basis? Should we set a requirement to discontinue service based on percentages of calls within certain timeframes that are presumptively illegal based on call analytics? If so what should those percentages and timeframes be? Are there other standards we should set to address traffic management practices to evade our proposed requirements?

27. As part of this requirement, we propose to require that voice service providers document their decisions to refuse or discontinue service—including their findings, supporting documents, and conclusions—and provide this information, or a summary thereof, in a notice to the upstream provider. We propose to require that providers deliver the notice to an upstream provider five (5) business days prior to discontinuing service. We do not believe a timeline is necessary for when a provider declines to provide service so long as a notice is delivered. We do not propose to prohibit providers from accepting new information or explanations from upstream providers and reconsidering their decisions. We seek comment on these proposals and views. Should we prohibit providers from counseling upstream providers on how to resolve issues?

28. We seek comment on how quickly a voice service provider must complete evaluations and take responsive action when it finds, receives, or is made aware of information or evidence concerning an upstream provider, such as through monitoring practices. Should we require that providers complete evaluations and take responsive action as soon as feasible and no later than 30 days after finding, receiving, or being made aware of information or evidence? Does that time period adequately balance the need to stop illegal calls quickly with giving providers sufficient time to conduct evaluations and take responsive action? How much time should providers permit upstream providers to respond to any concerns?

29. *Remedies.* We believe that to the extent providers dispute whether a decision to refuse or discontinue service based on KYUP information is erroneous that they are positioned to remedy the disputes themselves. We seek comment on this belief. We also nevertheless seek comment on whether

---

Commission action has been revoked, but we believe that establishing a rule will more clearly put providers on notice of this obligation.

we should establish specific avenues for providers to remedy such disputes. We also seek comment on the costs associated with dispute resolution.

30. *Barriers to performing KYUP responsibilities.* We do not believe there are meaningful barriers to voice service providers performing the proposed KYUP requirements and we seek comment on this view. Because providers would obtain the required information directly from upstream providers, we do not believe there are barriers to obtaining that information. We believe providers have the means to conduct compliance reviews and monitoring using information from readily available public sources and will find, receive, or be made aware of information or evidence for monitoring purposes from its own call analytics tools and monitoring practices, the ITG, the Governance Authority, the Commission and other federal agencies, state entities (e.g., state Attorneys General), and other voice service providers. The proposed verification process would require fairly basic due diligence and we do not believe it would pose an unmanageable responsibility. Is there certain compliance information that providers would be unable to easily obtain, such as an upstream provider's traceback history? Are all voice service providers in the call path able to obtain information about an upstream provider's attestation practices? What about number access, license, and SPC token revocation information? Should we take steps to facilitate any necessary information sharing?[71] Do we need to revise our rules implementing Section 222's privacy protections to allow certain information sharing?[72] Are there any competitive concerns with facilitating sharing of the information described above? Would there be particular challenges for small providers in complying with our proposed KYUP obligations, and if so, how should we reduce the burden for such providers? Are there alternatives to the proposed information collection, compliance review, information verification, and monitoring obligations that would allow small providers flexibility to identify bad actors?

31. We also seek comment on any barriers to voice service providers refusing or discontinuing service. Are providers prevented from refusing service under federal or state laws or regulations in certain circumstances? We believe that most contracts between voice service providers include broad service discontinuance provisions that may be triggered by violation of applicable laws, and thus we believe that the discontinuance reasons we propose would be consistent with industry practice. Is this belief correct?

32. *Use of third-party KYUP services.* We propose to allow voice service providers to use third-party services to conduct some or all of their KYUP obligations. We believe that allowing providers to use third-party KYUP services may help reduce any costs that result from the KYUP requirements we propose, including for small providers, and we seek comment on the costs of these services relative to providers performing KYUP obligations themselves. We also believe that third-party services will be able to develop into information clearinghouses as they collect information about a wide number of voice service providers in the ecosystem and use that information to inform their KYUP determinations for all the providers they work with. We seek comment on whether we should designate one or more specific entities to be an information clearinghouse and require providers to use that entity for some or all the information they must obtain, and if so, which third parties we should select. Should we require providers to use the Global Legal Entity Identifier System (GLEIS) to obtain certain information?[73] While we propose to allow the use of third parties, we believe that the obligation to properly fulfill KYUP

[71] *See* Twilio Call Branding Comments at 6 (advocating for a safe harbor related to KYC practices, including information sharing with the Commission and other providers participating in the safe harbor).

[72] *See* 47 U.S.C. § 222; 47 CFR §§ 64.2001–64.2011.

[73] *See, e.g.*, Cloud Communications Alliance Call Branding Comments at 4-5 (arguing that the GLEIS is an independent verification process that should be the model or tool to verify the identity of a business entity in the call branding context and describing it as having a governance structure that resembles the STIR/SHAKEN governance framework but with global reach, oversight by regulators from various countries, and non-profit principles designed to ensure affordability); ACA International Call Branding Comments at 7-9 (same); *see also* GLEIF, *Our Vision: One Global Identity Behind Every Business*, https://www.gleif.org/en/about/our-vision (last visited Apr. 27, 2026) (the entity that administers the GLEIS).

obligations should remain with providers. This, we believe, will ensure that providers only work with legitimate third parties that have adopted KYUP practices that meet the baseline standards we establish.

33. *Compliance and recordkeeping responsibilities.* We believe that for voice service providers to fulfill their KYUP obligations, they will need to have adequate policies and procedures in place, and we seek comment on whether we should require providers to establish any specific policies and procedures. We note that the I3Forum Know Your Customer/Know Your Traffic Code of Conduct suggests that providers should "identify at least one person who will have particular responsibility for upholding the policy" and it suggests and describes the duties of that compliance leader.[74] Should we adopt such a requirement for the KYUP obligations? Should we require that providers implement close coordination between sales teams and compliance teams to ensure that the KYUP steps occur before a provider agrees to provide service to an upstream provider?

34. We propose that voice service providers retain the KYUP information they 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—i.e., for a minimum of four years.[75] We seek comment on this proposal. Should we consider a longer or shorter retention timeframe? What are the industry standard retention periods for business customer information? In the event we allow providers to use third parties to complete their KYUP obligations, the provider would maintain the obligation to supply the information in the event of an investigation under our proposals, and would therefore need to ensure it can obtain the information from the third party in a timely manner upon request.

35. We also seek comment on whether voice service providers should undergo any compliance reviews related to their KYUP obligations. For instance, should we require providers to obtain independent verification of their compliance, such as through an independent auditor using generally accepted auditing practices? How often should such reviews be conducted? Should they be randomized? Should reviews generally evaluate all provider KYUP practices or be targeted toward specific practices, such as those where there appear to be the greatest weaknesses by providers at the time? What role, if any, should the Commission play in such compliance reviews? Should we require providers to report the findings of such reviews to the Commission?

36. *Implementation costs and cost recovery.* We seek comment on the costs of the KYUP obligations on voice service providers. As an initial matter, we believe that many legitimate providers already perform many of the baseline KYUP steps we propose above to fulfill their existing obligation to know their upstream providers, and therefore their costs will be minimal. We believe the largest cost would be on providers that have not implemented the most basic KYUP practices to comply with that existing obligation, and we believe that cost is warranted. We seek comment on what share of providers would have to adopt new processes and what share would only need to make minor adjustments. What

---

[74] I3Forum KYC/KYT Code of Conduct at 4 ("Communications providers should educate their employees about the corporate KYC and KYT policy with the goal of ensuring the policy is followed consistently in real life. To further pursue this goal, each communications provider should identify at least one person who will have particular responsibility for upholding the policy. The duties of the KYC compliance leader and their team include: [p]erforming pre-agreement reviews of all prospective customers to determine whether they meet the corporate KYC and KYT policy requirements, keeping documentation of all information considered, decisions reached, and all the individuals involved in the review[;] [p]erforming escalated enhanced due diligence reviews and making KYC decisions for higher-risk clients identified through the standard review process[;] [e]nsuring corporate policy is sufficient to meet changes in legal and regulatory obligations and consulting with internal teams on legal questions that arise as part of KYC processes[;] [s]upporting the development or implementation of the tools, systems, or other resources needed to perform and document KYC and KYT in a timely manner[; and] [w]orking with line management and human resources management to ensure the adequacy of the KYC and KYT training that is given to staff.").

[75] *See KYC FNPRM*, FCC-CIRC2604-02, at 8, para. 24 (noting that the statute of limitations is four years for spoofing or intentional TCPA violations and seeking comment on whether to require providers retain KYC information and supporting records for that period) (citing 47 U.S.C. § 227(b)(4)(E)(ii), (e)(5)(A)(iv)).

costs would providers who only require minor changes to their current procedures incur? We believe that providers that seek to enter into business with a number of upstream providers will also have greater costs but that those costs are warranted as they will ensure that wholesale providers are employing proper measures to deter bad actor providers. Upstream providers that only have a direct relationship with end users will not have to incur these costs. We also believe our proposed baseline KYUP requirements minimize the costs on providers with an obligation to perform KYUP requirements by largely relying on upstream providers to supply the information the provider must obtain and by only requiring providers to conduct basic due diligence. Additionally, we believe that responsible providers already collect most of this information as part of their normal onboarding process with new upstream providers. We seek comment on this assessment and on the specific costs providers, including small providers, may face for each of the requirements we propose above.

37. We also think that the costs associated with being subject to a downstream provider's KYUP obligations will be reasonable for legitimate and responsible upstream providers. Nearly all voice service providers may bear some costs in compiling and providing the requested KYUP information to downstream providers, but we believe many upstream providers will have this information readily available. Upstream providers will also be able to share the same information with all downstream providers with which they do business. In any event, the fact that they will have to provide information will, we believe, spur all voice service providers in the ecosystem to be more responsible actors, ensuring that they have completed necessary registrations and can provide information showing they are a legitimate business. We seek comment on these views.

38. We seek comment on whether we should put guardrails on how voice service providers will recover these costs. Will providers treat this as a cost of doing business and recover such costs from their customers? Will they attempt to charge upstream providers for the costs of performing their KYUP obligations? Should we explicitly permit or prohibit any specific cost recovery approaches?

39. *Safe harbor for accepting calls from upstream providers who obtain SPC Tokens.* Below we propose to require that the Governance Authority strengthen its SPC token access policy, including certain steps to know voice service providers that are modeled off the KYUP requirements above, and increase its enforcement of the policy. In the event we adopt those requirements, we seek comment on whether we should create 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. We believe such a safe harbor could reduce providers' costs of performing KYUP requirements. However, we are concerned it could undermine the ability of providers to perform KYUP monitoring obligations because they would not have obtained certain information about upstream providers to compare against. Should we require the Governance Authority to share information with providers that they can use to support their monitoring activities? Should this safe harbor only apply to small providers?

40. *Best practices.* We seek comment on whether, instead of requiring voice service providers to follow the specific baseline KYUP obligations we propose above, we should establish those proposed requirements as best practices or advise providers to use existing resources as best practices. Should we delegate authority to the Wireline Competition Bureau (Bureau) to establish and maintain best practices, as needed, in coordination with the Consumer and Governmental Affairs Bureau and the Enforcement Bureau? Are there specific existing best practices resources we should advise providers to use? Should we establish a safe harbor from Commission enforcement of the general KYUP requirement for providers that do adopt the best practices? How would such a safe harbor work? Alternatively, should we adopt a rule requiring providers to use a specific best practices resource?

41. *Liability standard for Commission enforcement.* We seek comment on whether we should establish a liability standard the Commission could use to hold voice service providers accountable to complying with their KYUP obligations. We remain concerned that certain providers may seek to circumvent these obligations. Should we establish that the Commission can hold providers accountable if they knew or should have known that an upstream provider is using its network or services

to transmit illegal traffic? Should we establish a different liability standard? If so, what liability standard would best spur providers to take their KYUP obligations seriously without placing an unreasonable threat of enforcement on those providers that make legitimate efforts to fulfill those obligations? Should we establish a liability standard as an alternative to establishing the baseline KYUP obligations we propose? Should we establish a liability standard for providers who abuse their KYUP obligations, such as using them to advance anticompetitive goals? If so, should the standard be whether a decision to refuse or discontinue service was objectively reasonable?

2. Enhancing Oversight of Voice Service Providers by the STIR/SHAKEN Governance Authority

42. The STIR/SHAKEN framework is predicated on trust. The STIR/SHAKEN Governance Authority[76] establishes and enforces 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.[77] The technical requirements establish a secure mechanism to transmit authentication information so that it remains trustworthy.[78] As originally contemplated, this framework would allow for originating providers to develop a reputation based on the calls they sign and for terminating providers to treat calls differently based on that reputation, which might deter originating providers from transmitting illegal calls.[79] However, trust in the STIR/SHAKEN framework can break down when there are bad actor providers in the ecosystem that are not implementing the framework consistently and correctly,[80] including originating providers that fail to authenticate calls or do not apply the proper attestations, downstream providers that accept those calls, and terminating providers that fail to verify authentication information.

43. We do not believe that the Governance Authority's current policies and practices are sufficiently preventing bad actor providers from entering the STIR/SHAKEN ecosystem.[81] Because this can undermine the trust on which STIR/SHAKEN is built, we propose and seek comment on steps we can take to enhance the Governance Authority's role in serving as a gatekeeper to the ecosystem. Specifically, we propose to require that the Governance Authority adopt improved policies for the issuance of SPC tokens and the selection of Certification Authorities, and that the Governance Authority

---

[76] When we refer to the Governance Authority, we include the Policy Administrator and the Certification Authorities even though each entity may perform specific functions, unless otherwise specified.

[77] *See supra* Section II; *see also* STI-GA, SIPNOC 2025 Update on the STI-GA & How to Know Your Customer at 2 (Sept. 16, 2025) (stating that the Governance Authority "[e]nsures security and integrity of STIR/SHAKEN ecosystem"); ACA International Triennial Report Comments at 12-13 (noting that the Governance Authority "is charged with protecting the STIR-SHAKEN framework against potential misuse of 'signing' authority").

[78] *See supra* Section II.

[79] *See* ATIS-1000074 at 6 ("The use of standardized cryptographic digital signatures to validate the originator of a signed identity can provide a verifiable mechanism to identify the authorized originator of a call into the VoIP network with non-repudiation. Further, the use of an assigned attestation indicator and an origination identifier depending on how and where the call is originated in the VoIP network represents the originating signer's ability to vouch for the accuracy of the source of origin of the call. For example, if the originating service provider has an authenticated direct relationship with the originator of the call, this attestation is categorized differently than for calls that are originated from different networks or gateways that the service provider may have received from an unauthenticated network, or that are unsigned. Verifiers of signatures can use these attestations as information to employ traceback mechanisms, as well as to provide information to feed into call analytics enabled on behalf of their customer.").

[80] Second Triennial STIR/SHAKEN Report at 17-18.

[81] ATIS STIR/SHAKEN NOI Comments at 8 (Aug. 14, 2017) (explaining that, as contemplated, the Governance Authority would amend policies and procedures "based on actual deployment experience and the response of malicious entities" and that the modifications would be timely "to address potential gaps before they become major issues").

apply those policies to existing SPC token holders and Certification Authorities within six (6) months after any rules we adopt go into effect. Additionally, we propose that the Governance Authority adopt improved policies for the revocation of SPC tokens and removal of Certification Authorities, including taking greater action to enforce those policies. We believe these enhancements will not only help restore trust in the STIR/SHAKEN framework, but will help keep bad actor providers off the voice network, particularly if we adopt our proposal to prohibit voice service providers from accepting unauthenticated SIP calls.[82]

44. In advancing these proposals, we acknowledge that we would be applying a more directed oversight approach with the Governance Authority, but we believe Commission intervention now is necessary to restore trust in the STIR/SHAKEN framework, and that we have authority to do so. Although the Commission found that intervention in the independent STIR/SHAKEN governance structure was not appropriate when it first mandated that voice service providers implement STIR/SHAKEN, given that the Commission "[did] not know the nature and scope of the problems that may arise,"[83] it has consistently contemplated beginning before the Governance Authority was established that it could play a greater oversight role if necessary.[84] With greater experience, we now believe that we have identified problems that the Commission can address by requiring updated policies and requirements. We seek comment on these views.

45. *Policies for the issuance of SPC tokens and selection of Certification Authorities.* We propose to direct the Governance Authority to add to its SPC Token Access Policy baseline vetting requirements prior to the issuance of SPC tokens that are modeled off the KYUP requirements we propose above, and that these requirements should also be applied to existing SPC token holders. We do not believe that the Governance Authority's current SPC Token Access Policy is sufficient to prevent bad actor providers from obtaining a token, which in turn authorizes them to access the certificates needed to authenticate calls, and then using those tokens to transmit calls that are not in compliance with the STIR/SHAKEN authentication framework and the Commission's STIR/SHAKEN rules.[85] Although the existing policy subjects voice service providers seeking SPC tokens to some level of scrutiny, it does not

[82] *See infra* Section III.C.4.

[83] *First Caller ID Authentication Order*, 35 FCC Rcd at 3268, para. 56. The Commission maintained this position and similarly declined to intervene in or impose new regulations on the Governance Authority's policies in the *Second Caller ID Authentication Order*, 36 FCC Rcd at 1883, para. 52 n.181.

[84] *Call Authentication Trust Anchor*, WC Docket No. 17-97, Notice of Inquiry, 32 FCC Rcd 5988, 5994-96, paras. 18-27 (2017) (asking several questions about the STIR/SHAKEN governance structure including the Commission's role in selecting and overseeing the structure); *Advanced Methods to Target and Eliminate Unlawful Robocalls*; *Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, 34 FCC Rcd 4876, 4901, para. 79 (2019) (seeking comment on what role the Commission should have in STIR/SHAKEN governance, including whether "there any aspects of the governance authority that the Commission should handle itself" or whether "the Commission's role [should] be limited to a formal oversight one with regard to the governance regime"); *First Caller ID Authentication Order*, 35 FCC Rcd at 3268, para. 56 (stating that "*at this time*, it 'is not necessary for the Commission to have a role in STIR/SHAKEN governance'" (emphasis added)); *id.* ("We do not think that our intervention in the governance structure is appropriate *at this stage* . . . ." (emphasis added)); *Second Caller ID Authentication Order*, 36 FCC Rcd at 1883, para. 50 n.181 (maintaining its position not to intervene in or impose new regulations on the STIR/SHAKEN governance structure when declining a request to do so by a commenter, but not disclaiming the Commission's authority to do so).

[85] Under the existing SPC Token Access Policy, providers must: (1) have a current form 499-A on file with the Commission, (2) have been assigned an Operating Company Number (OCN), and (3) have certified with the Commission that they have implemented STIR/SHAKEN or comply with the Commission's robocall mitigation program requirements and are listed in the RMD. STI-Governance Authority, Policy Decision Binder, Version 9.1, Policy Decision 001: SPC Token Access Policy Version 1.2, at 6 (Jan. 13, 2026) (Governance Authority Policies), https://cdn.atis.org/sti-ga.atis.org/2026/01/14175322/260113-STIGA-Board-Policy-Decision-Binder-v9-1-1.pdf.. The policy also applies these requirements to Resp Orgs, to which we believe our proposals should also apply. *Id.*

include an evaluation of whether the provider is a legitimate entity or provide the gatekeeping necessary to keep potential bad actor providers out of the STIR/SHAKEN ecosystem. Accordingly, we propose to require the Governance Authority to modify its policy to include all of the KYUP information collection, compliance review, and verification requirements we propose above. We also propose to require that the Governance Authority adopt a policy to review this information and deny an SPC token when there is a reasonable basis for believing the SPC token holder is unlikely to comply with the STIR/SHAKEN authentication framework, the Commission's STIR/SHAKEN rules, and/or the Governance Authority's policies. We seek comment on our proposals and associated analysis. Are there any such KYUP requirements we should not require the Governance Authority to follow? How do these relate to the information collection requirements of, and due diligence performed by, the National Exchange Carrier Association (NECA) when providers request OCNs?[86]

46. We likewise propose to require the Governance Authority to largely follow the KYUP requirements to vet Certification Authorities prior to their selection, and that these requirements should be applied to existing Certification Authorities. The Governance Authority has not published a written policy governing the selection of Certification Authorities. Rather, the Governance Authority has established a policy for governing the issuance of certificates that is consistent with the STIR/SHAKEN standards, which Certification Authorities must follow in order to be considered a "trusted" Certification Authority.[87] We are concerned that some Certification Authorities may not be following the certificate issuance policy and may be nefarious actors. While a robust Certification Authority removal process could address such concerns, we believe the Governance Authority should take steps to identify bad actors before they are selected as Certification Authorities. Accordingly, we propose to require the Governance Authority to follow all of the information collection and information verification requirements we propose above. We also propose to require that the Governance Authority adopt a policy to review this information and deny Certification Authority when there is a reasonable basis for believing the Certification Authority is unlikely to comply with the STIR/SHAKEN authentication framework, the Commission's STIR/SHAKEN rules, and/or the Governance Authority's policies. We seek comment on our proposals and associated analysis, including whether we should require greater or lesser due diligence obligations. Should we also require the Governance Authority to adjust the certificate issuance policy, such as by establishing a maximum expiration timeline for certificates?

47. We also seek comment on whether we should require the Governance Authority to establish a conflict of interest policy governing Certification Authorities' relationships with voice service providers, including when they are also acting as voice service providers, and what that policy should entail. Although the Governance Authority has established a policy concerning conflicts as to a Certification Authority also serving as the Policy Administrator,[88] it has not established a conflict-of-interest policy as to a Certification Authority also acting as a provider or having a close relationship with providers. We are concerned about such relationships because a Certification Authority may have incentive to issue certificates to providers to which they are related without following the certificate issuance policy. We seek comment on this assessment.

48. *Policies for the revocation of SPC tokens and removal of Certification Authorities.* We propose to require that the Governance Authority play an active role in obtaining information about providers misusing their SPC tokens and take action on any information it receives or obtains. Under the Governance Authority's existing SPC Token revocation policy, providers must sign an agreement that contains the terms for which tokens may be used, such as in compliance with the STIR/SHAKEN standards governing proper attestations.[89] The policy further states that the Governance Authority may

[86] *See* NECA, *Company Code Request Instructions*, https://www.neca.org/business-solutions/company-codes/company-code-request-instructions (last visited Apr. 27, 2026).

[87] *See* Governance Authority Policies at 8-70.

[88] *See id.* at 96-97.

[89] *See id.* at 72-73.

revoke SPC tokens upon indication that a provider is in breach of the agreement, and lays out other specified reasons for revocation.[90] Additionally, the policy imposes a standardized process stakeholders must use to report potential SPC token misuse.[91] Despite well-known reports that providers are applying improper attestations to calls or otherwise failing to follow the STIR/SHAKEN standards,[92] the Governance Authority has reported to Commission staff that it has only revoked SPC tokens for providers that have failed to pay required fees or failed to supply annual FCC Form 499 revenue data, which the Governance Authority uses to calculate fees.[93] We believe the Governance Authority may be hindered in enforcing the SPC token policy by relying on an overly formal reporting process to obtain information. To address this, we propose to require that the Governance Authority establish formal information sharing arrangements with the Industry Traceback Group and call analytics providers to receive information about specific providers' practices. We also propose to require the Governance Authority to review and evaluate information it receives from any sources, even in the absence of formal reports. Should we require the Governance Authority to seek additional information about providers, modeled off of the KYUP monitoring requirements we propose to establish above? Should we require it to relax its reporting policy so that stakeholders can submit information informally or anonymously? We seek comment on our proposals and any aspects of our analysis.

49. We propose to require that the Governance Authority also play a more active role in seeking, and taking action on, information it receives about Certification Authorities failing to follow its policies. As noted, the Governance Authority has established a policy governing the issuance of certificates by Certification Authorities.[94] It has also established a policy for the suspension or removal of Certification Authorities that violate the policy, violate their agreement with the Governance Authority, or have been involved in a cybersecurity incident.[95] Anecdotally, Commission staff has learned that certain Certification Authorities issue a disproportionate number of certificates that are being used by voice service providers applying improper attestations to their calls. We believe this is indicative of Certification Authorities not following the Governance Authority's certificate issuance policy. To our knowledge, the Governance Authority has not suspended or removed any Certification Authorities.[96] We propose to require that the Governance Authority establish a process to accept information about Certification Authority practices from stakeholders, including a process to regularly obtain information from call analytics providers. We further propose to require that the Governance Authority initiate investigations into Certification Authorities with suspect practices, such as a high volume of illegal calls associated with their certificates, and remove Certification Authorities who are found to be violating the

---

[90] *See id.* at 73; *see also* STI-GA, SIPNOC 2025 Update on the STI-GA & How to Know Your Customer at 7 (Sept. 16, 2025) (describing Governance Authority enforcement considerations to ensure authorized voice service providers and Certification Authorities comply with Governance Authority policies and STIR/SHAKEN attestation and authentication standards).

[91] The stakeholders identified by the policy include the Policy Administrator, Certification Authorities, voice service providers, members of the Governance Authority board, ATIS staff, regulatory authorities (e.g., the FCC and FTC), consumers, and third parties. *See* Governance Authority Policies at 74-75.

[92] *See infra* Section III.B.

[93] STI-Governance Authority, 2024 STI-GA SHAKEN Report at 4 (2024), https://cdn.atis.org/sti-ga.atis.org/2025/02/19165205/2024-STIGA-Public-Report-Final.pdf; *see also* STI-GA, SIPNOC 2025 Update on the STI-GA & How to Know Your Customer at 7 (Sept. 16, 2025) (stating that the Governance Authority revokes SPC tokens "in the event of nonpayment or when an [provider] fails to provide data necessary for the [Governance Authority] to determine a participant's correct fee"); *see also* ZipDX Triennial Report Comments at 3 (noting how the assumption that problematic signers would have their SPC tokens revoked has not borne out in practice).

[94] *See* Governance Authority Policies at 8-70.

[95] *See id.* at 90-94.

[96] Commission staff has observed changes in the number of Certification Authorities, but believes those have been due to voluntary decisions by Certification Authorities.

certificate policy or their agreement with the Governance Authority. We seek comment on whether we should require the Governance Authority to obtain other information about Certification Authority practices that would inform their oversight. We also seek comment whether the Governance Authority has established adequate steps providers must take when they were issued certificates from a Certification Authority that was subsequently removed.

50. We seek comment on whether we should require that the Governance Authority review and act on any information it receives or obtains about voice service providers or Certification Authorities within a specific time. We note that bad actor providers can transmit a significant number of non-compliant calls in a short period of time. Is 10 business days a sufficient time period in which the Governance Authority can reasonably review evidence of wrongdoing and take action? Should it be longer or shorter? Should we require the Governance Authority to adopt a policy to immediately suspend an SPC token or Certification Authority when presented with evidence of egregious activity, after which it can conduct a more thorough review and final determination?

51. *Implementation barriers.* We seek comment on any barriers to the Governance Authority following any of the requirements we proposed above. Are there steps the Commission or the Governance Authority can take to facilitate information sharing? Are there specific reasons the Governance Authority may be deterred from obtaining information or enforcing the policies, such as resource or liability concerns? Can any costs associated with obtaining any such information be incorporated into other Governance Authority operational expenses that are paid for by fees from providers obtaining SPC tokens? Is there a safe harbor we can grant to the Governance Authority for denials and revocations that would support it taking action, and if so, how would the safe harbor be applied? Should we permit the Governance Authority to use third parties to perform some or all of the required vetting?

52. *Appeals.* We propose to allow parties to appeal Governance Authority decisions to the Commission. The Commission has already established a process for voice service providers to appeal token revocation decisions to the Commission.[97] Should we establish a similar process for entities removed as Certification Authorities, as well as for when providers are denied SPC tokens and entities denied as Certification Authorities in the first instance? How, if at all, should the appeals process be different? Should aggrieved entities be required to appeal to the Governance Authority before it would be allowed to file such appeals with the Commission? Should we also allow stakeholders to appeal decisions by the Governance Authority declining to revoke an SPC token, remove a Certification Authority, or initiate an investigation? How might this appeal process work or might there be a better process for entities to alert the Commission to the Governance Authority's decisions they perceive to be erroneous? Should we require the Governance Authority to respond to stakeholders that submit complaints if it declines to take any of those actions?

53. *Reporting.* We propose to require that the Governance Authority report to the Commission on a quarterly basis information about its enforcement activity, including complaints it has received, investigations it has initiated or concluded, and decisions concerning SPC token revocations and Certification Authority removals, including any reports documenting the Governance Authority's final determinations. We believe that such reporting will aid the Commission in its efforts to identify and take action against bad actor providers. We seek comment on this proposal.

B. Raising STIR/SHAKEN Attestation Standards

54. An attestation is a voice service provider's assertion about the knowledge it has about its customer and the customer's right to use a telephone number.[98] A provider may assert A-level (or "full")

[97] *See* 47 CFR § 64.6308; *Call Authentication Trust Anchor*; *Appeals of the STIR/SHAKEN Governance Authority Token Revocation Decisions*, WC Docket Nos. 17-97 and 21-291, Third Report and Order, 36 FCC Rcd 12878, 12884-91, paras. 12-28 (2021). To date, no providers have appealed token revocations to the Commission.

[98] ATIS-1000074 at 12.

attestation when it (1) is responsible for the origination of the call onto the IP network, (2) has a direct authenticated relationship with its customer and can identify the customer, and (3) has established a verified association between its customer and the telephone number used for the call.[99] It may assert B-level (or "partial") attestation when it can satisfy elements (1) and (2), but not (3).[100] It must assert C-level (or "gateway") attestation when the provider has no relationship with the originator of a call, such as when a provider is acting as an international gateway.[101] By asserting full (A-level) attestation, the provider is claiming that is has knowledge that the number has not been spoofed. While calls receiving partial (B-level) or gateway (C-level) attestations are not necessarily spoofed, they indicate that the voice service provider lacks sufficient knowledge to conclusively determine that fact.

55. Many calls are being authenticated by originating providers with improper attestations, according to a 2024 report from the STIR/SHAKEN Governance Authority.[102] The *Call Branding FNPRM* record is replete with comments making the same case.[103] The Commission has acknowledged the problem too,[104] and has taken some steps to address it. The *Lingo Order* represents the most high-profile example, in which the Commission found that Lingo Telecom applied A-level attestations to 3,978 spoofed robocalls carrying a deepfake generative AI voice message purporting to be from then-President Joe Biden.[105] Recent data show that "93.4% of robocall traffic from the most prolific robocall signers now carry A-level attestations" and "48 percent of illegal calls are A-attested."[106] In an analysis done by the American Bankers Association "of 12,900 calls that illegally spoofed telephone numbers belonging to 47 large banks, retailers, and healthcare providers, more than half of the calls received an A-level or B-level attestation."[107] Improper signing practices are not limited to bad actor providers. Transaction Network Services reports that, based on internal data covering the first half of 2025, "certain top tier carriers had marked around 8% of their invalid number calls with A-level attestation, and non-top tier carriers had marked 57% of their invalid number calls with A-level attestation."[108]

56. These findings call for enhancements to the Commission's STIR/SHAKEN attestation policies. Improper attestations undermine the trust in and integrity of the STIR/SHAKEN framework,

---

[99] *Id.*

[100] *Id.*

[101] *Id.* at 13. The ATIS standards also permit a C-level attestation when a provider is unable to satisfy the criteria of A- or B-level attestations. *Id.*

[102] *See* STI-Governance Authority, 2024 STI-GA SHAKEN Report at 5 (2024), https://cdn.atis.org/sti-ga.atis.org/2025/02/19165205/2024-STIGA-Public-Report-Final.pdf ("The STI-GA Board always expected that, with such a large number of providers in the fold, that some providers would accidentally, or perhaps intentionally, use their STI certificates to sign calls incorrectly. It was for this reason that the policies that deal with [service provider] revocation and reinstatement, as well as the guidance on improper attestation, were created.").

[103] *See, e.g.*, Letter from Keith Buell, General Counsel and Head of Global Public Policy, and Rebekah Johnson, Founder and Chief Executive Officer, Numeracle, to Marlene H. Dortch, Secretary, FCC, CG Docket 17-59, WC Docket 17-97, CG Docket 02-278, CG Docket 25-307, at 2 (filed Oct. 21, 2025) (Numeracle Call Branding *Ex Parte*); NCTA Call Branding Comments at 3; First Orion Call Branding Comments at 7; ZipDX Call Branding Comments at 3; USTelecom Call Branding Comments at 3; T-Mobile Call Branding Comments at 9; TransNexus Call Branding Comments at 4; American Bankers Association et al. Call Branding Comments at 20; NCLC Call Branding Comments at 7.

[104] Second Triennial STIR/SHAKEN Report at 12.

[105] *Lingo Order*, 39 FCC Rcd 9304.

[106] *See* Numeracle Oct. 21 *Ex Parte* Letter at 2.

[107] American Bankers Association et al. Call Branding Comments at 21.

[108] Transaction Network Services Call Branding Comments at 7-8.

and its value in supporting efforts to combat illegal robocalls.[109] When attestations are improper, terminating providers do not have trustworthy information concerning whether the number used for the call was illegally spoofed.[110] Because voice service providers also use attestations to inform call analytics engines,[111] improper attestations can undermine their effectiveness, contributing to inaccurate blocking and labeling determinations.[112] And because the Commission has proposed in the *Call Branding FNPRM* to prohibit terminating providers from delivering indications of A-level attestations to consumers' devices unless they also deliver verified caller identity information,[113] improper attestations may subvert the validity of caller identity information rather than serve to enhance it.[114] Ultimately, improper attestations may lend false legitimacy to bad actors and may undermine the credibility of good actors.[115]

57. Given these stated harms, stakeholders have called on the Commission to take a stronger role in overseeing and enforcing voice service providers' compliance with the ATIS attestation standards.[116] We believe one of the primary causes for improper attestations is disagreement about what mechanisms are permitted to close the attestation "knowledge gap." As we understand it, this knowledge

---

[109] *See* Second Triennial STIR/SHAKEN Report at 12 & n.67; *see also, e.g.*, *Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12911, para. 23 n.105; CTIA Triennial Report Comments at 2 ("While STIR/SHAKEN continues to play an important part in the industry's multilayered approach to fighting robocalls, not all stakeholders are applying STIR/SHAKEN consistently, which threatens to erode the framework's value and trust.").

[110] *See, e.g.*, VON Coalition Call Branding Comments at 3 (explaining that STIR/SHAKEN is designed to "allow service providers to pass information about whether the caller identification is valid" so that terminating providers know whether a caller has the right to use the telephone number); Somos Call Branding Comments at 16 ("Preserving meaningful attestation levels. As outlined in ATIS-1000092, attestation levels are intended to communicate a level of confidence in the caller's identity and right to use the number.").

[111] Second Triennial STIR/SHAKEN Report at 17 & n.103.

[112] *Id.* at 17-18 & n.105.

[113] *Call Branding FNPRM* at 9, para. 23. The *Call Branding FNPRM* proposes to define "caller identity information" as having the same meaning given the term "caller identification information" in section 64.1600(c) of our rules, but excluding the originating telephone number or portion thereof and billing number information. *See id.* at 10-11, paras. 27-29; 47 § CFR 64.1600(c).

[114] *See, e.g.*, CTIA Call Branding Comments at 14; TNS Call Branding Comments at 7-8; SOMOS Call Branding Comments at 6.

[115] *See, e.g.*, Numeracle Oct. 21 *Ex Parte* Letter at 2 ("This means the current STIR/SHAKEN model is being used to lend false legitimacy to bad actors, proving that implicit trust in carrier self-attestation has failed."); USTelecom Call Branding Reply at 3-4; T-Mobile Triennial Report Comments at 6; Convo Call Branding Comments at 7-8 (expressing concern that Convo users' video relay service (VRS) calls may receive C-level attestations, which could "unjustly cause its users' calls to be blocked or marked as SPAM, thereby effectively denying Deaf callers access to the PSTN").

[116] *See, e.g.*, Transaction Network Services Call Branding Comments at 9 ("[T]he Commission must first resolve this A-level attestation issue and continue to improve its STIR/SHAKEN regime before attempting to rely on any attestation level as a trigger to mandate delivery of caller identity information."); Verizon Call Branding Comments at 6 ("Inconsistent verification practices and a lack of accountability for call signing abuse will degrade existing robocall mitigation tools without constant vigilance. Verizon therefore urges the Commission to direct its anti-robocall firepower towards providers who are abusing the building blocks currently being deployed by legitimate providers to create cutting-edge call labeling solutions."); Unified Office, Inc. Call Branding Comments at 8 ("Any new verification requirements should build upon, not replace, the STIR/SHAKEN A-level attestation system that providers have already implemented. We acknowledge concerns about bad actors obtaining A-level attestations, but the solution is not to abandon the framework—it is to strengthen oversight and enforcement."); Québec Inc. DBA VoIP.ms Call Branding Comments at 8 ("The Commission should . . . [p]rovide clear instruction to voice service providers on assigning attestation levels to ensure that higher attestation levels provide real validation of traffic quality."); CTIA Call Branding Reply at 17 ("CTIA therefore recommends that the Commission continue to enforce appropriate call signing practices throughout the calling ecosystem, as such practices are the bedrock of the STIR/SHAKEN framework.").

gap generally occurs in the following general scenarios:

> *Scenario 1* – When the originating provider that is authenticating the call is a separate entity from the telephone number service provider (TNSP) that provisioned the telephone numbers to the customer initiating the call, such as when a TNSP assigns direct inward dialing (DID) numbers to a customer that initiates the call with another voice service provider.[117]
>
> *Scenario 2* – When the originating provider does not have a direct relationship with the end user because the end user obtained voice service from an intermediary provider, such as a reseller that may be several steps removed from the originating provider if the service is resold multiple times.[118]

We do not believe these scenarios are mutually exclusive, and therefore both could exist with respect to a single call. We seek comment on this assessment. Are there other scenarios that cause a knowledge gap?[119] We believe that bad actors may take advantage of the "knowledge gap" to obscure their identity to the originating provider and use that obscurity to generate spoofed or unlawful calls. As we raised in the *Call Branding FNPRM*, the knowledge gap can also undermine the ability for providers to verify caller identity verification information.[120]

58. We propose specific requirements and guardrails to govern STIR/SHAKEN attestation-level decisions to ensure that voice service providers base such decisions on sufficient knowledge about their customer and the customer's right to use a number, and not on factors that may be unrelated to caller ID information.[121] Although we believe the main driver of improper attestations is the presence of bad actor providers in the ecosystem, which we believe will be addressed by the KYUP and Governance Authority proposals above, we also want to ensure that all providers in the ecosystem are applying

---

[117] *See* ATIS-1000089 at 7 & fig.7-1 ("The TNSP and OSP are different Service Providers. Normally under SHAKEN definitions this call would receive an Attestation 'B' since OSP B is not the TNSP, and therefore cannot directly establish a relationship between the customer and the caller ID."); *see also Lingo Order*, 39 FCC Rcd at 9309, para. 9 (finding that Lingo Telecom mis-assigned A-level attestations to a customer based simply on the customer's certification that it had a verified association with the telephone numbers used for the calls). ATIS-1000089 is a Technical Report that discusses potential mechanisms providers may use to assign A-level attestations to calls when the voice service provider does not have direct knowledge about its customer's association with the number used. *See* ATIS-1000089 at i. It is not one of the ATIS standards that voice service providers are required to follow to implement STIR/SHAKEN.

[118] *See* ATIS-1000088 at 18 ("In most reseller use cases, an originating [service provider] does not know the identity of the ultimate end users and only identifies and authenticates the reseller customer. Identification of end users relies on the communications reseller to make any such determination, and further layers of indirection might obscure the ultimate source."); *Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12908, para. 19 (encouraging voice service resellers to "provide . . . wholesalers with enough information to enable them to determine the appropriate attestation level of the calls initiated by the resellers' end users"). This scenario is a direct result of the STIR/SHAKEN implementation exemption for non-facilities-based providers that is inherent in the STIR/SHAKEN framework and which we propose to codify below. *See infra* Section III.C.1.f. We also propose to close this knowledge gap by requiring all voice service providers serving end users directly to make attestation-level decisions regarding those end users' calls. *See infra* Section III.C.3.

[119] As a technical matter, we believe there is also a knowledge gap when a gateway provider is authenticating a call that it received from a foreign voice service provider and when an intermediate provider is authenticating an unauthenticated call it receives, but these circumstances are outside the scope of the problem we seek to address here.

[120] *See Call Branding FNPRM* at 19-20, paras. 65-67.

[121] CTIA Call Branding Comments at 7 ("In the STIR/SHAKEN context, for example, CTIA and others have highlighted poor call vetting practices resulting in inappropriate 'A' attestations.").

attestations consistently and correctly.[122] We also seek to provide a clearer foundation for enforcement when providers misapply attestations. Accordingly, we propose to: (1) codify the attestation levels established in the ATIS standards and the criteria that apply to them, (2) set out requirements to satisfy the attestation-level criteria including closing the attestation knowledge gap in Scenario 1,[123] and (3) codify the definition for and prohibitions on improper attestations that are implicit in providers' obligation to implement the STIR/SHAKEN standards. We believe the proposals will serve to enhance the STIR/SHAKEN standards and better achieve the intended outcomes of the TRACED Act without superseding the requirement that providers implement the STIR/SHAKEN standards, as required by the TRACED Act.[124] We seek comment on this analysis, including the extent to which our proposals will address all causes of improper attestations and our authority to take these actions. We also seek comment on whether we should require providers to implement the most current version of the STIR/SHAKEN standards, rather than the version that was in effect at the time they were first required to implement STIR/SHAKEN.[125]

1. Codifying the Attestation Levels

59. We propose to codify the three attestation levels—A, B, and C—and the criteria that apply to each level. We believe that this step goes hand-in-hand with establishing steps voice service providers must take to satisfy the attestation-level criteria, as we propose to do below. We also think it will clarify any perceived ambiguity about the attestation levels by providers and provide a stronger foundation for oversight and enforcement of attestation-level decisions. We seek comment on this proposal. In particular, are there meaningful concerns with codifying the attestation levels when the Commission has acknowledged that ATIS standards may change over time?[126] Are ATIS and/or the Governance Authority continuing to study the problem of improper attestations and planning to issue more particularized guidance? Is ATIS in the process of changing the attestation levels or their criteria, particularly in light of the issues with improper attestations? We note ATIS's view in the context of non-IP caller ID authentication standards that "[s]tandards are not a proxy for regulations" and that "standards should not be used as the primary basis for regulation without significant independent legal and factual analysis to evaluate whether the standard is viable or appropriate for a regulatory mandate to implement solution(s) based on that standard."[127] Given the widespread support for and investment in STIR/SHAKEN, we believe that the attestation portion of the standard is viable and appropriate for codification. We seek comment on these views and any other legal or factual analysis that we should consider in our assessment.

---

[122] TransUnion Call Branding Comments at 8 ("TransUnion has observed that originating providers are inconsistent in how they sign and attest calls that originate on their network.").

[123] In a later section, we also propose to close the knowledge gap in Scenario 2. *See infra* Section III.C.3.

[124] 47 U.S.C. § 227b(b)(1).

[125] In the *First Caller ID Authentication Report Order* and in subsequent orders, the Commission required providers to comply with the versions of those standards that were in effect at the time of their respective compliance deadlines, including any errata as of those dates or earlier. *See First Caller ID Authentication Order*, 35 FCC Rcd at 3258-59, para. 36; *Gateway Provider Order*, 37 FCC Rcd at 6887-88, para. 53; *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2585-86, para. 21. The Commission delegated to the Bureau authority: (1) to determine whether to seek comment on requiring compliance with revised versions of the three ATIS standards associated with the STIR/SHAKEN authentication framework, and all documents referenced therein; (2) to require providers subject to a STIR/SHAKEN authentication requirement to comply with those revised standards; and (3) to set appropriate compliance deadlines regarding such revised standards. *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2587, para. 25. In doing so, the Commission noted that providers will only be required to implement new standards if the benefits to the STIR/SHAKEN ecosystem outweigh any compliance burdens. *Id.* Notwithstanding our delegation of authority to the Bureau, we seek to address the question here.

[126] *See Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2586-87, paras. 24-25.

[127] ATIS Non-IP Authentication *Ex Parte* Letter, Attach. at 4 (Oct. 1, 2025).

2. Requirements to Satisfy the Attestation Level Criteria

60. We propose and seek comment on specifying how voice service providers may satisfy the criteria used for applying the STIR/SHAKEN attestation levels to dispel any perceived ambiguity about how the criteria apply and ensure providers are making proper attestation decisions. We believe doing so is necessary, given the evidence of improper attestations by providers of all types and stakeholders' requests that the Commission provide greater oversight of attestation practices. We seek comment on this proposal. Do commenters agree it is necessary to specify how attestation-level criteria are satisfied to address improper attestations? Are providers using the absence of such specificity to skirt their attestation responsibilities? Are there other reasons, beyond differences in interpretation or implementation of the ATIS standards, as to why many providers are improperly attesting to calls? Rather than adopting requirements, should we establish best practices, and should we delegate authority to establish those best practices to the Bureau? If we do establish requirements for satisfying attestation-level decisions, would this instill enough trust in attestations that we should prohibit blocking or spam labeling of calls with A-level attestations? What about B-level attestations? What incentives would that provide to originating providers?

61. *Responsibility for call origination.* We propose that for a voice service provider to satisfy the requirement that it is responsible for the origination of the call onto the IP network,[128] it must qualify for the definition of "origination" that we propose to adopt below.[129] We seek comment on this proposal. If we adopt our proposal to define "origination" as the technological act of placing a customer's outgoing call onto the network using the provider's own facilities,[130] does this offer enough clarity about which provider is responsible for originating a call onto the IP network? If not, how can we provide greater clarity? We believe that intermediate providers, including gateway providers, cannot be responsible for the origination of a call under our definition. Is this understanding correct?

62. *Direct authenticated relationship with the customer and ability to identify the customer.* We propose that for an originating provider to satisfy the requirement that it have a direct, authenticated relationship with the customer associated with the call and be able to identify the customer,[131] it must satisfy any KYC or KYUP requirements established by the Commission. We seek comment on this proposal. The KYC requirement would apply when the originating provider is authenticating a call for an end user customer. Section 64.1200(n)(4) of the Commission's rules establishes the current KYC requirement,[132] and in the *KYC FNPRM*, the Commission seeks comment on specific requirements originating providers must follow to fulfill this requirement.[133] The KYUP requirement would apply when the originating provider is authenticating a call from a customer that is a direct upstream provider, such as when the originating provider's customer is a reseller. As discussed above, section 64.1200(n)(5)

[128] ATIS-1000074 at 12.

[129] *See infra* Section III.C.1.c.

[130] *See Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12907, para. 18 ("ATIS-1000074 only permits A- and B-level attestations to be made by providers that originate calls onto the IP-based service provider network. Although not defined in ATIS-1000074, that standard uses the term originating service provider, or OSP, consistent with related standards documents, such as ATIS-1000089, which defines originating service provider as: '[t]he service provider that handles the outgoing calls from a customer *at the point at which they are entering the public network*. The OSP performs the SHAKEN Authentication function.' Thus, when an originating service provider authenticates a call based on what it knows about its customer and its customer's right to use a telephone number, it is performing its own STIR/SHAKEN implementation obligation, not that of its upstream customer in a third-party capacity.").

[131] ATIS-1000074 at 12.

[132] 47 CFR § 64.1200(n)(4) (stating that a voice service provider must "[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").

[133] *KYC FNPRM*, FCC-CIRC2604-02, at 4-8, paras. 9-24.

of the Commission's rules establishes a KYUP requirement, and all voice service providers must describe their KYUP practices in the robocall mitigation plans they file in the RMD.[134] We also propose above to establish specific requirements providers must follow to fulfill the KYUP requirement.[135] We believe that tying KYC and KYUP requirements to attestation-level decisions will help ensure originating providers actually know their customer before assigning A- or B-level attestations to calls, making such attestations more accurate and thereby better deterring impermissible spoofing.[136] Do commenters agree? Are there other benefits? Are there any drawbacks? Should we only require originating providers to rely on specific KYC or KYUP practices to fulfill this criterion? If so, which practices? We also seek comment on how this proposal relates to the *Call Branding FNPRM*, which seeks comment on requiring originating providers to verify customer identity information as a condition of A-level attestation.[137]

63. *Establishing a verified association between the customer and the telephone number used for the call.* We propose to specify permissible and impermissible mechanisms an originating provider may use to establish a verified association between its customer and the telephone number used for a call. We do not believe all originating providers are meaningfully verifying a customer's association with a telephone number, leading to improper attestations. This stems, we believe, from ATIS-1000074, which states that "[u]ltimately it is up to service provider policy to decide what constitutes [a] 'legitimate right to assert a [telephone number]' but the service provider's reputation may be directly dependent on how rigorous they have been in making this assertion."[138] We believe that some originating providers are interpreting this direction too broadly.[139]

64. To resolve these practices, we propose two mechanisms that providers may use to establish a customer's association with a number. First, we propose to find that an originating provider may establish a verified association between its customer and the telephone number used when the originating provider is the TNSP (i.e., it assigned the telephone number to the customer either as an individual number or as part of a range of numbers).[140] Second, we propose to partially close the knowledge gap in Scenario 1 by finding that delegate certificates are a viable method for originating

[134] *See supra* Section II.

[135] *See supra* Section III.A.1.

[136] Twilio Call Branding Comments at 4-5 ("The FCC should require all originating providers to take reasonable steps to verify the legitimacy of a caller before assigning an A-level attestation. Providers that fail to take these steps should be held accountable. When an A-level attestation is assigned without proper vetting, recipients are more likely to receive caller IDs that are spoofed, leading to a further loss of trust from the consumer. This gap occurs because some originators apply A-level attestation without verifying the identity of the originating entity placing the call, which allows bad actors to enter the network. Clear accountability and rigorous vetting processes are essential to protect consumers and maintain confidence in caller ID authentication." (footnotes omitted)); American Bankers Association et al. Call Branding Comments at 22-23 ("Today, bad actors are able to place illegally spoofed calls with A-level attestation in large part because originating providers do not regularly engage in meaningful diligence of the caller before granting A-level attestation to its calls."); Somos Call Branding Comments at 13 ("OSPs should be required to verify caller identity information prior to transmission when asserting high trust levels (e.g., 'A' attestation).").

[137] *Call Branding FNPRM* at 19-20, paras. 65-68.

[138] ATIS-1000074 at 12.

[139] American Bankers Association et al. Call Branding Comments at 24 (stating that its "research found that originating providers currently do not verify that the caller has the legal right to use the number displayed in the recipient's caller ID display before providing an A-level attestation for the call").

[140] *See* Somos Call Branding Comments at 15 ("[I]f the [originating service provider (OSP)] has direct control over the number assignment and can verify the identity of the calling party, including their right to use the telephone number and the authenticity of the calling name, then the OSP should assert "A" attestation and sign the call accordingly.").

providers to establish a verified association between a customer that is an initiating provider[141] and the number being used to initiate the call, and we seek comment on this view.[142] Delegate certificates, which are described in ATIS-1000092 (a separate ATIS standard than those required for STIR/SHAKEN implementation),[143] allow an entity to obtain a certificate from the TNSP that demonstrates the entity's authority to use the number and present that certificate to the originating provider.[144] We believe this process would enable initiating providers to satisfy this criterion whenever its end user customer uses a telephone number that the initiating provider assigned to the end user. To what extent are providers already using delegate certificates for this purpose? What measures, if any, are needed to ensure that delegate certificates are accepted as a valid form of showing an initiating provider has a relationship with a number? Must we require that originating providers accept delegate certificates from initiating providers as evidence they have a verified association with a number, and if so, should we place any guardrails on this requirement?[145] What are the benefits and drawbacks of the delegate certificate approach? Because the delegate certificate would be associated with the TNSP, would it enable the TNSP to be held accountable for the illegal calls transmitted by entities to which they assigned numbers?[146] Should we further find that delegate certificates are a viable method for originating providers to establish a verified association between an end user customer, such as a non-voice service provider enterprise, and the number being used to initiate the call?[147] If so, does the Governance Authority need to modify its SPC token policy so that such end users can obtain SPC tokens and certificates? What are the risks and benefits of allowing non-provider entities to have a role in the STIR/SHAKEN ecosystem? We seek comment on any additional provider and customer arrangements for which delegate certificates could be used to establish a customer's association with a number.

65. Conversely, we believe there are two mechanisms a voice service provider cannot use to establish a verified association between its customer and the telephone number used. First, we do not believe this association can be established by a business agreement or certification that includes only a general statement that the customer will only use numbers with which it has a verified association. This is essentially the mechanism that Lingo Telecom used when it misassigned A-level attestations for spoofed calls.[148] Second, we do not believe an association can be established when a number qualifies as a Do-Not-Originate (DNO) number by default.[149] We seek comment on these beliefs.

---

[141] *See infra* Section III.C.1.b (proposing to define "initiation" and "initiating provider").

[142] *See* Somos Call Branding Comments at 14 (supporting number verification tools that are "cryptographically linked to a valid, policy-bound credential (e.g., a number-level certificate) issued by the entity with administrative authority over the number" (footnote omitted)).

[143] ATIS-1000092; *see also* ATIS-1000089 at 12.

[144] ATIS-1000092 at 1-2, 7; *see also* ATIS-1000089 at 12.

[145] In the *Eighth Caller ID Authentication Order*, the Commission declined to mandate acceptance of delegate certificates, concluding that such a mandate was beyond the scope of the third-party authentication rules adopted in that *Order* and that the record in that proceeding was insufficient to weigh the benefits and burdens of imposing such a requirement. *Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12910-11, para. 23 n.102. Given our aim to close the knowledge gap, we seek to develop a more robust record on the issue.

[146] *See, e.g.*, HTDNET, LLC Call Branding Comments at 2; WISPA Call Branding Comments at 3; Somos Call Branding Comments at 15.

[147] ATIS-1000092 contemplates that end users that are non-provider enterprises could also obtain delegate certificates from a TNSP and present them to voice service providers to establish their association with the telephone number they are using. *See* ATIS-1000092 at 9 ("[T]he VoIP Entity can be a VoIP provider or enterprise customer that has contractually leased telephone number resources from the TNSP.").

[148] *Lingo Order*, 39 FCC Rcd at 9309, para. 9.

[149] *See* 47 CFR § 64.1200(o); *see also* STI-GA, *Improper Authentication and Attestation*, at 1, https://sti-ga.atis.org/wp-content/uploads/2023/07/230724-Improper-Auth-and-Attest-Def-Final.pdf (*STI-GA Improper*

(continued….)

66. We seek comment on whether we should specify other mechanisms an originating provider can use to establish a customer's association with a telephone number. Should we require that providers obtain reasonable evidence of a customer's association with a number? Should we allow business agreements or certifications that specify the active telephone numbers the customer will use?[150] In the *Numbering Policies NPRM*, we sought comment on "better means of tracking the chain of custody of numbering resources," such a numbering database,[151] and we seek comment on whether any such solution we establish could be used by providers to verify customer associations with telephone numbers. Do commenters believe the still-in-development VESPER standard, which is described as an extension of delegate certificates that establishes an entity or individual's verified right-to-use a number after the entity is vetted, could be used for this purpose?[152]

3. Attestation Prohibitions

67. We propose to define improper attestation and establish an affirmative prohibition on voice service providers engaging in improper attestation practices, including willfully assigning improper attestations and using other criteria to make attestation-level decisions. Although we believe the existing requirement that providers implement STIR/SHAKEN using the STIR/SHAKEN standards necessarily requires that they apply attestations based on the criteria described above, we believe that codifying these prohibitions will establish a clear floor and ceiling for each attestation level and a firmer foundation for enforcement of improper attestations. We seek comment on these views.

68. *Defining "improper attestation."* We propose to define improper attestation as any attestation level that does not conform to ATIS-1000074 and the Commission's rules, including any attestation that is inconsistent with the information the voice service provider has, or is required to have, about the call. This proposed definition largely mirrors the definition established by the Governance Authority in guidance concerning improper authentication and attestations,[153] and we believe it properly captures what constitutes an improper attestation. We seek comment on this proposal.

Authentication and Attestation Guidance) (providing an example of an improper attestation as "[a]n A-Level [a]ttestation on . . . [a call originating from a telephone number that is] unallocated, invalid[,] or on a reasonable Do Not Originate list").

[150] *See* ATIS-1000074 at 12 n.1 (including among potential mechanisms by which an originating service provider may assert that its customer can legitimately use a telephone number that "the signing service provider has ascertained that the customer is authorized to use a [telephone number] (e.g., by business agreement or evidence the customer has access to use the number)"); BCID Call Branding Comments at 10 (stating that registrants in CTIA's Branded Calling ID ecosystem must submit: "a complete list of telephone numbers that the caller wishes to have vetted and validated against third-party databases and sources; a representation and warranty that the caller has the requisite rights to use the numbers; and a representation and warranty by the registrant that it has the requisite rights to submit the telephone numbers on the caller's behalf").

[151] *Combatting Illegal Robocalls Through FCC Numbering Policies*; *Implementation of TRACED Act Section 6(a)—Knowledge of Customers by Entities with Access to Numbering Resources*; *Numbering Policies for Modern Communications*; *Telephone Number Requirements for IP-Enabled Service Providers*, WC Docket Nos. 26-49, 20-67, 13-97, and 07-243, Notice of Proposed Rulemaking, FCC 26-17 at 19, para. 44 (Mar. 27, 2026) (*Numbering Policies NPRM*); *see also* ATIS-1000089 at 14 (describing a central telephone number database as a potential solution).

[152] *See* Letter from Joel Bernstein, Vice President, Somos, Inc., to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59 et al., at 1 (filed Aug. 12, 2025); Chris Wendt, Somos, Inc., VESPER Framework: A Path to RTU and Verifiable Trust for Telephone Numbers, https://www.sipforum.org/download/7-evolving-trust-in-telephone-numbers-an-industry-update-on-the-vesper-framework-rtu-and-transparency-advances/?wpdmdl=5489 (last visited Apr. 27, 2026).

[153] *STI-GA Improper Authentication and Attestation Guidance* at 1. We do not, at this time, propose to establish requirements related to improper authentication, but we note that the guidance defined improper authentication as the use of a certificate "to authenticate any information contained within an STI-GA recognized SHAKEN extension that is known to be false, or information that is outside the scope of the U.S. STIR/SHAKEN framework." *Id.*

69. *Prohibiting voice service providers from willfully making improper attestations.* We propose to prohibit voice service providers from willfully assigning attestations that are higher or lower than permissible under the STIR/SHAKEN standards and any rules we establish. ZipDX provides evidence that voice service providers may improperly apply higher-than-permissible attestations if they want their calls to be viewed as more trustworthy and lower-than-permissible attestations if they want their calls to be transmitted with less scrutiny.[154] Is there other evidence that providers are or have the incentive to willfully apply improper attestations? Should we find that specific practices constitute improper attestation, such as a C-level attestation by a provider that originates a call or an A- or B-level attestation when the provider authenticating the call is a gateway provider[155] or non-gateway intermediate provider?

70. *Prohibiting providers from using other criteria in making attestation-level decisions.* We propose to prohibit voice service providers from using other information or standards for setting attestation levels. We are concerned, in particular, about actual or *de facto* pay-for-attestation or attestation retribution or reward practices. This might occur, for example, if a provider tells a customer (whether an end user or upstream provider) that the customer may or must buy a particular product or service to receive a higher-level attestation or that the customer's attestations will be lowered if it does not take a specific action, notwithstanding what attestation would be proper for the call under the STIR/SHAKEN standards and the Commission's rules. We seek comment on this proposal. We do not intend to intervene in legitimate third-party signer or similar arrangements. We seek comment on what legitimate arrangements may be implicated by this rule, and how to ensure our rule is cabined to exclude them. Would such a prohibition risk preventing providers from using advanced tools or strategies to help inform their attestation level decisions? Do providers have evidence of such pay-for-attestation arrangements or retribution/reward schemes, and if so, are they a widespread problem? Are there other criteria on which providers rely in making attestation-level decisions that may or may not be useful to consider in this analysis?

C. Closing STIR/SHAKEN Implementation Loopholes

71. The STIR/SHAKEN framework enables an end-to-end system for authenticating caller ID.[156] For this system to work, the Identity header must travel the entire length of the call path, from originating provider to terminating provider,[157] which can include networks of various types of voice service providers.[158] The Commission's caller ID authentication rules apply to all voice service providers in a call path—namely voice service providers that perform the origination of calls,[159] non-gateway

---

[154] *See* ZipDX Feb. 17 *Ex Parte* Letter, Attach. at 3.

[155] *STI-GA Improper Authentication and Attestation Guidance* at 1-2 (providing as an example of an improper attestation "[a] C-Level [a]ttestation on a call when the [originating service provider] provides the [a]ttestation").

[156] *See* ATIS-1000074 at 6.

[157] *Second Caller ID Authentication Order*, 36 FCC Rcd at 1922-23, para. 132.

[158] *See* TransUnion Call Branding Comments at 10 (arguing that "the Commission should focus on completing Congress's original mandate—full deployment of SHAKEN throughout the [voice] ecosystem"); Numeracle Triennial Report Comments at 4 ("What's missing is ubiquitous end-to-end STIR/SHAKEN as the foundation for Rich Call Data. For the objectives to be realized, implementation must be by all the carriers, all the devices, all the pathways, and all of the time. Without this requirement, authentication data will continue to be inconsistent, incomplete, and unreliable for downstream analytics, enforcement, traceback, and consumer display." (footnote omitted)). The Commission has recognized that the existing of non-IP networks is among the most significant hinderances to full STIR/SHAKEN implementation and continues to explore avenues to advance the IP transition as well as its proposals for non-IP caller ID authentication solutions. *See Call Authentication Trust Anchor*, WC Docket No. 17-97, Notice of Proposed Rulemaking, 40 FCC Rcd 3467, 3469, para. 4-5 (2025) (*Non-IP Caller ID Authentication Notice of Proposed Rulemaking*).

[159] *Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12905, para. 17; *see also* 47 CFR §§ 64.6301(a)(2)(ii) (applying authentication requirements on voice service providers that "originate[]" SIP calls), 64.6305(d)(4)(vi)(A)-

(continued….)

intermediate providers that carry or process the calls without performing the origination or termination of them,[160] gateway providers that receive calls from foreign originating or intermediate providers at their U.S. facilities and transmit them downstream,[161] and voice service providers that perform the termination of calls.[162] But we believe that certain providers do not consider themselves subject to the caller ID authentication rules based on perceived ambiguity in the definitions for these types of providers in the Commission's rules. We also believe Commission rules that permit certain implementation exemptions are no longer needed. Additionally, non-facilities-based providers currently do not have an obligation to participate in the STIR/SHAKEN ecosystem. Beyond these issues, we are concerned about other loopholes that may contribute to the number of calls that terminate without authentication information, including providers intentionally choosing to initiate or route authenticated calls over non-IP networks that cannot carry STIR/SHAKEN authentication information, providers accepting unauthenticated SIP calls, and our rule requiring only the first intermediate provider in a call path to authenticate an unauthenticated call. We propose to close these loopholes below and seek comment on any other steps we should take to enhance STIR/SHAKEN.

1. Clarifying Definitions for Providers That Must Implement STIR/SHAKEN

72. In this section, we examine a variety of terms and definitions found in our caller ID authentication rules and seek comment on a variety of proposals to amend or adopt definitions to ensure that our rules are precise, clear, administrable, and do not enable bad actor providers to skirt their obligations. Specifically, we seek to define important terms that describe all aspects of the transmission of a call, from the point it is initiated by a calling party to the point it is received by the call recipient, and all voice service provider types that play a role in this transmission. We believe that doing so will strengthen the caller ID authentication regulatory framework by putting all voice service providers on notice as to their precise obligations.[163] We intend for the definitions we adopt to apply on a call-by-call basis, and we seek comment on this approach.[164] In connection with this task, we seek to know the universe of entities that participate in the voice ecosystem, the types of arrangements between these entities related to the provision of voice service, and whether the definitions we discuss below will indeed clarify the roles and obligations of each entity.

a. Voice Service and Voice Service Provider

73. We propose to change our interpretations of the definitions of "voice service" in the RAY BAUM'S Act and the TRACED Act to encompass the same scope of providers, and propose to define "voice service provider" in reference to the "voice service" definition in the TRACED Act. We believe the harmonized interpretations represent the best reading of the definitions and will remove ambiguity concerning the applicability of the Commission's rules concerning illegal calls to providers.

74. *Statutory definitions of "voice service."* Congress has adopted two definitions of "voice service" that apply to the Commission's rules concerning illegal calls. The 2018 RAY BAUM'S Act defines "voice service" as "any service that is interconnected with the public switched telephone network and that furnishes voice communications to an end user using resources from the North American

---

(B) (requiring voice service providers to state whether they serve end users directly or act as a wholesale provider originating calls on behalf of another provider or providers).

[160] *See* 47 CFR § 64.6302(e).

[161] *See* 47 CFR § 64.6302(d).

[162] *See* 47 CFR § 64.6301(a)(3).

[163] We also anticipate this will strengthen our RMD regulatory framework, which requires, among other things, that providers identify their role in the call path and certify to their STIR/SHAKEN implementation for the type of provider they are and whether any exemptions apply. *See* 47 CFR § 64.6305(d)(4), (e)(4), (f)(4).

[164] *See Second Caller ID Authentication Order*, 36 FCC Rcd at 1930, para. 151 (noting that "[a] single entity therefore may act as a voice service provider for some calls on its network and an intermediate provider for others").

Numbering Plan or any successor to the North American Numbering Plan adopted by the Commission under section 251(e)(1) of the Communications Act of 1934, as amended; and . . . [i]ncludes transmissions from a telephone facsimile machine, computer, or other device to a telephone facsimile machine."[165] The 2020 TRACED Act adopted an identical definition of "voice service," except that it includes the language "[w]ithout limitation, any service that enables real-time, two-way voice communications, including any service that requires internet Protocol-compatible customer premises equipment and permits out-bound calling, whether or not the service is one-way or two-way voice over internet Protocol."[166]

75. *Inconsistent interpretations of the statutory definitions.* Despite the nearly identical statutory language, the Commission's interpretation of each definition has differed, causing providers to be considered voice service providers for some of our rules pertaining to illegal calls and not for others. The Commission codified the earlier definition of "voice service" in the RAY BAUM'S Act in section 64.1600(r) of its rules and interpreted it broadly to encompasses all entities that originate, carry, or terminate voice calls through TDM, VoIP, or commercial mobile radio service.[167] It has applied that definition to the Commission's telemarketing, Truth in Caller ID, call blocking, and ring signaling integrity rules.[168] The Commission codified the later TRACED Act definition in section 64.6300(o), and interpreted it more narrowly to exclude intermediate providers.[169] It has applied that definition to its caller ID authentication rules.[170] In interpreting the TRACED Act's definition, the Commission did not discuss its prior interpretation of the RAY BAUM'S Act's definition, and only later acknowledged the divergence in interpretation.[171]

76. *Harmonizing the interpretations of "voice service."* We propose to conclude that the two "voice service" definitions cover the same scope of providers, and that the best reading of both definitions is to include intermediate providers. We believe the definitions cover the same scope of providers notwithstanding the added language in the TRACED Act's definition, because we believe that language merely provides more specificity as to what is included within the scope of "voice service" without

[165] 47 U.S.C. § 227(e)(8)(E); *see also* Consolidated Appropriations Act, 2018, Pub. L. 115-141, 132 Stat. 348, 1092 § 503(a)(2)(E) (codified at 47 U.S.C. § 227(e)(8)(E)).

[166] 47 CFR § 64.6300(o); *see* 47 U.S.C. § 227b(a)(2). The Commission defines "interconnected VoIP service" in section 9.3 of its rules. 47 CFR § 9.3.

[167] *See* 47 CFR § 64.1600(r); *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking, 35 FCC Rcd 7614, 7615 n.3 (2020) (*Third Call Blocking Order*) (adopting a broad definition of "voice service provider"); *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2575, para. 4 n.11; *see also Implementing Section 503 of RAY BAUM'S Act Rules and Regulation Implementing the Truth in Caller ID Act of 2009*, WC Docket Nos. 18-335, 11-39, Second Report and Order, 34 FCC Rcd 7303, 7313-16, paras. 24-30 (2019) (*Truth in Caller ID Second Order*) (first interpreting the RAY BAUM'S Act definition without directly addressing the intermediate providers).

[168] *See* 47 CFR §§ 64.1200, 64.1203, 64.1600(c), (d), (p), 64.1604, 64.2201.

[169] *See First Caller ID Authentication Order*, 35 FCC Rcd at 3259, para. 37; *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2575, para. 4 n.11 (interpreting the TRACED Act's definition of "voice service" to "exclude[] intermediate providers"); *First Caller ID Authentication Further Notice of Proposed Rulemaking*, 35 FCC Rcd at 3274, para. 69 ("We do not preliminarily read [the TRACED Act's] definition to include intermediate providers.").

[170] *See* 47 CFR §§ 64.6300(a), (c), (e), (h), (l), (n), 64.6301, 64.6302, 64.6303, 64.6304, 64.6305, 64.6306, 64.6307, 64.6308. *Compare, e.g.*, 47 CFR § 64.6305(a) (attaching robocall mitigation program requirements to voice service providers), *with id.* § 64.6305(b)-(c) (attaching robocall mitigation program requirements to intermediate providers).

[171] *See Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2575, para. 4 n.11; *see also Third Call Blocking Order*, 35 FCC Rcd at 7615, para. 3 n.3 (stating that the TRACED Act's definition of "voice service" is "inconsistent" with its definition of "voice service provider" for the purposes of the call blocking rules).

expanding or narrowing the scope.[172] We also believe that both definitions apply to the furnishing of voice communications to an end user directly or indirectly, such that all providers involved with an end user's voice communications, including intermediate providers, provide voice service to that end user. Both definitions require that voice communications be furnished to an end user, but we do not believe that the RAY BAUM'S Act or the TRACED Act expressly require the voice communications to be furnished *directly* or foreclose a reading that such voice communications may be furnished to an end user *indirectly*. Indeed, in one provision, the TRACED Act uses the term "voice service provider" to refer to providers that "originate *or* transmit" calls, suggesting that Congress intended the definition to include intermediate providers.[173] We seek comment on this proposal and analysis.

77. We do not believe that harmonizing the interpretation of these rules will change the scope of providers that are subject to any of our rules concerning illegal calls, and we seek comment on this view. While the proposed interpretation of the RAY BAUM's Act definition codified in section 64.1600(r) would effectively include within its scope, under our proposed interpretation, "any service that enables real-time, two-way voice communications, including any service that requires internet Protocol-compatible customer premises equipment and permits out-bound calling, whether or not the service is one-way or two-way voice over internet Protocol," we believe those providers already fell within the scope of that definition and that our proposed interpretation will not subject any new providers to our telemarketing, Truth in Caller ID, call blocking, and ring signaling integrity rules. The proposed interpretation of the TRACED Act's definition codified in 64.6300(o) also will not change the scope of providers subject to our caller ID authentication rules because our rules already require intermediate providers to implement STIR/SHAKEN in their IP networks.

78. *Defining "voice service provider."* We also propose to adopt a definition of "voice service provider" as any entity that provides voice service for a given call. This will establish a consistent approach by having definitions for each category of provider, including the umbrella category for all voice service providers. It also would make clear that whether an entity is a voice service provider is determined on a call-by-call basis. We also reiterate that the term "voice service provider" includes all initiating, originating, intermediate, and terminating providers, including facilities-based providers and non-facilities-based providers, which includes VoIP resellers and MVNOs, and irrespective of whether the provider is claiming an exemption from the STIR/SHAKEN implementation obligation.

79. *Conforming amendments to caller ID authentication rules.* In connection with our proposal to streamline the Commission's caller ID authentication rules, we propose to incorporate our proposed interpretation of the TRACED Act's definition of "voice service" inclusive of intermediate providers. Specifically, we propose to use the term "voice service provider" when a requirement applies to all categories of providers and to refer to specific categories of voice service providers when a requirement applies only to that category. We believe this specificity will facilitate our streamlining and add clarity to voice service providers' regulatory obligations depending on their position in a call path. We seek comment on this proposal and assessment.

80. *Foreign voice service provider and domestic voice service provider.* We propose to amend the definition of "foreign voice service provider" and establish a definition of "domestic voice service provider" to ensure that our proposed understanding of "voice service" does not lead to unintended confusion as to whether a provider is foreign or domestic and to deter bad actor foreign voice service providers from attempting to nominally establish themselves as domestic voice service providers to avoid scrutiny. Specifically, we propose to define "foreign voice service provider" as a voice service provider that was created, incorporated, or organized outside of the United States, regardless of whether it

[172] *See Second Caller ID Authentication Order*, 36 FCC Rcd at 1870, para. 22 ("We read the phrase 'without limitation' as indicating that the subsequent phrase 'permits out-bound calling' is not a limitation on the initial, general definition of 'voice service,' which encompasses in-bound VoIP.").

[173] TRACED Act § 13(e) (emphasis added). We also maintain our understanding that "voice service" includes termination.

has an office, operation, or facilities in the United States. We also propose to define "domestic voice service provider" as a voice service provider that is not a foreign voice service provider. We believe that these changes are necessary because the current definition of "foreign voice service provider" is a provider that provides voice service "outside the United States." Under our proposed understanding of voice service as furnishing voice communications to an end user both directly and indirectly, this means that any provider in the United States may be a "foreign voice service provider" so long as it terminates calls outside of the United States. We thus instead seek to tie the definition of "foreign voice service provider" to the business's location—where it was created, incorporated, or organized—rather than the nature of the service that it provides. We believe our proposed definition of "domestic voice service provider" as not a foreign voice service provider adequately covers the scope of providers that are created, incorporated, or organized within the United States. We also believe that these definitions will enable us to provide a clearer definition of "gateway provider," as we propose to do below. We seek comment on these proposals.

b. Initiation and Initiating Provider

81. We propose to establish definitions of "initiation" and "initiating provider" for the purposes of our caller ID authentication rules to clarify the relationship of a customer to a voice service provider and to remove ambiguity as to which entity is responsible for each phase in the lifecycle of a call. Specifically, we propose to define "initiation" as "the action performed by a voice service customer in commencing a call, and does not include origination" and "initiating provider" as "a voice service provider that performs initiation for its end users' calls."

82. We believe that adopting such definitions of "initiation" and "initiating provider" is likely necessary to enable us to better describe the action performed by a customer—such as an end user or a provider that serves end users—in placing a call, as distinct from the technological processes performed by the originating provider to enable that customer's call to traverse the voice network. In particular, under this definition, a non-facilities-based resale provider (as a customer of a facilities-based wholesale provider) that has a direct relationship with an end user would perform the "initiation" of a call on behalf of that end user, but the facilities-based wholesale provider would perform the "origination" of that call. When the facilities-based provider serves an end user directly (meaning the end user is the customer of the facilities-based provider), it would perform the "origination" of the end user's calls, while the end user would perform the "initiation." We also believe that, according to this proposed definition, only the non-facilities-based provider that directly serves end users can be considered an initiating provider. Non-facilities-based providers in the middle of a chain of resellers would not fall within the definition, which we believe is appropriate given our understanding that they are not technologically in the path of a call.[174]

83. We also believe that the existence of ambiguity as to how the term "initiation" is used in the ATIS standards and in our orders suggests that adopting a definition is appropriate. For example, in the *Eighth Caller ID Authentication Order*, the Commission used the term "initiate" in one instance to differentiate the action that a voice service customer does from a voice service provider.[175] The Commission described a complex call path in which an originating provider's customer is not the ultimate end user of a voice service, "such as where an originating service provider authenticates calls *initiated* by a reseller that itself maintains a direct relationship with the calling party."[176] However, given the lack of a

[174] These providers would still be subject to the requirement to ensure the services they resell are not used to transmit illegal calls under section 64.1200(n)(5) of our rules, including the KYUP requirements we propose above.

[175] *See Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12902, para. 11 ("[A]n originating service provider authenticates calls initiated by a reseller"); *id.* at 12905, para. 15 ("[A] wholesale provider originates a call onto the public network for its reseller customer that initiated the call on behalf of an end user.").

[176] *Id.* at 12901-02, para. 11 (emphasis added); *see also id.* at 12905, para. 15 ("These scenarios involve circumstances where the end user of the voice service is not the same as the 'customer,' as defined by the ATIS-1000088 Technical Report, such as when a wholesale provider originates a call onto the public network for its reseller customer that *initiated* the call on behalf of an end user." (emphasis added)). The Commission also used the

(continued….)

codified definition in the Commission's rules or ATIS's standards, the Commission in the same *Order* also used the word as a synonym for origination.[177] The ATIS standards appear to use the term in a similar way to our proposed definition, but limits its usage to customers that have a direct relationship with an originating provider.[178]

84. Do commenters agree that a definition of "initiation" and "initiating provider" is necessary to enable us to be more precise about exactly which actions or entities we are describing when discussing the initial stage in the life of a call? Should we adopt a different definition of "initiation," such as only the action performed by a direct voice service customer of an originating provider? If so, how should we describe the action that is performed by the end user and the action performed by an end user's voice service provider that is not the customer of the originating provider? Should we instead define "initiate" as only the action performed by an end user in commencing a call? In that case, how should we define the action performed by the end user's voice service provider when it is not the originating provider? Do we need to establish a term and definition other than resale for the action that resellers in the middle of a chain of resellers perform? If yes, what should that term and definition be? Should we define initiation to include any such action?

c. Origination and Originating Provider

85. We propose to establish a definition of "origination" for the purposes of our caller ID authentication rules to remove ambiguity as to voice service providers' obligations at this stage in a call path, and propose to define "originating provider" in reference to this definition. While the Commission has interpreted the word consistently with the ATIS standards when describing its caller ID authentication rules,[179] we have not adopted a definition in our rules. Because of our proposal above to interpret "voice service" as including all providers that carry voice communications on behalf of an end user, regardless of a direct relationship with the end user,[180] we find it necessary to revise our caller ID authentication rules by replacing the term "voice service provider" with the term "originating provider" and/or "terminating provider" where appropriate.[181]

86. *Commission precedent and ATIS standards.* The Commission's caller ID authentication rules apply, as relevant here, to voice service providers that originate calls.[182] ATIS-1000089 defines

term "initiated" to refer to the action a reseller's end user does, rather than the reseller on behalf of an end user. *See id.* at 12908, para. 19 n.88 (encouraging voice service resellers to "provide . . . wholesalers with enough information to enable them to determine the appropriate attestation level of the calls *initiated* by the resellers' end users" (emphasis added)).

[177] *See id.* at 12910, para. 23 n.100 ("We disagree . . . that we should simply issue a declaratory ruling to clarify that the Commission's rules already require voice service providers and intermediate providers to ensure that calls that they *initiate* onto the voice network are signed with their certificate, and to make all attestation-level decisions, regardless of which entity actually performs the act of signing." (emphasis added)).

[178] For example, ATIS-1000088 describes an "initiating [user agent]" that "signals the call to the originating [service provider]" and which is "typically in the possession of or under the control of a 'customer,' which is typically an entity that has a direct commercial relationship with the originating [service provider] and may or may not be the ultimate source of the call (the end-user entity)." ATIS-1000088 at 9. This "SIP [User Agent]" is "authenticated by the originating service provider . . . network" and, "[w]hen the SIP [User Agent] is under direct management control of the [originating service provider], the [originating service provider's] network can assert the calling party identity in originating SIP INVITE requests initiated by the SIP [User Agent]." ATIS-1000074 at 8.

[179] *See Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12907, para. 18.

[180] *See supra* Section III.C.1.a.

[181] We propose to define "terminating provider" below. *See infra* Section III.C.1.e.

[182] *Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12905, para. 17; *see also* 47 CFR §§ 64.6301(a)(2)(ii) (applying authentication requirements on providers that "originate[]" SIP calls), 64.6305(d)(4)(vi)(A)-(B) (requiring

(continued….)

"originating service provider" as "[t]he service provider that handles the outgoing calls from a customer at the point at which they are entering the public network."[183] An originating provider may serve end user customers directly, or indirectly—such as through a voice service provider customer (e.g., a reseller or value-added service provider).[184] In both circumstances, as stated in the ATIS standards and in the *Eighth Caller ID Authentication Order*, the originating provider is the entity that handles the call at the point at which it is entering the public network.[185]

87. *Need for establishing a definition of "origination."* We find that the absence of a specific definition of "origination" in our caller ID authentication rules has led to persistent industry confusion as to the scope of caller ID authentication obligations applicable to certain providers. On one end of the spectrum, for example, there appears to be some ambiguity as to whether an entity is a voice service provider (and therefore subject to caller ID authentication requirements) or is instead an end user.[186] On the other end of the spectrum, although the Commission stated clearly in the *Eighth Caller ID Authentication Order* that a wholesale provider originating voice traffic on behalf of a non-facilities-based reseller fulfills its own STIR/SHAKEN authentication obligation as an originating provider when signing the reseller's traffic,[187] some wholesale providers may nevertheless mistakenly consider themselves to be "intermediate" providers carrying their reseller customers' traffic, and not originators of their resellers' traffic. This misunderstanding of origination may cause a wholesale provider to think that it may apply only a C-level attestation, because the first criteria for both A- and B-level attestation is responsibility for origination.[188] Another source of potential confusion may be that, outside of the Commission's caller ID authentication rules, the Commission has used the word "originate" or "origination" in a variety of different ways.[189] Do commenters agree that confusion exists and is at least

voice service providers to state whether they serve end users directly or act as a wholesale provider originating calls on behalf of another provider or providers).

[183] ATIS-1000089 at 4.

[184] *See, e.g.*, ATIS-1000088 at 5 ("[A]n end user may directly be the customer of a service provider or may indirectly use the VoIP-based telecommunications service through another entity such as a reseller or value-added service provider.").

[185] *See Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12905-08, paras. 17-19 & n.82; *cf., e.g.*, 47 CFR §§ 9.3 (defining interconnected VoIP service as "[p]ermit[ting] users generally to receive calls that *originate* on the public switched telephone network and to terminate calls to the public switched telephone network" (emphasis added)), 9.10(s)(1) (describing voice calls "originating on [a nationwide CMRS provider's] internet Protocol-based network[]"), 9.28 (defining "[o]riginating service providers" as "[p]roviders that originate 911 traffic").

[186] *See, e.g.*, Numeracle June 5, 2023 Comments at 5 ("For example, a practice management software company for medical offices that implements a feature to allow its customers to schedule automated calls for appointment reminders probably does not consider itself to be a voice service provider subject to the Commission's rules. It partners with a company that performs the traditional originating service provider functions and routes the call and complies with regulatory obligations. Is the software company that has enacted such a feature an [originating service provider] subject to STIR/SHAKEN? The answer to that question is unclear.").

[187] *See Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12906-07, para. 17 & n.82.

[188] *See* ATIS-1000074 at 12.

[189] *Compare, e.g.*, 47 CFR §§ 9.3 (defining interconnected VoIP service as "[p]ermit[ting] users generally to receive calls that *originate* on the public switched telephone network and to terminate calls to the public switched telephone network" (emphasis added)), 9.10(s)(1) (describing voice calls "originating on [a nationwide CMRS provider's] internet Protocol-based network[]"), 9.28 (defining "[o]riginating service providers" as "[p]roviders that originate 911 traffic"), *with, e.g.*, 47 CFR §§ 1.50001(a) (defining "Advanced communications service" as "high-speed, switched, broadband telecommunications capability that enables users to *originate* and receive high-quality voice, data, graphics, and video telecommunications using any technology with connection speeds of at least 200 kbps in either direction" (emphasis added)), 4.7(f) (describing telephone numbers as being able to "*originate*, or terminate telecommunications" (emphasis added)), 6.3(c) (describing CPE as being used "to *originate*, route, or terminate

(continued….)

partly responsible for non-compliance with our caller ID authentication rules, including improper attestations? If so, do commenters agree that this confusion merits establishing definitions of "origination" and "originating provider" in our rules, or do commenters advocate for a different solution?

88. *Definition of "origination" and "originating provider."* In the context of our caller ID authentication rules, we propose to define "origination" as the technological act of placing a customer's outgoing call onto the network using the voice service provider's own facilities, and "originating provider" as the voice service provider whose network performs the origination of a given call. We find that this definition is consistent with ATIS's usage,[190] but also includes additional detail concerning the facilities used to place the call onto the network, which we believe is necessary to clear up industry confusion. Specifically, we find that tying origination to a technological act of placing a call onto the network using a voice service provider's own facilities means that a non-facilities-based provider cannot perform the "origination" of its customers' calls. As in the ATIS Technical Report, we use the term "customer" rather than "end user" to recognize instances when a facilities-based provider is originating calls on behalf of a non-facilities-based provider customer.[191] We seek comment on our proposed definitions. Are they sufficiently clear to distinguish originating providers from intermediate providers that merely "carr[y] or process[] voice traffic"? Do commenters agree that a non-facilities-based provider cannot perform the "origination" of voice traffic on behalf of its customers and that this is consistent with ATIS' usage of the term "origination"? If not, should we adopt a more expansive definition of "origination" to include when a call is "initiated" by a customer with a non-facilities-based provider, as we proposed to define "initiation" above? If so, should we use qualifying words to differentiate "types" of origination, such as "facilities-based origination" and "non-facilities based origination"?

d. Intermediate Provider, Gateway Provider, and Non-Gateway Intermediate Provider

89. *Intermediate provider.* We propose to modify the definition of "intermediate provider" in section 64.6300(g) of the Commission's rules only to account for the new definitions of "voice service provider," "origination," and "termination."[192] We believe that the existing definition is otherwise sufficiently precise as to when a voice service provider is serving as an intermediate provider with respect to its caller ID authentication obligations, especially when coupled with the proposed definitions of "origination" and "termination." We seek comment on this view. Does the definition, for example, prevent originating providers from shirking their STIR/SHAKEN authentication obligations when handling calls from a non-facilities-based reseller customer?

90. *Gateway provider.* We propose to modify the definition of "gateway provider" in section 64.6300(d) of the Commission's rules to account for the new definitions of "domestic voice service provider" and "foreign voice service provider."[193] We believe that because the existing definition defines a gateway provider as a provider that has facilities located in the United States, it has incentivized bad

telecommunications" (emphasis added)), 7.3(c) (same), 9.10(d)(2) (describing a handset as capable of "originat[ing] a 911 call").

[190] *See, e.g.*, ATIS-1000089 at 4 (defining "Originating Service Provider" as "[t]he service provider that handles the outgoing calls from a customer at the point at which they are entering the public network").

[191] We propose definitions of "customer" and "end user" below. *See infra* Section III.C.1.h.

[192] *See* 47 CFR § 64.6300(g). Specifically, we propose to change "any entity that carries or processes traffic that traverses or will traverse the public switched telephone network at any point" to a "voice service provider that carries or processes traffic" since the "voice service provider" definition captures the relationship of the traffic to the public switched telephone network. Additionally, we propose to change "originates" and "terminates" to "performs the origination or termination" to grammatically accommodate the newly proposed terms.

[193] *See* 47 CFR § 64.6300(d). Specifically, we propose to define "gateway provider" as a "domestic voice service provider that is an intermediate provider that accepts voice calls directly from a foreign voice service provider before transmitting the call downstream to another domestic voice service provider."

actor foreign voice service providers to establish nominal facilities in the United States with the intent to avoid scrutiny by gateway providers when their call traffic enters the United States. Given that our proposed definition of "foreign voice service provider" refers to a voice service provider that was created, incorporated, or organized outside of the United States, regardless of whether it has an office, operation, or facilities in the United States, we believe that defining gateway provider in reference to the foreign voice service provider definition will more clearly delineate when a voice service provider is functioning as a gateway provider for any given call. We seek comment on this proposed definition. Should we modify the definition in a different way to ensure that bad actor foreign voice service providers cannot avoid scrutiny? For instance, NCLC argues that the existing definition "is underinclusive to the extent that some domestically originated calls will feature foreign calling parties either because a foreign participant is connected after an otherwise domestic call is answered or because a nominally domestic provider is in fact operating as a foreign proxy."[194] It requests that the Commission define "foreign-originated call" as "any call received from a 'foreign originating provider or foreign intermediate provider.'"[195] Does our proposed definition resolve NCLC's concern? If not, should we adopt a definition of "foreign originated call" as NCLC proposes?[196]

91. *Non-gateway intermediate provider.* We believe that the definition of "non-gateway intermediate provider" in section 64.6300(i) of the Commission's rules is sufficiently precise as to when a voice service provider is serving as a non-gateway intermediate provider with respect to its caller ID authentication obligations that we propose to leave it substantively unaltered, and we seek comment on this proposal.[197]

e. Termination and Terminating Provider

92. To remove ambiguity as to voice service providers' obligations at the final stage in a call path, we propose to establish a definition of "termination" for the purposes of our caller ID authentication rules and propose to define "terminating provider" in reference to this definition. Specifically, we propose to define "termination" as the technological act of serving to a customer an incoming call received on a voice service provider's own facilities that are interconnected with the public network, and "terminating provider" as the voice service provider whose network performs the termination of a given call. We believe that this proposed definition is consistent with ATIS's definition.[198] Under the STIR/SHAKEN framework and the Commission's rules, terminating providers are responsible for performing the SHAKEN verification function to ensure that the caller ID associated with the call it terminates was properly authenticated.[199] We believe that tying termination to the technological act of serving a call received on the provider's own facilities makes clear that a non-facilities-based provider

[194] *See* NCLC Call Branding Reply at 6.

[195] *Id.* at 5.

[196] We note that the Commission declined to adopt a similar proposal when it first established the "gateway provider" definition. *Gateway Provider Order*, 37 FCC Rcd at 6876, para. 26.

[197] *See* 47 CFR § 64.6300(i).

[198] *See* ATIS-1000089 at 5 (defining "Terminating Service Provider (TSP)" as "[t]he [service provider] whose network terminates the call (i.e., serving the called party)").

[199] *See First Caller ID Authentication Order*, 35 FCC Rcd at 3245, para. 6 ("When the terminating voice service provider receives the call, it sends the SIP INVITE with the Identity header to a verification service, which uses the public key that corresponds uniquely to the originating voice service provider's private key to decode the encrypted information and verify that it is consistent with the information sent without encryption in the SIP INVITE. The verification service then sends the results of the verification process—including whether the decoding process was successful and whether the encrypted information is consistent with the information sent without encryption—to the terminating voice service provider."); *see* 47 CFR §§ 64.6301(a)(3) (requiring voice service providers to "[v]erify caller identification information for all SIP calls it receives from another voice service provider or intermediate provider which it will terminate and for which the caller identification information has been authenticated"), 64.6300(n) (defining "[v]erify caller identification information").

does not "terminate" calls for its end users. As in the definition of "origination," we use the term "customer" rather than "end user" to preserve the possibility of a facilities-based provider terminating calls on behalf of a non-facilities-based provider customer. We seek comment on this definition. Do commenters agree that our definition should be limited to our caller ID authentication rules? Do commenters agree that, under the ATIS standards, a non-facilities-based provider cannot "terminate" voice traffic on behalf of its end users? Should we instead adopt a more expansive definition of "termination" to include service of an incoming call to an end user by a non-facilities-based provider? For example, should we use "termination" in a generic sense of "end point service" of an incoming call along with qualifying words to differentiate "types" of termination, such as "end user termination" or "facilities-based termination"?

f. Facilities-Based Provider and Non-Facilities-Based Provider

93. To ensure that providers know whether they have an obligation to implement STIR/SHAKEN or are subject to the implementation exemption for providers that lack control of the network infrastructure necessary to implement STIR/SHAKEN (hereafter "non-facilities-based provider implementation exemption"), we: (1) propose to define the terms "facilities-based provider" and "non-facilities-based provider" for the purposes of our caller ID authentication rules and seek comment on how best to do so; and (2) propose to codify and clarify the non-facilities-based provider implementation exemption as it relates to those terms. The Commission has previously only given limited guidance on what it means to "lack control of the network infrastructure." Our intent with these proposals therefore is to make clear which providers may claim the "non-facilities-based provider exemption" by: *first*, clarifying what it means to be a "non-facilities-based provider"; and *second*, clarifying what it means to lack control of the network infrastructure necessary to implement STIR/SHAKEN. Although non-facilities-based providers do not have a STIR/SHAKEN implementation obligation under the exemption, we put them on notice that, to the extent they serve end users directly, they may nevertheless have STIR/SHAKEN-related duties under our separate proposal to require that all voice service providers that serve end users directly (including non-facilities-based providers) make attestation-level decisions for their end users' SIP calls.[200]

94. *Defining "facilities-based provider" and "non-facilities-based provider."* As a starting point for defining "facilities-based provider" and "non-facilities-based provider," we believe the definitions should reflect the following assumptions:

> *First*, we believe we should define these terms without reference to the facilities' ability to carry STIR/SHAKEN authentication information to reflect that a voice service provider can also be a facilities-based provider when it provides voice service over its own non-IP networks.
>
> *Second*, we believe that "facilities" refers to network infrastructure, such as physical elements (e.g., switches, routers, copper wires, fiber wires, spectrum, wireless transmitters and receivers, and satellites) and any software, services, or facilities used to operate those physical elements.
>
> *Third*, we believe a facilities-based provider is one that owns, leases, and/or operates the network infrastructure, and therefore "controls" those elements.
>
> *Fourth*, we believe that whether a provider is facilities-based or non-facilities-based is circumstantial, not conditional, meaning that a provider may be facilities-based in some circumstances and not in others.

95. We seek comment on these views. We also seek comment on whether we should incorporate a fifth assumption based on the relationship a provider has with end users, and if so, what that assumption should be. For example, the definition of "facilities-based provider" in our FCC Form 477

[200] *See infra* Section III.C.3.

rules describes such providers as entities with facilities that terminate at end user premises.[201] In the *Fourth Caller ID Authentication Order*, the Commission implicitly adopted a similar, but narrower definition of "facilities-based," as relating to the last-mile connection between the voice service provider's network and an end user. Specifically, as part of its determination that "non-facilities-based small voice service providers" "must implement STIR/SHAKEN in the IP portions of their network," the Commission "define[d] a voice service provider as 'non-facilities-based' if it offers voice service to end-users solely using connections that are not sold by the provider or its affiliates."[202] In other words, for example, a provider that owns a switch that it uses to provide voice service but does not own the fiber wire that connects the switch to the end user would be a non-facilities-based provider under that definition. Should one of these approaches be reflected in a fifth assumption? Conversely, we note that our existing definition of "gateway provider" includes a reference to such providers' facilities,[203] even though those facilities may not connect with end users, suggesting that intermediate providers could qualify as a facilities-based provider. Should we follow this approach and simply decline to adopt a fifth assumption?

96. We also seek comment on whether our assumptions as to how "facilities-based" should be defined are valid with respect to all voice service providers that should be obligated to implement STIR/SHAKEN. Do the assumptions hold true for all originating, intermediate, and terminating providers as we propose to define those terms above? For example, given our proposal to include "facilities" in the definition of "origination,"[204] do commenters agree that a non-facilities-based provider cannot and should not be considered an originating provider? If so, and thus all originating providers are "facilities-based," are our assumptions accurate as to all originating providers? We also seek comment on whether our assumptions about what "facilities-based" should mean are true for other types of providers. For example, do our assumptions describe some or all VoIP resellers and MVNOs? What about PBXs (hosted or otherwise), dialing platforms, cloud service providers, over-the-top service providers, call centers, value-added-service providers, or TNSPs?[205]

97. If commenters agree with our proposed assumptions about "facilities-based providers,"

---

[201] *See* 47 CFR § 1.7001(a)(2) (defining "facilities-based provider" as an entity that provides service using: "(i) Physical facilities that the entity owns and that terminate at the end-user premises; (ii) Facilities that the entity has obtained the right to use from other entities, such as dark fiber or satellite transponder capacity as part of its own network, or has obtained; (iii) Unbundled network element (UNE) loops, special access lines, or other leased facilities that the entity uses to complete terminations to the end-user premises; (iv) Wireless spectrum for which the entity holds a license or that the entity manages or has obtained the right to use via a spectrum leasing arrangement or comparable arrangement pursuant to sections 1.9001-1.9080 of our rules; or (v) Unlicensed spectrum").

[202] *Call Authentication Trust Anchor*, WC Docket No. 17-97, Fourth Report and Order, 36 FCC Rcd 17840, 17848, para. 19 (2021) (*Fourth Caller ID Authentication Order*). It adopted this definition because it "captures those providers that lack facilities-based voice connections [and] provides certainty to both affected voice service providers and the Commission." *Id.* at 17848-49. It stated that "[a] voice service provider's voice service that does not use connections sold by the provider or its affiliates, by definition, 'rides atop' another provider's transmission service. Therefore, such voice service is not offered over the voice service provider's own facilities." *Id.* at 17849. The Commission noted that a voice service provider "readily knows whether it is offering voice service that relies on its own (or its affiliates') facilities . . . , and therefore can easily determine whether it is subject to this definition." *Id.*; *see also* 47 CFR § 64.6300(h) (defining "non-facilities-based small voice service provider" for the purposes of our caller ID authentication rules as "a small voice service provider that is offering voice service to end-users solely using connections that are not sold by the provider or its affiliates").

[203] *See* 47 CFR § 64.6300(d) ("The term "gateway provider" means a U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities . . . .").

[204] *See supra* Section III.C.1.c.

[205] Our understanding is that these arrangements are captured by terms like unified communications as a service (UCaaS), communications platform as a service (CPaaS), and contact center as a service (CCaaS), but we seek comment on the best shorthand terminology to use to refer to these types of arrangements.

how should we distill such assumptions into a definition of "facilities-based provider" and "non-facilities-based provider" for the purposes of our caller ID authentication rules? If we should assume that a facilities-based provider has a relationship with an end user, would the existing definition in our FCC Form 477 rules satisfy all five of the assumptions?[206] Should we instead adopt an end-user-connection-based definition that follows the "non-facilities-based small voice service provider" definition adopted in the *Fourth Caller ID Authentication Order*?[207] If we decline to assume that a facilities-based provider has a relationship with an end user, should we adopt a definition of "facilities-based provider" that includes any provider with facilities used in the call path, including intermediate providers? If we do not adopt a definition consistent with the "non-facilities-based small voice service provider" definition in the *Fourth Caller ID Authentication Order*, is it necessary to modify our rules to clarify the implementation obligation for such providers in light of the fact that the implementation exemption for such providers has expired?[208] If our assumptions describe any providers that should not be obligated to implement STIR/SHAKEN, how should we define "facilities-based-provider" and/or "non-facilities-based provider" to exclude such providers? For example, should we define "non-facilities-based provider" simply as "a provider that is not a facilities-based provider"? Or, should we also include in the definition of "non-facilities-based provider" additional types of providers that otherwise would have satisfied a definition of "facilities-based provider" in order to ensure they are subject to the non-facilities-based provider exemption?

98. *Codification of non-facilities-based provider exemption.* We propose to codify in our rules an exemption from implementing STIR/SHAKEN for non-facilities-based providers, however we define that term, which the Commission has thus far referred to as an exemption for providers that lack control of the network infrastructure necessary to implement STIR/SHAKEN.[209] Although the Commission first acknowledged this exemption in the *First Caller ID Authentication Order*,[210] it has not codified the exemption in its rules[211] or fully explained its scope, which we believe has resulted in industry confusion. In proposing to codify the exemption, we seek to resolve this confusion.

99. As an initial matter, we believe this exemption is inherent in the STIR/SHAKEN

[206] 47 CFR § 1.7001(a)(2). We note that in the *Fourth Caller ID Authentication Order*, the Commission declined to adopt a similar definition to that in our FCC Form 477 rules because it would place a higher compliance obligation on small voice service providers to determine whether they meet its terms compared to the Commission's more straightforward definition. *See Fourth Caller ID Authentication Order*, 36 FCC Rcd at 17850, para. 21.

[207] *Fourth Caller ID Authentication Order*, 36 FCC Rcd at 17848, para. 19; 47 CFR § 64.6300(h).

[208] *Fourth Caller ID Authentication Order*, 36 FCC Rcd at 17851, para. 23 (concluding that non-facilities-based small voice service providers "must implement STIR/SHAKEN in the IP portions of their network by June 30, 2022").

[209] This exemption only relates to providers whose calls are originated in IP and "is distinct from the Commission's continuous extension for non-IP portions of a provider's network." *See Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12898-99, para. 8 & n.35; 47 CFR § 64.6304(d).

[210] *See First Caller ID Authentication Order*, 35 FCC Rcd at 3260, para. 40 ("Finally, we clarify that the rules we adopt today do not apply to providers that lack control of the network infrastructure necessary to implement STIR/SHAKEN."); *Second Caller ID Authentication Order*, 36 FCC Rcd at 1868, para. 19 (citing *First Caller ID Authentication Order*, 35 FCC Rcd at 3260, para. 40); *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2592, para. 36 n.137 ("When referencing those providers 'without' a STIR/SHAKEN implementation obligation, we mean those providers that are subject to an implementation extension . . . or that lack control over the facilities necessary to implement STIR/SHAKEN."); *Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12898-99, para. 8 ("Providers that lack control over the network infrastructure necessary to implement STIR/SHAKEN, such as switches for voice service in the IP portion of their network, are exempt from STIR/SHAKEN implementation requirements." (footnote omitted)); *see also* 47 CFR § 64.6305(d)(2)(i), (e)(2)(i), (f)(2)(i).

[211] However, providers may claim the exemption if they certify to partial or no STIR/SHAKEN implementation in their RMD filing, so long as they explain in detail how it applies to them. *See Sixth Caller ID Authentication Order and Further Notice*, 38 FCC Rcd at 2588-93, paras. 28-39; *see also* 47 CFR § 64.6305.

framework and implicitly adopted in the TRACED Act. Because the STIR/SHAKEN framework relies on the transmission of information in the Identity header of the SIP INVITE, it only operates on the IP portions of a voice service provider's network.[212] Our rules, mirroring the TRACED Act, therefore only require voice service providers to implement the STIR/SHAKEN authentication framework in the IP portions of their networks.[213] That is, because STIR/SHAKEN only works in IP networks, only facilities-based voice service providers that have IP-based facilities used for voice service on which they can install STIR/SHAKEN solutions are subject to this implementation requirement. If a provider does not have IP-based facilities for voice services on which it can install STIR/SHAKEN solutions, it cannot technically implement STIR/SHAKEN and therefore does not have an implementation obligation.[214]

100. We also believe the scope of the exemption is clarified based on the second and third assumptions we set out above about facilities-based providers and non-facilities-based providers. We believe that part of the confusion about the scope of the existing exemption stems from a lack of guidance from the Commission as to the meaning of "network infrastructure" and "control."[215] Under the second assumption, we describe network infrastructure as including physical elements (e.g., switches, routers, copper wires, fiber wires, spectrum, wireless transmitters and receivers, and satellites) and any software, services, or facilities used to operate those physical elements. Under the third assumption, we describe facilities-based providers as having "control" over the network infrastructure, which we describe as owning, leasing, and/or operating the network infrastructure. When viewed together, we believe a customer (including a non-facilities-based provider) that purchases services from a facilities-based provider is simply a user of the facilities-based provider's network infrastructure and cannot own or control the network infrastructure necessary to implement STIR/SHAKEN. We further believe that a facilities-based provider cannot give control of its network infrastructure to a non-facilities-based provider (and thereby essentially turn a non-facilities-based provider into a facilities-based provider) by, for example, providing the non-facilities-based provider with access to software that enables them to enter attestations and certificate information for the purpose of authentication.[216] We seek comment on these

[212] *First Caller ID Authentication Report and Order*, 35 FCC Rcd at 3245, para. 7; ATIS-1000074 at 1 (describing SHAKEN as a framework "for the validation of legitimate calls and the mitigation of illegitimate spoofing of telephone identities *on IP-based service provider voice networks*" (emphasis added)); *see also* Consumer Access & Choice Coalition Call Branding Reply at 7 ("STIR/SHAKEN implementation relies on control over the IP portion of the network infrastructure because the entire framework is defined around SIP signaling and Internet-style public key cryptography, which only operate natively in IP environments. STIR/SHAKEN signing and verification must occur at SIP-capable IP elements (e.g., softswitches) that can insert and interpret identity headers and manage certificates.").

[213] *See* 47 CFR § 64.6301; *id.* § 64.6302; 47 U.S.C. § 227b(b)(1)(A).

[214] *See, e.g.*, ACA Connects Comments at 2 (claiming that "resellers of voice service . . . lack control of the infrastructure necessary to implement STIR/SHAKEN and therefore do not bear any implementation obligation"); WISPA Call Branding Comments at 1 ("Eliminating the exemption would place VoIP resellers in an untenable position, as it is not possible for such providers to attain STIR/SHAKEN compliance."); Consumer Access & Choice Coalition Call Branding Reply at 7-8.

[215] The *Eighth Caller ID Authentication Order* gave one example of "network infrastructure," namely "switches for voice service in the IP portion of their network." *Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12898-99, para. 8.

[216] In other words, we do not believe a facilities-based provider can establish a STIR/SHAKEN implementation obligation for another provider by virtue of the services it provides. *Cf. Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12908, para. 19 & n.88 ("We . . . decline [to] incorporate providers that lack control over the network infrastructure necessary to implement STIR/SHAKEN as first parties under th[e third-party authentication] framework when they 'hold [themselves] out as the originating service provider (even though [they] do[] not actually "touch" the call)' and 'arrange for somebody (the infamous third party) to sign the calls' for them. . . . [S]uch a fluid conception of 'originating service provider' would conflict with the text of the Commission's rules establishing the scope of providers subject to a STIR/SHAKEN implementation obligation and would be inconsistent with how the ATIS standards and technical reports use that term.").

views. If we decline to follow the meanings of "facilities-based" and "non-facilities-based" used in the *Fourth Caller ID Authentication Order*, could a provider be facilities-based for the purposes of that *Order* but non-facilities-based for the purposes of this exemption? If so, do we need to resolve that issue given that the "non-facilities-based provider" extension in the *Order* has lapsed?

101. Given the express limitation of our STIR/SHAKEN implementation obligation to a voice service provider's IP networks, codification of the exemption may not be strictly necessary, but we now believe doing so will promote regulatory clarity.[217] We seek comment on our proposal and beliefs. Is the scope of the exemption sufficiently clear? Are there any potential downsides or unintended consequences to codification? We stress our view that the exemption is not status-based, but circumstantial. That is, if a provider is facilities-based in some circumstances (such as with respect to certain calls) and not in others, it has an implementation obligation in the former circumstance and not the latter. We invite comment on these proposed conclusions and analysis.

g. Upstream and Downstream

102. Given the confusion in the record,[218] and their importance in determining caller ID authentication and KYUP obligations, we propose to define the terms "upstream" and "downstream" for the purposes of our caller ID authentication rules. Specifically, we propose to define "upstream" as nearer to the source of a call, and "downstream" as nearer to the destination of a call. This usage accords with the definitions given for the words in the dictionary as applied to a stream or river.[219] Thus, as applied to providers, an "upstream provider" is a provider that is closer to the source of the call, and a "downstream provider" is closer to the destination of the call. We are careful to not conflate the "source" of a call with the "origination point" of a call, as the ATIS standards consider non-facilities-based providers that are near the source of the call to be "upstream" of the facilities-based providers that originate the calls, for example.[220] While undefined in the Commission's rules, the rules use the term "upstream" consistently with our proposed definition.[221] Similarly undefined in the Commission's rules, our proposed definition of "downstream" accords with existing rules that use the term.[222] We seek comment on our proposed definitions.

h. Customer and End User

103. To remove ambiguity and ensure that voice service providers understand their regulatory obligations, we propose to define the terms "customer" and "end user" for the purposes of our caller ID authentication rules. Specifically, we propose to define "customer" as any individual or entity that

---

[217] In the *Call Branding FNPRM*, we sought comment on whether and how to repeal the exemption. *See Call Branding FNPRM* at 20, para. 67. Upon further evaluation, we do not believe the exemption can be repealed because it is a necessary outcome of the fact that STIR/SHAKEN can only be implemented in IP networks.

[218] *See, e.g.*, Consumer Access & Choice Coalition Call Branding Reply at 7-8 (describing wholesale providers that sign resellers' calls as "upstream" of those resellers).

[219] *See, e.g.*, *Upstream*, Webster's New International Dictionary (2d ed. 1934) (defining "upstream" as "[a]t or toward a location nearer the source of a stream"); *Downstream*, Webster's New International Dictionary (2d ed. 1934) (defining "downstream" as "[i]n the direction or flow of a stream").

[220] *See, e.g.*, ATIS-1000088 at 9 ("[T]he 'UNI' will refer to the interface between the customer networks or devices and the originating [service provider] network and not any *upstream* interfaces between the customer and any indirect end users that may be the ultimate source of calls received by the originating [service provider].").

[221] *See, e.g.*, 47 CFR §§ 64.6300(d)(2) (defining "[r]eceives a call directly" as "the foreign provider directly *upstream* of the gateway provider in the call path sent the call to the gateway provider, with no providers in-between" (emphasis added)), 64.6305(2)(ii) (describing section 64.1200(n)(5) as an obligation on a gateway provider to "know its *upstream* providers" (emphasis added)).

[222] *See, e.g.*, 47 CFR § 64.6300(d) (defining "gateway provider" as "a U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call *downstream* to another U.S.-based provider").

purchases voice service from a voice service provider, and "end user" as the ultimate consumer of voice service. The ATIS-1000088 Technical Report defines "customer" as "[t]ypically a service provider's subscriber, which may or may not be the ultimate end-user of the telecommunications service."[223] Under this definition, a customer "may be a person, enterprise, reseller, or value-added service provider."[224] In the *Eighth Caller ID Authentication Order*, the Commission declined to adopt a definition of "customer" that means "solely the end user that initiated the voice service," as was suggested by certain commenters, because it was not necessary to do so for the purposes of the third-party authentication rules it adopted in that *Order*.[225] In doing so, however, it noted that such a definition "would be a significant departure from a plain reading of the ATIS standards and reference documents, and could be disruptive to the use cases that those standards and reference documents clearly contemplate as functioning within the STIR/SHAKEN ecosystem."[226] We believe our proposed definition is consistent with this determination and ATIS's usage, and seek comment on this belief. Regarding "end user," ATIS defines the term as "[t]he entity ultimately consuming the VoIP-based telecommunications service," which may be "the direct customer of [an originating] service provider or may indirectly use the VoIP-based telecommunications service through another entity such as a reseller or value-added service provider."[227] ATIS-1000088, therefore, makes clear that, in some cases, the "customer" and "end user" are not the same.[228] We believe that our proposed definition is consistent with ATIS-1000088. We also believe that our proposed definition of "end user" is consistent with our definition of the term for the purposes of FCC Form 477.[229] We seek comment on our proposed definitions. Should we instead define "end user" with a cross reference to section 1.7001(a)(3) of our rules?

i. Additional Guidance

104. Given the complexity of arrangements related to the provision of voice service, we are cognizant that entities may desire even more certainty regarding their role in providing such service. Although we believe the definitional changes we propose above should resolve supposed ambiguity as to each entity's role in the provision of voice service, and thereby bring clarity regarding each voice service providers' obligations under our rules, we seek comment on whether we should establish a mechanism that would allow for faster resolution of uncertainty, should any remain.[230] This, we believe, would both

[223] ATIS-1000088 at 10.

[224] *Id.* at 5; *see also* ATIS-1000089 at 4 (adding that, "[i]n the context of the SHAKEN attestation model, the Customer is the entity with a direct business relationship and a direct user-to-network interface with the OSP. Enterprises, hosted/cloud service providers, Over the Top (OTT) providers and other service resellers may be considered customers of an OSP depending on the use case").

[225] *Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12907, para. 18 n.85.

[226] *Id.* (citations omitted).

[227] ATIS-1000088 at 5; *see also* ATIS-1000081 at 2 (stating that the terms "end user" and "consumer" are "[u]sed interchangeably to refer to a customer of telecommunications service that is not a carrier or a device, and for whom the service was ultimately created or intended"). The *Eighth Caller ID Authentication Order* also affirmed—but did not codify—this understanding of "end user." *See Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12905, para. 15 n.70.

[228] ATIS-1000088 at 10-11; *see also, e.g.*, *Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12905, para. 15 (describing a complex call path in which "a wholesale provider originates a call onto the public network for its reseller *customer* that initiated the call on behalf of an *end user*" (emphasis added)). According to ATIS-1000088, end users may include individual or enterprise subscribers, enterprise PBXs. *See* ATIS-1000088 at tbl. A-1.

[229] *See* 47 CFR § 1.7001(a)(3) (defining "end user" as "[a] residential, business, institutional, or government entity that subscribes to a service, uses that service for its own purposes, and does not resell that service to other entities").

[230] In the *Eighth Caller ID Authentication Order*, we declined ZipDX's request to provide clarification regarding the operation of our rules, including applicable KYC requirements, in a variety of hypothetical caller ID authentication scenarios, finding that such guidance would be unproductive in the absence of a more focused record. *Eighth Caller*

(continued….)

benefit entities and advance the Commission's goal to ensure that all voice service providers are meeting their obligations. We therefore seek comment on whether we should delegate authority to the Bureau to issue guidance to the extent further definitional clarification is needed, such as in the form of a Frequently Asked Questions document or Public Notice. Should we instead establish a process by which entities may request a non-binding advisory opinion from the Bureau regarding whether they are a voice service provider and if so, which category of voice service provider they are for the services they provide for each type of call they transmit? Are any such mechanisms necessary given the definitional improvements we propose above?

2. Repealing STIR/SHAKEN Implementation Extensions

105. We propose to repeal the two remaining undue hardship extensions to STIR/SHAKEN implementation to further advance ubiquitous deployment of the framework, and seek comment on whether new, narrower extensions may be appropriate. The TRACED Act empowers the Commission to grant classes of voice service providers and types of calls extensions to STIR/SHAKEN implementation on the basis of undue hardship.[231] The Commission has previously assessed whether STIR/SHAKEN implementation would cause "undue hardship" by balancing the "burdens and barriers to implementation" with the benefit to the public of implementing STIR/SHAKEN expeditiously.[232] Pursuant to the TRACED Act's directive, the Commission has granted and maintained two ongoing undue hardship extensions for:[233] (1) voice service providers that cannot obtain the SPC token necessary to participate in STIR/SHAKEN due to the Governance Authority's policy for obtaining a token; and (2) small voice service providers that originate calls via satellite using NANP numbers.[234] If a voice service provider certifies to less than full STIR/SHAKEN implementation as part of its obligation to certify to its

---

ID Authentication Order, 38 FCC Rcd at 12907-08, para. 18 n.85. We seek comment now on whether establishing a procedural mechanism would facilitate such additional guidance in the future.

[231] 47 U.S.C. § 227b(b)(5)(A). Because STIR/SHAKEN only works on IP-based voice networks, the TRACED Act also grants an ongoing implementation extension for the portions of a provider's network that rely on technology that cannot initiate, maintain, carry, process, and terminate SIP calls (i.e., non-IP networks). *See* 47 U.S.C. § 227b(b)(5)(B); *see also* 47 CFR § 64.6304(d); *Second Caller ID Authentication Order*, 36 FCC Rcd at 1884-85, 1892-96, paras. 52-53, 66-70. That extension is not relevant to our discussion here.

[232] *See Fourth Caller ID Authentication Order*, 36 FCC Rcd at 17847-48, 17851, 17857, paras. 16-17, 23, 35 (weighing the reduced burdens of STIR/SHAKEN implementation given "recent marketplace progress to increase the availability of STIR/SHAKEN solutions" against the benefit of shortening the extension for a subset of small voice service providers that pose "an increased risk of originating illegal robocalls"); *Second Caller ID Authentication Order*, 36 FCC Rcd at 1877-82, paras. 40-48 (determining that an extension for small voice service providers was appropriate because of their high implementation costs compared to their revenues, the limited STIR/SHAKEN vendor offerings available to them, the likelihood that costs would decline over time because they could spread their costs over time, and because they serve only a small percentage of total voice subscribers, limiting potential consumer harm of an extension).

[233] In 2020, the Commission granted three categorical implementation extensions based on undue hardship. *See Second Caller ID Authentication Order*, 36 FCC Rcd at 1877-83, paras. 39-51 (granting (1) an extension for small voice service providers with 100,000 or fewer voice subscriber lines until June 30, 2023; (2) a continuing extension for providers unable to obtain the SPC token necessary to participate in STIR/SHAKEN due to the Token Access Policy; and (3) an extension for services scheduled for section 214 discontinuance until June 30, 2022). The Commission thereafter advanced to June 30, 2022, the end date of the extension for a non-facilities-based small voice service providers, which it found were likely to be a source of illegal robocalls, while maintaining June 30, 2023, as the end date of the extension for facilities-based small voice service providers. *See Fourth Caller ID Authentication Order*, 36 FCC Rcd at 17844, para. 9; *see also* 47 CFR § 64.6304(a)(1).

[234] *See* 47 CFR § 64.6304(b), (a)(1)(iii); *Second Caller ID Authentication Order*, 36 FCC Rcd at 1882-83, paras. 49-50; *Gateway Provider Order*, 37 FCC Rcd at 6893, para. 61; *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2614-15, paras. 79-82.

STIR/SHAKEN implementation status in its RMD filing,[235] it "must both explicitly state the rule that exempts it from compliance and explain in detail why that exemption applies."[236] The TRACED Act also directs the Commission to address any issues that formed the basis for any undue hardship extensions it has granted and "enable as promptly as reasonable full participation of all classes of providers of voice service and types of voice calls to receive the highest level of trust."[237] In the absence of undue hardship, there is no basis to maintain an extension. We believe that there is no longer an undue hardship for the two remaining undue hardship extensions, and therefore that the extensions are no longer needed.

106. *SPC token extension.* We believe that all providers that meet the voice service provider definition and have an existing obligation to implement STIR/SHAKEN are able to obtain SPC tokens without undue hardship, and therefore propose to repeal the extension for voice service providers that cannot obtain an SPC token due to the Governance Authority policy.[238] In the March 2023 *Sixth Caller ID Authentication Order*, the Commission sought comment on whether to eliminate this extension based on the Bureau's finding in its December 2022 *Annual Evaluation of STIR/SHAKEN Implementation Extensions* that token access no longer stood "as a significant barrier to full participation in STIR/SHAKEN."[239] In the November 2024 *Eighth Caller ID Authentication Order* that the Commission adopted based on that record, it held off on modifying the extension because the Bureau was still performing a review of submissions in the RMD claiming the extension, the results of which it believed would better inform its decision on the matter.[240] In its December 2025 *Annual Evaluation of STIR/SHAKEN Implementation Extensions*, the Bureau "tentatively [found] that the extension for providers that are incapable of obtaining an SPC token may no longer be necessary" based in part on Bureau staff's initial assessment of RMD submissions.[241] The Bureau nevertheless concluded that the extension remained necessary so that it could complete its evaluation of RMD submissions claiming the

---

[235] 47 CFR § 64.6305(d)(1), (e)(1), (f)(1); *see also Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2595-97, paras. 42, 46.

[236] *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2596-97, para. 45 (footnote omitted); *see also id*. at 2597, para. 45 & n.170 (noting that a voice service provider must state the rule that exempts it from compliance, by, for example, explaining that it lacks the necessary facilities to implement STIR/SHAKEN or it cannot obtain an SPC token); *id*. at 2597, para. 45 & n.171 (noting that to explain why the exemption applies a provider must, for example, explain that it is a pure reseller with some facilities, but that they are not sufficient to implement STIR/SHAKEN, or the steps it has taken to "diligently pursue" obtaining a token); 47 CFR § 64.6305(d)(2)(i) (explaining that voice service providers must identify the type of extension it has and the basis for the extension); 47 CFR § 64.6305(e)(2)(i) (same for gateway providers); 47 CFR § 64.6305(f)(2)(i) (same for non-gateway intermediate providers).

[237] 47 U.S.C. § 227b(b)(5)(D).

[238] 47 CFR § 64.6304(b). Below, we acknowledge that certain VRS providers assert in comments responding to the *Call Branding FNPRM* that they are unable to obtain SPC tokens, in connection with assertions that they do not meet the definition of voice service provider or qualify for the non-facilities-based provider exemption. *See infra* Section III.D.1. We seek comment there on whether we should establish a new undue hardship extension for such providers in the event we find they do have a STIR/SHAKEN implementation obligation.

[239] *See Sixth Caller ID Authentication Report Order and Further Notice*, 38 FCC Rcd at 2623, paras. 107-08; *Wireline Competition Bureau Performs Required Evaluation Pursuant to Section 64.6304(f) of the Commission's Rules*, WC Docket No. 17-97, Public Notice, 37 FCC Rcd 14876, 14882 (WCB 2022). In the *Sixth Caller ID Authentication Further Notice*, the Commission also sought comment on, *inter alia*, whether it should explicitly authorize use of third party caller ID authentication solutions, and if so, whether it should require third parties to sign calls using the provider's SPC token. *Sixth Caller ID Authentication Report Order and Further Notice*, 38 FCC Rcd at 2622, para. 103.

[240] *Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12915-16, para. 29 & n.137.

[241] *Wireline Competition Bureau Performs Required Evaluation of STIR/SHAKEN Implementation Extensions Pursuant to Section 64.6304(f) of the Commission's Rules*, WC Docket No. 17-97, Public Notice, DA 25-1058, at 5 (WCB Dec. 16, 2025).

extension.[242]

107. Bureau staff has now completed that assessment, and we believe repeal of the extension is warranted based on the Bureau's findings. The Bureau identified 338 filings—3.2% of all the filings in the database at the time of review—that affirmatively assert the exemption,[243] but that it does not believe "explain[ed] in detail why the exemption applies," as they are required to do.[244] Specifically, 272 filers asserted, in relation to claiming the SPC token exemption, that they lack control over the network infrastructure necessary to implement STIR/SHAKEN, but that constitutes a separate exemption.[245] For another 57, the Bureau does not believe the justifications supplied are sufficient, such as the steps the provider took to "diligently pursue" obtaining a token.[246] The remaining filings claiming the exemption are TRS providers, which we address separately below and do not believe bear on whether we should repeal this exemption.[247] In the absence of any stated reasons why voice service providers cannot meet the token access policy, we do not believe there is any undue hardship basis for maintaining the SPC token extension. We seek comment on this proposal and our assessment, including whether any voice service provider has attempted to obtain an SPC token and been denied, and the reasons why.

108. *Small providers originating calls via satellite using NANP numbers.* We likewise believe that small voice service providers that originate calls via satellite using NANP numbers are able to implement STIR/SHAKEN without undue hardship, and therefore propose to repeal the extension for such providers.[248] When the Commission established the extension in the *Sixth Caller ID Authentication Order*, it did so on the basis that "the number of satellite subscribers using NANP resources 'is min[u]scule'" and "that there is little evidence that satellite providers or their users are responsible for illegal robocalls," in part because "satellite service costs make the high-volume calling necessary for robocallers uneconomical."[249] Upon further consideration, we do not believe that either of these justifications concern barriers or burdens to STIR/SHAKEN implementation for these small providers. In the absence of such justifications, and in light of the TRACED Act's goal of full implementation, we believe repealing this undue hardship extension is appropriate.[250] We seek comment on this proposal,

[242] *Id.* at 5-6.

[243] The Bureau's calculation does not include filings explaining that the provider is in the process of obtaining an SPC token, filings that merely state the provider does not have an SPC token without claiming that the provider is unable to obtain one, or filings submitted by providers that appear on the STI-PA list of authorized providers.

[244] *See Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2596-97, para. 45.

[245] *See id*. at 2597, para. 45 & n.170 (noting that to state the rule, the provider must, for example, explain that it cannot obtain an SPC token); *id*. at 2597, para. 45 & n.171 (noting that to explain why the exemption applies a provider must, for example, explain the steps it has taken to "diligently pursue" obtaining a token); 47 CFR § 64.6305(d)(2)(i) (explaining that voice service providers must identify the type of extension that applies to them and the basis for the extension); 47 CFR § 64.6305(e)(2)(i) (same for gateway providers); 47 CFR § 64.6305(f)(2)(i) (same for non-gateway intermediate providers).

[246] *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2596-97, para. 45 & n.171. For instance, some providers say they are not required to submit a Form 499—a requirement to obtain an SPC token—but fail to explain why they are not required to if they are a voice service provider that must implement STIR/SHAKEN. Other providers say they cannot obtain an operating company number (OCN) from NECA—another requirement to obtain a token—but do not explain the steps they took to obtain an OCN and whether they were denied and why. *See* NECA, *Company Code Request Instructions*, https://www.neca.org/business-solutions/company-codes/company-code-request-instructions (last visited Apr. 27, 2026). Others still note they are relying on their downstream provider to authenticate calls or lack numbering resources to obtain an SPC token, which are both invalid justifications.

[247] *See infra* Section III.D.1.

[248] 47 CFR § 64.6304(a)(1)(iii).

[249] *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2614-15, para. 81.

[250] We also believe this repeal will have a small impact, as only nine providers have claimed the exemption in the RMD.

including whether there are any actual STIR/SHAKEN implementation barriers or burdens for small providers originating satellite calls using NANP numbers that constitute an undue hardship.

109. *Need for new extensions.* Given the TRACED Act's direction for the Commission to achieve full STIR/SHAKEN deployment and that many of the measures herein are geared toward that outcome, we do not believe that new undue hardship extensions are appropriate. We also do not believe that the proposed definitional clarifications above would impose an implementation obligation on any classes of providers that were not already required to implement STIR/SHAKEN. Nevertheless, we seek comment on whether our proposed clarifications do make any entities newly aware of their implementation obligation and whether there are barriers or burdens to implementation of STIR/SHAKEN that would pose an undue hardship.

3. Requiring Providers Serving End Users Directly to Assign Attestations

110. To make STIR/SHAKEN a more valuable resource for caller ID information,[251] and thereby reduce the vectors for bad actors to put spoofed calls on the voice network, we propose to require all voice service providers that serve end users directly to make attestation-level decisions for their end users' SIP calls.[252] We further propose to require originating providers to authenticate such calls (whether themselves or through a third-party) using the attestation-level decisions of the provider serving end users directly. This proposal would not change the obligations for originating providers when they serve end users directly; they will continue to be required to authenticate such calls using their own attestation-level decisions. This proposal would, however, add an obligation for initiating providers—i.e., non-facilities-based voice service providers that serve end users directly[253]—by requiring them to make attestation-level decisions regarding their end users' SIP calls and for originating providers that perform the origination of such calls by requiring them to authenticate the calls with the attestation level selected by the initiating provider. We believe that if we adopt this proposal, every voice service provider that has a relationship with a call that is originated in IP will be participating in the STIR/SHAKEN ecosystem. We also believe this proposal will close the knowledge gap that exists when the originating provider does not have a direct relationship with the end user because the end user obtained voice service from an intermediary provider, such as a reseller (i.e., a non-facilities-based provider).[254] We seek comment on this proposal and analysis. If we adopt this proposal, are there any voice service providers that would remain not subject to a STIR/SHAKEN-related obligation related to SIP calls? If so, which providers? Are there any providers we should exempt from the attestation obligation, and if so, why?

111. *Mechanism for implementation.* We seek comment on whether we should designate one or more mechanisms to ensure that originating providers apply initiating providers' attestation-level decisions when authenticating calls, and if so, which mechanism(s) we should designate. Should we

[251] *See* TransNexus Triennial Report Comments at 8 ("STIR/SHAKEN is more effective when the voice service provider closest to the caller authenticates the calls it originates, for two reasons: (1) they know the caller and the called number and can provide more useful authentication information, and (2) when the voice service provider closest to the caller authenticates the call, they identify themselves with non-repudiation.").

[252] Under existing conditions, the originating provider, as the facilities-based provider, is supposed to authenticate calls initiated by the non-facilities-based-provider using the originating provider's certificate with an attestation based on its knowledge of the non-facilities-based provider. *See Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12905-07, para. 17.

[253] *See supra* Section III.C.1.b. (proposing to define "initiation" and "initiating provider").

[254] This is the knowledge gap described as Scenario 2 above. *See supra* Section III.B; s*ee also* Convo Call Branding Comments at 3 (arguing that mandating acceptance of delegate certificates "would lead to more accurate attestation levels for a variety of types of calls in which the voice services provider may not know the end-user caller"); Somos Call Branding Comments at 15 (arguing that delegate certificates are a reasonable measure to address verification challenges that arise when the authenticating provider does not have a direct end-user relationship); WISPA Call Branding Comments at 3 (supporting use of delegate certificates to address the "knowledge gap" between authenticating providers and resellers).

permit or require the use of delegate certificates, which we propose to find are valid mechanisms for this purpose?[255] Should we instead require initiating providers to obtain an SPC token, use that token to obtain certificates, make all STIR/SHAKEN attestation-level decisions regarding calls initiated by their end users, and ensure originating providers sign calls with the initiating provider's certificate and attestation-level decision, similar to our third-party authentication rule?[256] To our knowledge, there are no barriers or burdens to non-facilities-based providers obtaining an SPC token under the existing Governance Authority policy,[257] and we believe requiring this would have the benefit of subjecting resellers to the same vetting that originating providers must undergo to obtain an SPC token. Is that accurate? If not, what are the barriers and burdens, and do they warrant extending the compliance deadline to account for them? Should we require the Governance Authority to change its policy? How would our proposed approach work when there are multiple levels of resale, given that the initiating provider may not have a direct relationship with the originating provider? We also seek comment on whether we should require the use of specific mechanisms in different circumstances and the reasons for doing so. Additionally, we seek comment on the feasibility for initiating providers to implement any mechanisms.

112. *Impact on other providers.* We seek comment on any other impacts our proposal may have on voice service providers that bear a connection to a call. What obligations, if any, should we attach to non-facilities-based providers when they are not serving end users directly, such as when they are a reseller in a multi-level resale chain, aside from any existing and proposed requirements? Should they be held responsible if the initiating provider does not assign attestations to calls or applies an improper attestation? Likewise, should a TNSP that assigns numbers to a non-facilities-based provider be

---

[255] *See supra* Section III.B.2.

[256] *See* 47 CFR § 64.6301(b); *see also* ATIS-1000089 at 13 (describing enterprise certificates). While the Commission adopted a rule in the *Eighth Caller ID Authentication Order* permitting voice service providers with a STIR/SHAKEN implementation obligation to engage a third party to perform on their behalf the technological act of signing the calls they originate, it declined to consider those providers that lack control over the network infrastructure necessary to implement STIR/SHAKEN as "originating service providers" and thus "first parties" for the purposes of third-party authentication. *See Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12903-04, 12908, paras. 14, 19 & n.88. It concluded that such a definition would conflict with the text of the Commission's rules establishing the scope of providers subject to the STIR/SHAKEN implementation obligation and would be inconsistent with how the ATIS standards and technical reports use that term. *Id.* at 12908, para. 19 & n.88. The Commission did, however, acknowledge that some resellers voluntarily attempt to authenticate caller ID information despite not having control over the network infrastructure necessary to implement STIR/SHAKEN (and, thus, lacking a STIR/SHAKEN implementation obligation) by relying on their wholesale providers to sign their calls. *Id.* The Commission therefore encouraged, but did not require, such resellers to provide their wholesalers with enough information to enable the wholesalers to determine the appropriate attestation level of the calls initiated by the resellers' end users, pursuant to the wholesalers' obligations as originating providers under the Commission's rules and the STIR/SHAKEN standards. *Id.*; *see also* ATIS-1000088 at 13 ("In those cases [in which a service provider's (SP) customer is a reseller,] the SP's customer should provide assurances that they can trace the identity of an indirect end user and that user's authorization to utilize a calling TN. The customer should be able to certify that only the authorized party (or calls originated on their behalf) will use the particular set of authorized TNs, and any traceback to the ultimate source will rely on the cooperation of the SP's customer."); ATIS-1000074 at 12 n.1 (describing various mechanisms by which an originating service provider may assert that its customer can legitimately use the telephone number that appears as the calling party).

[257] Consistently, ZipDX asserts that resellers that lack control of the infrastructure necessary to implement STIR/SHAKEN would be able to obtain an SPC token of their own should we require them to do so. *See* ZipDX LLC Comments at 3 (rec. June 5, 2023) ("If, for example, a reseller [without the control over the infrastructure necessary to implement STIR/SHAKEN] wants to hold itself out as the originating service provider (even though it does not actually 'touch' the call), then it needs to . . . get its own SHAKEN token, and arrange for somebody (the infamous third party) to sign the calls with that token."). *But see* INCOMPAS Reply at 6 (rec. July 5, 2023) (arguing that, because "many providers do not operate a business model that allows them to get an OCN from the Commission," they may have a challenge obtaining an SPC token from the Governance Authority).

held responsible when the non-facilities-based provider further assigns those numbers to an initiating provider that fails to properly follow the attestation requirements? Should an originating provider that is not the TNSP also be held responsible for mis-attested calls? Would these various threads of liability be connected through tracebacks and the KYUP proposals above? If an originating provider uses a third-party to perform the technical act of signing a call that must be authenticated with the attestation level selected by an initiating provider, what obligations should the initiating provider have in that signing arrangement, if any? What impact, if any, will our proposal have on the ability for terminating providers to verify calls if they are attested to by an initiating provider and/or authenticated with an initiating provider's certificate? What will be the impact on industry traceback efforts?

113. *Issues related to use of initiating provider attestations.* Regardless of the mechanism(s) we choose, we seek comment on feasibility and other issues that may arise with requiring originating providers to use the attestation level designated by the initiating provider. We note that under ATIS-1000074, a voice service provider may only apply an A- or B-level attestation when it is responsible for originating the call onto the IP network.[258] Would it be permissible under the ATIS standards for initiating providers to apply an A- or B-level attestation? Should we modify the attestation criteria to make it permissible? We also note that the ATIS standards contemplate that the originating provider will always remain the ultimate authority in assigning attestation levels.[259] Is it permissible under the standard for the originating provider to apply the attestation selected by the initiating provider, and if not, should we adopt a rule making it permissible? Does requiring the originating provider to apply the attestation level selected by the initiating provider raise concerns regarding the validity of the attestation decision? For instance, under the mechanism where the initiating provider obtains its own SPC token and certificates from the Governance Authority, the originating provider could be required to authenticate a call with an A-level attestation designated by the initiating provider when the originating provider has no knowledge regarding whether there is a legitimate association between the end user and the number being used. Is this a valid concern? Should we maintain the requirement for originating providers to make the ultimate attestation decision based on their own determinations of the attestation criteria? If so, would it still be worthwhile to require that initiating providers obtain their own SPC token and certificates and therefore undergo the vetting and oversight associated with the Governance Authority's token access and token revocation policies?

4. Ensuring Calls Are Authenticated

114. To further support our effort to ensure ubiquitous STIR/SHAKEN implementation and increase the number of calls that terminate with attestation information, we propose to: (1) prohibit voice service providers from intentionally routing calls to strip authentication information; (2) require that providers block unauthenticated SIP calls transmitted directly to them (except public safety calls); and (3) require that all intermediate providers authenticate any unauthenticated non-SIP calls they receive. We believe these requirements, in combination with the KYUP requirements we propose above, will serve to

---

[258] ATIS-1000074 at 12; *see Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12912, para. 24 (noting that all calls with an A- or B-level attestation "will need to be signed using the originating service provider's certificate"). *Compare* ATIS-1000089 (defining "Originating Service Provider" as "the service provider that handles the outgoing calls from a customer at the point at which they are entering the public network. The OSP performs the SHAKEN Authentication function"), *with* ATIS-1000088 at 19 (stating that resellers and VASPs may "originate" their end users' calls "through multiple [originating] service providers"), *and* ATIS-1000074 § 4 at 6 ("[I]f the originating service provider has an authenticated direct relationship with the *originator* of the call, this attestation is categorized differently than for calls that are originated from different networks or gateways that the service provider may have received from an unauthenticated network, or that are unsigned." (emphasis added)).

[259] *See, e.g.*, ATIS-1000074 at 12 ("The 'attest' claim allows the originating service provider that is populating an Identity header to clearly indicate the information it can vouch for regarding the origination of the call."); *see also* ATIS-1000088 at 8 (describing the "attestation indicator" as "encod[ing] the extent to which the originating SP has itself identified and authenticated its customer and determined the customer's 'association' to the calling party telephone number).

remove bad actor providers from the voice network, as well as reduce the incentives for providers to maintain non-IP networks, thereby further supporting the IP transition. We discuss each proposal in turn, as well as seek comment on other authentication-related issues.

115. *Prohibiting elective non-IP call routing.* We propose to prohibit voice service providers from intentionally routing a call over a network that does not support the transmission of STIR/SHAKEN authentication information when it has the technical ability to route a call over a network that does support such transmission. In the *Second Caller ID Authentication Order*, the Commission declined to adopt one commenter's proposal to prohibit intermediate providers from passing a SIP call to a downstream provider in TDM when there is a downstream IP option available.[260] As the Commission explained at the time, it did not wish to interfere with call routing decisions when the voice industry was in the early stages of STIR/SHAKEN deployment.[261] In the six years since that order was adopted, STIR/SHAKEN has been widely deployed throughout the voice ecosystem, and yet the benefits of STIR/SHAKEN have been frustrated by the persistence of call routing over TDM networks—indeed, current data suggest the problem may be worsening. According to statistics provided by TransNexus, the percentage of calls terminating in the United States that are signed with STIR/SHAKEN dropped from 49% in October 2024 to 38% in September 2025.[262] TransNexus attributes this downward trend, at least in part, to the routing of calls over non-IP segments along the call path.[263] TransNexus argues that, if providers are choosing to route their calls over non-IP segments, this tactic would "enable such providers to claim compliance with the Commission's call authentication rules while remaining unaccountable for their calls within the STIR/SHAKEN ecosystem."[264] ACA International et al. also contend that "scam calls are deliberately routed through TDM interconnections for the purpose of stripping out STIR/SHAKEN information to reduce the chances that the calls will be blocked."[265]

116. We seek comment on this proposal. How easily can providers intentionally route calls over networks that do not support the transmission of authentication information? To what extent can they ensure that calls are routed over networks that support transmission of authentication information when available? What impact would such a prohibition have on providers' least-cost routing practices (where call routing is based on the lowest cost rather than on signaling protocol)? We believe that the benefits of preserving STIR/SHAKEN authentication information with a call outweigh any additional cost of selecting an IP route for the call, and we note that, in 2018, the NANC recommended that "all carriers that route calls between originating and terminating carriers, such as long-distance providers and least-cost routers, maintain the integrity of the required SHAKEN/STIR signaling."[266] We seek comment on these views. What percentage of calls are routed over networks that cannot support the transmission of authentication information due to least cost routing? Are there existing least cost routing arrangements that may prevent providers from routing calls over networks that support the transmission of authentication information? Do commenters support the inclusion of intent in this rule, or should we instead adopt a strict liability regime? What evidentiary findings would establish intent? By what metric should we consider that a provider has the technical ability to route a call over IP? Would such a rule risk incentivizing bad actor providers to cease interconnecting in IP altogether so that the only "available option" for routing a call is over a TDM interconnection point? If so, how could we deter this? Would downstream providers be able to determine when a bad actor is seeking to interconnect in TDM specifically to circumvent this rule, such as by using the KYUP measures we propose above? Should we

---

[260] *Second Caller ID Authentication Order*, 36 FCC Rcd at 1925, para. 139.

[261] *Id.*

[262] *See* TransNexus Comments at 4 (rec. Oct. 3, 2025).

[263] *See id.*

[264] *Id.*

[265] ACA International et al. Comments at 6-7.

[266] 2018 NANC CATA Working Group Report at 17.

place more direct obligations on downstream providers to ensure that the upstream providers with which they interconnect are not engaged in prohibited routing practices? If so, what obligations should we adopt? Rather than adopting this prohibition, should we instead require the use of a non-IP caller ID authentication mechanism, as explored in the *Non-IP Caller ID Authentication NPRM*?[267]

117. *Blocking unauthenticated SIP calls.* We propose to require that non-gateway intermediate providers and terminating providers block SIP calls that use NANP resources in the caller ID field transmitted directly to them without STIR/SHAKEN authentication information, except 911, 988, and other public safety calls.[268] We believe that some providers may not be fulfilling their obligation to authenticate SIP calls, potentially to obscure the identity of the originating provider and/or the caller. For instance, ZipDX notes that in "approximately 65% of tracebacks, the originating provider is identified as having signed the call," suggesting that the remaining 35% were unsigned.[269] All voice service providers are required to have implemented STIR/SHAKEN in their IP networks, and if we adopt our proposal below that intermediate providers authenticate any unauthenticated calls they receive (namely, those received from non-IP networks), no providers should receive an unauthenticated SIP call unless the upstream provider is violating our rules, subject to a certain narrow technical and security exemption that we address herein. We believe that unauthenticated SIP calls are presumptively unlawful, and therefore that blocking is warranted.[270] We seek comment on this view and additional evidence on the extent to which providers are not authenticating SIP calls they are transmitting. Apart from the circumstances that permit an intermediate provider to remove authentication information under our rules, are there any other legitimate reasons a lawful call on an IP network would not have authentication information? What is the scope of legitimate calls that may be blocked under this rule? Are there any technical limitations to identifying whether a call was transmitted in IP or blocking them when they are not authenticated? Would such a rule risk incentivizing bad actor providers to cease interconnecting in IP altogether so that they only transmit calls in non-IP? If so, how could we deter this? Is our proposal above to prohibit intentional non-IP call routing a necessary counterpart to this proposal in addressing this incentive issue? Should we instead require any provider that accepts an unsigned call to add to the call's identity header information about the voice service provider from which it received the call, such as the voice service provider's OCN, along with an indication of whether the call was received in TDM or IP?[271] Is there a legal and policy basis for requiring non-gateway intermediate providers and terminating providers to block unauthenticated SIP calls that do not use NANP resources in the caller ID field?

118. To facilitate this proposed blocking rule, we propose to modify our rule that allows intermediate providers to remove caller ID authentication information in certain circumstances to require that they reauthenticate any such calls if they will be transmitting the call to another provider in IP. Under our current rules, intermediate providers may strip such information: (1) where necessary for technical reasons to complete the call; and (2) where the intermediate provider reasonably believes the

[267] *See generally Call Authentication Trust Anchor*, WC Docket No. 17-97, Notice of Proposed Rulemaking, FCC 25-25 (Apr. 28, 2025) (*Non-IP Caller ID Authentication NPRM*); *see* TransNexus Comments at 4-5.

[268] For clarity, we are not proposing that providers block calls transmitted to them from a non-IP network, such as TDM. We also limit the proposed requirement to non-gateway intermediate providers because gateway providers may receive unauthenticated SIP calls from foreign voice service providers and we do not propose that such calls should be blocked.

[269] ZipDX Feb. 17, 2026 Non-IP Authentication *Ex Parte* Letter, Attach. at 6.

[270] *See, e.g.*, Somos Call Branding Comments at 27-28 ("Calls that present a U.S. telephone number without any verifiable RTU credentials, i.e., no signature from a trusted U.S. provider, Resp Org, or delegate, should increasingly be considered unauthorized spoofing for purposes of call authentication and trust enforcement, and should be prohibited.").

[271] Letter from David Frankel, CEO, ZipDX, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 17-97, at 2 (filed Apr. 14, 2025) (ZipDX Apr. 14, 2025 Non-IP Authentication *Ex Parte* Letter).

caller ID authentication information presents an imminent threat to its network security.[272] By requiring them to reauthenticate the call, it will ensure that all SIP calls arrive at the terminating provider with authentication information. It will also prevent the calls from being blocked by the next downstream provider in the call path under our proposed blocking rule. Is such reauthentication technically feasible? We also seek comment on whether the two exceptions remain necessary. Are there actual instances where they remain necessary?[273]

119. *Requiring non-gateway intermediate providers to authenticate non-SIP calls.* We propose to require that all non-gateway intermediate providers authenticate non-SIP calls using NANP resources in the caller ID field that they receive and will exchange with another provider as a SIP call.[274] While we propose above to require that non-gateway intermediate providers block any unauthenticated SIP calls using NANP resources in the caller ID field that they receive, they will still receive unauthenticated non-SIP calls, such as those sent from TDM networks. Under our current rules, the first intermediate provider in the call path must authenticate any unauthenticated calls they receive directly from an originating provider.[275] We propose to modify that rule to place the authentication requirement on all intermediate providers and by narrowing it to non-SIP calls that they will not be blocking based on the proposed rule above. While the existing rule only requires authentication by the first intermediate provider, if the call transits another TDM network later in the call path, the authentication information would be stripped. We believe that requiring all non-gateway intermediate providers to authenticate any unauthenticated IP calls they receive will increase the number of calls that arrive at terminating providers with authentication information. Although authentication by intermediate providers will necessarily carry a C-level attestation (because the provider is not originating the call), we believe having the non-gateway provider intermediate attestations may help efforts to identify non-IP gaps in the voice network.[276]

120. We seek comment on this proposal and analysis. What is the prevalence of unauthenticated calls transiting intermediate providers' networks due to non-IP networks? How often does an intermediate provider's authentication get stripped out by a later non-IP segment and then get passed to another intermediate provider? Will the intermediate provider attestations benefit call analytics and/or traceback efforts? Is there a legal and policy basis for requiring non-gateway intermediate

[272] *Id.* § 64.6302(b)(1)-(2).

[273] *See, e.g.*, Somos Call Branding Comments at 34-35 ("While the Commission appropriately included 'technically feasible' language during earlier stages of deployment, the continued presence of such language risks being interpreted as a permissive exception rather than a transitional accommodation.").

[274] As permitted by the Commission's third-party authentication rules, an intermediate provider could satisfy this proposed requirement through third-party authentication. *See* 47 CFR § 64.6302(f). We do not propose to apply this rule to gateway providers as they are already required to authenticate any unauthenticated calls they receive using U.S. NANP resources that they will exchange with another provider as a SIP call. 47 CFR § 64.6302.

[275] 47 CFR § 64.6302(e). Our rules technically require all intermediate providers to authenticate any unauthenticated caller ID information for the SIP calls they receive or, alternatively, cooperate with the industry traceback consortium and timely and fully respond to all traceback requests received from the Commission, law enforcement, and the industry traceback consortium. *See* 47 CFR § 64.6302(c); *Second Caller ID Authentication Order*, 36 FCC Rcd at 1926, para. 140. But in the *Fourth Call Blocking Order*, the Commission required all providers in the path of a SIP call to respond fully and in a timely manner to traceback requests, so intermediate providers could automatically decline to authenticate caller ID information. *See Fourth Call Blocking Order*, 35 FCC Rcd at 15227-29, paras. 15-21; 47 CFR § 64.1200(n)(1); *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2581, para. 15. In the *Sixth Caller ID Authentication Order*, the Commission established the requirement that the first intermediate provider in the path of an unauthenticated SIP call authenticate the call. *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2581, para. 15; 47 CFR § 64.6302(e).

[276] *See Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2582, para. 17 n.73 ("While we generally agree that higher-level attestations are more advantageous than C-level attestations, as we stated in the *Gateway Provider Order*, where a call is unauthenticated, a C-level attestation is better than no attestation and has value." (citing *Gateway Provider Order*, 37 FCC Rcd 6865 at 6889-91, para. 57)).

providers to authenticate non-SIP calls that do not use NANP resources in the caller ID field? We acknowledge that adoption of this proposal would depart from the Commission's decision in the *Sixth Caller ID Authentication Order* to not extend the authentication requirement to all intermediate providers due to progress toward non-IP authentication solutions and the transition to IP interconnection and because of the burdens on intermediate providers.[277] We now suspect that the burden on intermediate providers may be limited because many likely already have the capability to authenticate calls given that they could be the first one in the call path to receive an unauthenticated call. We also now believe that requiring authentication by intermediate providers will be beneficial while the IP transition is completed or providers adopt non-IP caller ID authentication solutions, and we note that the Commission resolved in the *Sixth Caller ID Authentication Order* to consider expanding a caller ID authentication requirement to all intermediate providers in the future, should such a step be warranted.[278] Are these views accurate?

121. *Other Authentication Issues*. We seek comment on whether to require a voice service provider to populate the origination identifier ("origid") field in a call's identity header with the provider's OCN, FRN, RMD number, or other standardized identifier to assist providers with identifying upstream providers generating unlawful calls or with traceback efforts.[279] ATIS-1000088 recommends that the origid value "be a persistent and/or permanently assigned value at the selected source granularity."[280] If we require standardized use of the origid field, what level of granularity should we require?[281] Would standardization of this field foreclose innovative uses? Could the Commission obligate downstream intermediate providers to cease accepting calls signed with a certain origid once it is discovered that a bad actor provider associated with that origid is the source of illegal robocalls?

122. We also seek comment on whether we should take steps to address "instances where forwarded calls are sent without the proper SIP headers," leading to improper call blocking and labeling by analytics systems.[282] How prevalent is this issue and what, if anything, should the Commission do to resolve it?

---

[277] *Id.* at 2582-85, paras. 17-20. The Commission has a pending proceeding proposing to require that providers adopt non-IP caller ID authentication solutions, *see Non-IP Caller ID Authentication Notice of Proposed Rulemaking*, 40 FCC Rcd 3467, and has also been undertaking numerous efforts to promote providers completing their transition to all-IP. *See, e.g.*, *Reducing Barriers to Network Improvements and Service Changes*; *Accelerating Network Modernization*, WC Docket Nos. 25-209 and 25-208, Report and Order, FCC 26-19 (Mar. 27, 2026); *Advancing IP Interconnection*; *Accelerating Network Modernization*; *Call Authentication Trust Anchor*, WC Docket Nos. 25-304, 25-208, and 17-97, Notice of Proposed Rulemaking, 40 FCC Rcd 8566 (2025).

[278] *See Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2583, para. 17.

[279] ATIS-1000088 describes the purpose of the origid as permitting providers to "assign an opaque identifier corresponding to all or part of the originating service provider's network . . . , customers, customer or interconnecting service provider nodes, classes of customer devices, or other groupings that a service provider might want to use to indicate common call sources for determining things such as reputation or trace back identification of customers or gateways." ATIS-1000088 at 14. In the *Call Branding FNPRM*, we sought comment on whether we should "require that providers use a specific origid to indicate a call is foreign originated." *Call Branding FNPRM* at 21, para. 70. The idea received a mixed response. *Compare, e.g.*, CTIA Call Branding Reply at 20 (rec. Feb. 20, 2026) (discouraging the Commission from mandating use of the origid field to label foreign-originated calls and citing ATIS Call Branding Comments at 5 and Verizon Call Branding Comments at 8, *with* ZipDX Apr. 14, 2025 Non-IP Authentication *Ex Parte* Letter at 2 (expressing support for "require[ing] any provider that accepts an unsigned call to indicate, as part of the OrigID field already present in the STIR/SHAKEN data, the four-character OCN of the sourcing provider along with an indication of whether the call was received via TDM or SIP").

[280] ATIS-1000088 § 6.2 at 15.

[281] *See* INCOMPAS Sixth Caller ID Authentication FNPRM Comments at 8-9 (June 5, 2023) (arguing that "[w]ider and more standardized use of 'Orig ID' in the IP header holds considerable promise for advancing STIR/SHAKEN and should be encouraged by the Commission").

[282] *See* T-Mobile Triennial Report Comments at 6.

D. Special Circumstances

1. STIR/SHAKEN for TRS Providers

123. We seek comment on how our STIR/SHAKEN requirements apply to TRS providers in light of the changes we propose above, and what the impact of those requirements are on such providers. Specifically, we seek to understand how the requirements apply to TRS providers, who do not have registered users, but receive calls to relay centers through consumers dialing 711 or a toll-free number;[283] how the requirements apply to Video Relay Service (VRS) and Internet Protocol Relay Service (IP Relay) providers that are required to assign telephone numbers to their registered users;[284] and how the requirements apply to Internet Protocol Captioned Telephone Service (IP CTS) providers that may assign telephone numbers if they are also providing voice services to their registered users.[285] Commenters representing these stakeholders responding to the *Call Branding FNPRM* and the *Triennial Report Public Notice* have indicated that downstream providers have begun treating them as voice service providers with a STIR/SHAKEN implementation obligation, and are treating, or have threatened to treat, their calls as unsigned and lower their attestation levels if these providers do not implement STIR/SHAKEN.[286] These practices by downstream providers, they say, disproportionally harm individuals with disabilities, whose calls would be viewed as untrustworthy by terminating providers and their customers.[287]

124. Stakeholders for the various types of TRS variously assert that TRS providers are not voice service providers and that even if they were, they would be subject to the non-facilities-based

[283] The two providers of TTY-based relay services, Speech-to-Speech relay services, and Captioned Telephone Services have agreements with state TRS programs to provide these services. The state TRS programs are each overseen by, or a part of, a state agency and each is certified with the Commission. 47 CFR §§ 64.604(c)(5)(iii)(F); 64.606(b)(1).

[284] VRS and IP Relay providers must be certified by the Commission to receive compensation for relay services. 47 CFR §§ 64.604(c)(5)(iii)(F)(*2*); 64.606(b)(2). An individual must register with and provide a certification of eligibility to a provider in order to use relay services under the TRS program. 47 CFR § 64.611(a). VRS users have a separate obligation for the verification of their identity and address in the TRS User Registration Database. 47 CFR § 64.611(a)(4).

[285] IP CTS providers must also be certified by the Commission to receive compensation for relay services. 47 CFR §§ 64.604(c)(5)(iii)(F)(2); 64.606(b)(2). An individual must register with and provide a certification of eligibility to a provider in order to use relay services under the TRS program. 47 CFR § 64.611(j)(1). An IP CTS user will also go through the identity and address verification process in the TRS User Registration Database, once the database is ready. 47 CFR § 64.611(j)(2).

[286] *See, e.g.*, Convo Call Branding Comments at 10-11 ("Convo's Voice Provider has informed Convo that it intends to provide a C-level caller ID attestation to Convo's user's calls, and Convo currently has no commercially feasible means of remediating this issue."); *see also* Hamilton Relay Call Branding Comments at 4 ("For PSTN-based TRS, the relay provider sits in the middle of the call—relaying the call. From a technical perspective, the inbound call is made to the relay center. But the outbound dial is a separate segment of the call. Hamilton relies on underlying voice service providers to make the outbound dial. . . . It has also been Hamilton's experience that attestation levels on its outbound calls are unevenly applied by different voice service providers due to inconsistent interpretations of how STIR/SHAKEN rules apply to a relay call.").

[287] *See, e.g.*, Sorenson Communications Call Branding Comments at 1-2.

provider exemption, cannot obtain SPC tokens,[288] or should receive A-level attestations by default.[289] We seek clarity on whether providers for each type of TRS are or are not voice service providers. Do our proposed revised definitions above resolve this question for each type of TRS provider? If any TRS providers are voice service providers, do they qualify for the non-facilities-based provider exemption we clarify above? If so, should we require them to attest their calls using delegate certificates or any other mechanism we choose, as we propose to do for other non-facilities-based providers? If they do not qualify for the exemption or we require an attestation mechanism that involves obtaining an SPC token, are all TRS providers able to obtain SPC tokens from the Governance Authority?[290] If not, should we establish an undue hardship extension for these providers? Or, should we require that the Governance Authority modify its policy so that they are able to obtain SPC tokens? Are there any issues for these providers related to the costs of implementing STIR/SHAKEN? Should we simply mandate that calls from TRS providers be given an A-level attestation to ensure that calls from individuals with disabilities are treated as trustworthy?[291] What are the practical and technical challenges, if any, with implementing such a requirement? Would such a requirement create a loophole that bad actors could easily exploit? What, if any, of these issues would be resolved by the IP transition, and should we simply continue our efforts to spur the transition?

2. Addressing Foreign Calls With KYUP and STIR/SHAKEN Authentication

125. We seek comment on how our proposals would serve to deter illegal calls that enter the United States from abroad, and whether we should take any further actions related to KYUP and caller ID

---

[288] We note that staff's review of RMD filings identified several providers of TRS, VRS, and IP CTS that claim the SPC token exception, asserting that they are not "telecommunications carriers" or a "provider of private telecommunications," that they are not required to have an FCC Form 499-A on file with the FCC, or that they have not been assigned an OCN. However, all of these providers also indicate that they lack control over the network infrastructure necessary to implement STIR/SHAKEN or rely on technology that cannot initiate, maintain, carry, process, and terminate SIP calls (i.e., non-IP networks). *See* Hamilton Relay, Inc. (RMD0018543); Sorenson Communications, LLC (RMD0004562); Convo Communications LLC (RMD0007603); ZP Better Together, LLC (RMD0008054); Mezmo Corporation (dba InnoCaption) (RMD0006693); ClearCaptions, LLC (RMD0007619); ClearCaptions, LLC (RMD0007619); Captel, Inc. (RMD0009123). One additional VRS provider filed in the RMD but did not affirmatively claim the SPC token extension. *See* Tive (RMD0012132).

[289] *See* Convo Call Branding Comments at 9 ("[As a VRS provider, Convo] is not eligible to obtain, and does not hold, an SPC token. Moreover, because Convo is not a voice service provider and is ineligible to hold an SPC token, Convo does not have STIR/SHAKEN obligations."); Sorenson Communications Call Branding Comments at 1-2 ("Unlike telecommunications carriers, TRS providers are either a provider of telecommunications transmission services or an information service provider, and thus, under current procedures, cannot directly obtain an SPC token that would permit them directly to certify calls."); Hamilton Relay Call Branding Comments at 2, n.3 (citing 47 U.S.C. § 225(a)(3) to assert that TRS is a telephone transmission service that is functionally equivalent to, but is not, a voice service for the purpose of facilitating the communications of individuals with hearing and/or speech disabilities); *id.* at 5-6 (noting that it is unable to obtain an SPC token because "it does not provide telecommunications, collects no revenue from end users, and is compensated instead from the interstate TRS Fund as an eligible TRS provider, [] is not required to have a Form 499-A on file with the FCC[, and] . . . as a relay provider without billing or interconnection relationships, [] is not eligible to obtain an OCN").

[290] Convo Call Branding Comments at 13-14 (suggesting the Commission could coordinate with the Governance Authority "to recognize a new eligibility category for certificated TRS providers, including certificated VRS providers, by "permit[ting] all TRS providers to qualify to hold SPC tokens based on their TRS certificates" "in lieu of requiring a provider to hold an OCN to qualify to obtain an SPC token," given that "TRS providers are extensively vetted, audited, and heavily regulated, and there are only a very small number of certificated providers").

[291] *See* Sorenson Communications Call Branding Comments at 9-10 (suggesting that the Commission require "any telecommunications carrier or interconnected voice provider that provides a VRS or IP CTS provider with the ability to originate calls, and any holder of a delegate certificate, STI Subordinate Certificate Authority, or STI Certificate Authority [to] provide an A-level attestation for traffic originated from an FCC-certified VRS or IP CTS provider").

authentication in that regard.

126. We believe the KYUP obligations we propose above will provide two mechanisms to identify foreign bad actor providers and foreign-originated calls. First, we believe that KYUP obligations will require gateway providers to scrutinize the foreign voice service providers from which they accept traffic and require that they refuse or discontinue service to foreign voice service providers who are transmitting illegal calls. Second, we believe the KYUP obligations will require all voice service providers to scrutinize upstream providers that claim to be domestic providers to determine whether that is in fact the case. In particular, we believe the KYUP obligations will allow providers to identify foreign voice service providers that have attempted to establish nominal operations within the United States to avoid their calls being scrutinized as foreign-originated.[292] Should we impose more specific obligations on providers to identify bad actor foreign providers or illegal foreign calls and stop them? Are there any KYUP obligations we propose above that we should not require providers to perform for foreign providers? Should we require gateway providers to adopt strict contract provisions with foreign providers that require the foreign providers to use meaningful KYUP and KYC requirements?

127. We also seek comment on how our proposals will advance or hamper ongoing efforts to achieve Cross Border Call Authentication (CBCA), and whether we should do more to support that effort. CBCA is an initiative that would purportedly "allow calls to be verified end-to-end in an all-IP traffic exchange environment, even if they originate in a country that has not yet deployed [STIR/]SHAKEN."[293] Would any of our proposals above hamper implementation of CBCA? Even if any would, given the broad array of stakeholders that have raised concerns about how STIR/SHAKEN is implemented in the United States, would that be outweighed by the benefits of enhancing STIR/SHAKEN implementation in the United States? Would maintaining the current standards to facilitate CBCA implementation serve to increase the risk that illegal calls will enter the United States from abroad, thereby exacerbating the problems that presently exist? Does the CBCA standard provide robust guardrails to prevent bad actors from using the mechanism to target U.S. consumers with foreign-originated illegal calls that will be authenticated as legal? What obligations will be placed on domestic providers to prevent misuse by foreign-based providers? Will the Commission and other U.S. enforcement entities have sufficient jurisdiction to address improper application of CBCA if it is implemented? Should we adopt rules applicable to domestic providers to facilitate CBCA while also protecting consumers from foreign-originated illegal calls? If so, what should those rules be?[294] Will CBCA facilitate the use of tracebacks to identify foreign intermediate providers at each point in a call path and the foreign originating providers

[292] Industry Traceback Group *Ex Parte*, Attach, at 10 (noting that some entities appearing in tracebacks claim to be U.S.-based but appear to be located overseas); ABA et al. Call Branding Comments at 29 ("Data obtained by ABA's consultant shows that most illegal calls originate inside the United States because illegal callers typically have established U.S.-based originating telecommunications companies to initiate the calls. Once the call is connected, the bad actor uses Voice Over Internet Protocol (VOIP) to initiate a secondary call to connect the first call to the overseas center where the scammer speaking on the phone is located."); NCLC Call Branding Reply at 6 (noting that "some domestically originated calls will feature foreign calling parties either because a foreign participant is connected after an otherwise domestic call is answered or because a nominally domestic provider is in fact operating as a foreign proxy").

[293] ATIS Call Branding Comments at 2; *see also* ATIS, Mechanism for Initial Cross-Border Signature-based Handling of Asserted Information Using toKENs (SHAKEN), ATIS-1000087 (Dec. 16, 2019), https://www.sipforum.org/download/mechanism-for-initial-cross-border-signature-based-handling-of-asserted-information-using-tokens-shaken-atis-1000087/?wpdmdl=3943&refresh=69d4cad641a881775553238.

[294] *See, e.g.*, Somos Call Branding Comments at 28-29 ("The Commission should prohibit the spoofing of U.S. telephone numbers by foreign-originated calls that lack proper credentials demonstrating a verifiable right to use those numbers. However, where a call is authenticated by an authorized U.S. provider or delegate who takes responsibility for the caller identity information, the geographic location of the calling party should not disqualify its legitimacy. This approach aligns the rules with the foundational principles of STIR/SHAKEN and maintains consistency across domestic and international trust enforcement.").

at the beginning of the call path, at least in the countries that use it?

128. We further seek comment on how foreign providers may be engaged in the U.S. STIR/SHAKEN ecosystem today. Are stakeholders, including the Governance Authority, taking adequate steps to prevent foreign providers from participating in the U.S. STIR/SHAKEN ecosystem? Should we take additional steps to ensure the Governance Authority does not grant SPC tokens to foreign providers? Are gateway providers accepting authentication information on foreign-originated calls and passing it unaltered to the next provider in the call path? If so, should we prohibit gateway providers from accepting authentication information from foreign voice service providers in the absence of CBCA?

3. Public Safety Safeguards

129. We seek comment on downstream impacts any of our proposals would have on 911 service and public safety, including Public Safety Answering Points (PSAPs), particularly as it relates to the transition to Next Generation 911 (NG911). As part of our efforts to expedite the deployment of modern, high-speed IP networks, we have recognized the importance of promoting a reliable and effective 911 system that protects consumers.[295] We have also proposed measures related to the use of IP technology and the transition to IP for combatting illegal calls while remaining cognizant of protecting consumer access to emergency services. Today, 911 Authorities have requested delivery of 911 Traffic in IP-based SIP format covering nearly 1,700 PSAPs.[296] In an all-IP, NG911 environment, we anticipate our proposals herein will help minimize disruptions, such as spoofing, to PSAPs receiving SIP calls. In addition, our proposals should help PSAPs and emergency services that rely on SIP to place return calls to end users and consumers. We invite comment on how any of our proposals would be implemented in transitional 911 environments (i.e., an environment with mixed TDM/IP facilities) that include legacy gateways for converting IP traffic. Since, in the 911 context, originating providers may have to convert IP traffic to TDM as part of the NG911 transition,[297] should we require providers to identify any TDM conversions that are necessary for delivering 911 service as part of the KYUP requirements? To the extent we establish exceptions to blocking requirements and other rules to prevent disruptions to 911 and other public safety calls, are there additional measures that we could apply to mitigate spoofing? For example, should we require providers to report suspicious 911 calls to the Commission and Governance Authority for investigation? Should 911 Authorities be allowed to report spoofing calls to the Commission and Governance Authority? What other measures should service providers, including 911 service providers, take to safeguard 911 and emergency communications in a mixed TDM/IP environment? Would requirements in this document lead to blocking 911 calls from Non-Service Initialized (NSI) callers? Commenters should also discuss any standards in development to mitigate spoofing to 911 and emergency communications.

130. We also seek comment on whether to amend the public safety exceptions in our call blocking and Robocall Mitigation Database rules to explicitly include calls made to emergency services other than 911, including calls to or from the 988 Suicide & Crisis Lifeline (Lifeline).[298] Our 988 rulemakings have established that the Lifeline is an "emergency network" under the Twenty-First Century

[295] *Reducing Barriers to Network Improvements and Service Changes; Accelerating Network Modernization*. WC Docket Nos. 25-209 and 25-208, Report and Order, FCC 26-19 (rel. Mar. 27, 2026) (adopting rules facilitating the retirement of copper lines while providing safeguards to protect public safety and ensure continuity of 911 services).

[296] Under Phase 1 of the FCC's NG911 transition rules, upon receipt of a 911 Authority's valid request, originating providers must, among other things, obtain and deliver 911 traffic to enable NG911 networks to transmit all 911 traffic to the destination PSAP. 47 CFR § 9.29. In addition, the originating provider must also complete connectivity testing to confirm that the 911 Authority receives 911 traffic in the IP-based SIP format requested by the 911 Authority. 47 CFR § 9.29.

[297] *See* 47 CFR § 9.33.

[298] *See* 47 CFR §§ 64.6305(g)(5); 64.1200(k)(4), (5).

Communications Video and Accessibility Act (CVAA).[299] And, in discussing protections for emergency services, the TRACED Act and the TCPA, which provide authority for our RMD and call blocking rules, refer generally to "emergency public safety calls" and "emergency telephone line[s]," including, but not limited to, 911.[300] However, in carving out exceptions for calls to emergency services, our RMD and call blocking rules refer exclusively to emergency calls to 911.[301] Should we revise these rules to explicitly include calls to the 988 Lifeline? Likewise, should we clarify that calls from a 988 crisis center are included under the umbrella of calls from "government emergency numbers" that providers must make reasonable efforts to avoid blocking under these rules? Are such amendments necessary? Would they impose significant burdens on providers or the Lifeline—including affiliated entities such as the Veterans Crisis Line or local crisis centers? Would they reduce the risk of providers blocking lawful calls to 988 seeking lifesaving care? Alternatively, would they subject the Lifeline to increased levels of illegally spoofed robocalls, or other malicious calls, thereby reducing the resources available to legitimate callers? Beyond the 988 Lifeline, are there other emergency services that we should consider including in these public safety exceptions to our robocall blocking rules?

E. Implementation Considerations

1. Enforcement and Other Accountability Measures

131. We propose to enhance base forfeiture amounts for violations of our existing and proposed KYUP and STIR/SHAKEN rules, which we believe will better encourage compliance and thereby enhance consumer protections against illegal calls.[302] Specifically, we propose to adopt a $2,500 per call base forfeiture for calls resulting from a failure to follow KYUP requirements. Additionally, we propose to codify a base forfeiture amount of $1,000 per call for violations of the proposed rules concerning improper attestations and unauthenticated calls. We further propose to codify a $2,500 base forfeiture amount, on a continuing violation basis, for providers who have failed to implement STIR/SHAKEN and are not subject to any exemption.

132. We seek comment on whether we should adopt or promote other measures to hold providers accountable to existing obligations and those we may adopt as proposed above. For instance, should we state that providers are violating our rules if they accept SIP calls from an upstream provider that does not have an SPC token? Should we encourage or require terminating providers to offer consumers tools to block calls or send them to voicemail based on the reputation of the originating provider?[303] Additionally, we seek comment on whether we should explore preemption of state

---

[299] *See Implementation of the National Suicide Hotline Improvement Act of 2018*, WC Docket No. 18-336, Second Report and Order, 36 FCC Rcd 16901, 16933, para. 55 (2021) (*Text-to-988 Second Order*).

[300] *See* 47 U.S.C. § 227(b)(1)(A) (generally prohibiting automatic telephone dialing system calls to "emergency telephone line[s]" including "any '911' line and any emergency line of a hospital, medical physician or service office, health care facility, poison control center, or fire protection or law enforcement agency," except for calls "made for emergency purposes"); *id.* at § 227(j) (requiring robocall blocking services to "make all reasonable efforts to avoid blocking emergency public safety calls"); *see also* 47 CFR § 64.1200(a); (f)(4) (defining "emergency purposes" as "calls made necessary in any situation affecting the health and safety of consumers").

[301] *See* 47 CFR § 64.6305(g) (prohibiting providers from accepting calls directly from a domestic voice service provider that does not appear in the RMD); *id*. at 64.6305(g)(5) (providing that, notwithstanding this prohibition, "[a] provider may not block a voice call under any circumstances *if the call is an emergency call placed to 911*; and (ii) A provider must make all reasonable efforts to ensure that it does not block any calls from public safety answering points and government emergency numbers") (emphasis added); *see also* 47 CFR § 64.1200(k)(5) (prohibiting blocking voice calls that are "emergency call[s] placed to 911"), (k)(6) (requiring providers to "make all reasonable efforts to ensure that calls from public safety answering points and government emergency numbers are not blocked").

[302] *See infra* Appendix A.

[303] ZipDX Triennial Report Comments at 4-6 (suggesting that providers should leverage reputational information they have about providers based on their STIR/SHAKEN signing practice to offer consumers tools to determine how

(continued….)

requirements in the field of caller ID authentication to prevent requirements that are inconsistent with the careful approaches we propose to adopt. Would this ensure a uniform foundation for federal and state enforcement activities?

2. Reporting to the Commission and Governance Authority

133. We propose to require that voice service providers report to the Commission's Enforcement Bureau and to the STIR/SHAKEN Governance Authority any providers they reasonably believe are or may be transmitting illegal calls or violating KYUP or authentication requirements, including improper attestations. We further propose that such reports include a summary of providers' findings and conclusions. We believe that such reporting will aid the Commission and the Governance Authority in their efforts to identify and take action against bad actor providers and the individuals and entities that are behind them.[304] We seek comment on whether we should establish a new mechanism for providers to submit reports to the Commission or use an existing mechanism, such as the Enforcement Bureau's Private Entity Robocall and Spoofing Portal.[305] We also seek comment on how providers will report to the Governance Authority. Do we need to adopt confidentiality measures for reporting? We also seek comment on whether we should set specific parameters of what the reports should contain or whether we should delegate authority to the Bureau to develop the parameters in consultation with the Enforcement Bureau.

3. Bringing Clarity to Caller ID Authentication Rules and Obligations

134. In this section we propose and seek comment on steps to bring clarity to the Commission's caller ID authentication rules and the Commission's obligations under the TRACED Act.

135. *Streamlining caller ID authentication rules.* We propose to take a comprehensive review of the Commission's existing STIR/SHAKEN caller ID authentication rules in sections 64.6300 through 64.6308. In doing so, we endeavor to simplify the rules to remove unnecessary redundancy, ensure consistency, and increase clarity, with the goal of enhancing providers' ability to understand their obligations. We also believe this will enhance the Commission's ability to administer the rules as we enforce and make future updates, including the updates we propose above. By this proposal, we intend to leave unaltered any obligations presently applicable to voice service providers, except to the extent we incorporate proposed modifications above[306] and the one proposed departure below. As such, we encourage commenters to closely review the proposed rules in Appendix A to ensure the streamlined rules reflect the provider obligations set out in prior Commission actions and proposed above.[307] The one

they receive calls, such as by "[a]llowing mobile subscribers to instruct their carrier to have calls from Suspect Signers answered immediately by voicemail, where the caller has the opportunity to leave a compelling message, rather than interrupting the subscriber by ringing their handset").

[304] *See* TransUnion Call Branding Comments at 10-11 (asserting that investigations and enforcement actions by the Commission and Governance Authority could be aided by providers reporting problematic practices, such as other providers "that are applying A-level attestations to calls that are known to have been spoofed"); Somos Call Branding Comments at 23 (urging the Commission to uphold the requirement that intermediate providers forward caller identity and authentication information unaltered); INCOMPAS et al. Triennial Report Comments at 4 (suggesting that providers and their third-party analytics partners be required to report data on STIR/SHAKEN performance to the Commission).

[305] FCC, *Private Entity Robocall and Spoofing Portal*, https://www.fcc.gov/enforcement/private-entity-robocall-spoofing-portal (last updated Dec. 20, 2022).

[306] We note that there are certain minor proposed changes that reflect codification of requirements that were stated in prior Commission orders, such as the requirement that providers implement the STIR/SHAKEN framework in accordance with the STIR/SHAKEN standards.

[307] Of particular note, we propose to remove the subparagraph numbers for the definitions in section 64.6300, which is consistent with the Federal Register Document Drafting Handbook recommendation, and will allow us to add future definitions in alphabetical order without causing confusion related to cross-references in the Commission's

(continued….)

departure concerns the scope of the robocall mitigation program obligation for gateway providers, which is currently limited to calls using U.S. NANP resources in the caller ID field.[308] We do not believe there is any statutory or policy requirement for limiting gateway providers' obligation to mitigate illegal calls to only calls they receive that use U.S. NANP resources in the caller ID field, and further believe that gateway providers should attempt to mitigate any illegal calls they receive. As such, we propose to modify gateway providers' obligation to require that their robocall mitigation programs apply to all calls they carry and process.

136. *Definitions related to the Governance Authority.* To promote better clarity in our rules, we propose to define "certificate," "Certification Authority," and "Policy Administrator" for the purposes of our caller ID authentication rules. Specifically, we propose to define "certificate" as a digital data object obtained from a Certification Authority which is used by a voice service provider to sign and verify caller identification information consistent with the STIR/SHAKEN authentication framework.[309] We propose to define "Certification Authority" as an entity that issues certificates and vouches for the binding between the data items in a certificate.[310] Finally, we propose to define "Policy Administrator" as a STIR/SHAKEN governance body that applies rules set by the Governance Authority, confirms that Certification Authorities are authorized to issue certificates, and confirms that voice service providers are authorized to request and receive certificates.[311] We also propose to amend the definition of SPC token to clarify that the SPC token allows a voice service provider to obtain a certificate from a Certification Authority.[312] We define these terms consistent with ATIS usage to avoid unnecessary industry confusion. We seek comment on these definitions.

4. Effective Date

137. We propose that the proposed rules herein become effective the later of 12 months after *Federal Register* publication of a Report and Order adopting the rules or 30 days after approval by the Office of Management and Budget (OMB) for rules that contain new or modified information collections subject to review under the Paperwork Reduction Act (PRA). We seek comment on this proposal. Should we adopt different effective dates for different rules or for different types of providers, such as small providers?

F. Legal Authority

138. We propose to adopt the above proposals pursuant to our authority in sections 201(b), 202(a), and 251(e) of the Act, the Truth in Caller ID Act, the TRACED Act, and, where appropriate, our ancillary authority, consistent with the authority we have invoked to adopt analogous rules in our *Caller ID Authentication* and *Call Blocking Orders*. We seek comment on these proposals.

---

rules and when rules are cited in Commission items over time. *See* Office of the Federal Register, Document Drafting Handbook, Revision 2.2, at 2-27 (2025), https://www.archives.gov/files/federal-register/write/handbook/ddh.pdf. We also note that we proposed a more limited set of streamlining changes in the *Non-IP Caller ID Authentication NPRM* and that the changes we propose here build on those proposed changes. *See Non-IP Caller ID Authentication Notice of Proposed Rulemaking*, 40 FCC Rcd at 3488, para. 43 n.145.

[308] 47 CFR § 64.6305(b)(1).

[309] *See* ATIS-1000074 at 3.

[310] ATIS-1000074 at 3.

[311] *First Caller ID Authentication Order*, 35 FCC Rcd at 3246, para. 10.

[312] It is common in industry parlance to describe a voice service provider as signing caller ID authentication information with the provider's SPC token. *See, e.g.*, *Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12912, para. 25 (quoting USTelecom). We understand this usage to be an elision, as it is the certificate which is most directly used to sign calls. *See, e.g.*, *First Caller ID Authentication Order*, 35 FCC Rcd at 3246, para. 9. As our rules properly obligate voice service providers to sign calls using the certificate, *see* 47 CFR § 64.6301(a)(1)-(2), amending the definition of SPC token will ensure consistency with those rules.

139. *Proposed KYUP Requirements.* We intend to rely on sections 201(b), 202(a), and 251(e) of the Act, as well as the Truth in Caller ID Act as support for the proposed KYUP and related call blocking requirements because they are aimed at reducing spoofing and curbing the use of NANP numbers for unlawful purposes.[313] Sections 201(b) and 202(a) provide the Commission with "broad authority to adopt rules governing just and reasonable practices of common carriers."[314] The Commission has previously concluded that the existing KYC and KYUP requirements are "clearly within the scope of our section 201(b) and 202(a) authority" with respect to common carriers.[315] In addition, the Commission has found that section 251(e) and the Truth in Caller ID Act provide the basis to prescribe rules to prevent the unlawful spoofing of caller ID and abuse of NANP resources by all voice service providers, which for purposes of our call blocking, KYC, and KYUP rules includes interconnected VoIP providers.[316] Specifically, the Commission has found that our "Section 251(e) numbering authority provides separate jurisdiction to prevent the fraudulent abuse of North American Numbering Plan (NANP) resources," which "particularly applies where callers spoof caller ID for fraudulent purposes and therefore exploit numbering resources, regardless of whether the voice service provider is a common carrier."[317] Similarly, the Commission has found that "the Truth in Caller ID Act grants us authority to prescribe rules to make unlawful the spoofing of caller ID information with the intent to defraud, cause harm, or wrongfully obtain something of value."[318] We believe these same statutory provisions support the enhanced KYUP and blocking requirements we propose here and seek comment on this view. Are there additional sources of authority we should consider?

140. We also intend to rely on authority in section 4 of the TRACED Act, which directs the Commission to, among other things, establish "when a provider of voice service may block a voice call based in whole or in part on information provided by the call authentication frameworks."[319] This provision lends support to the KYUP proposal because it may require providers to evaluate various aspects of an upstream providers' STIR/SHAKEN implementation when determining whether to accept calls from an upstream provider. Additionally, pursuant to section 7 of the TRACED Act, the Commission initiated a rulemaking to "help protect a subscriber from receiving unwanted calls or text messages from a caller using an unauthenticated number."[320] We believe the KYUP proposals and associated call blocking requirement would have the effect of protecting consumers from unwanted calls from unauthenticated numbers. We seek comment on this analysis.

---

[313] *Gateway Provider Order*, 37 FCC Rcd at 6912-13, paras. 116-17; *Fourth Call Blocking Order*, 35 FCC Rcd at 15232-34, paras. 32-38.

[314] *Fourth Call Blocking Order*, 35 FCC Rcd at 15233-34, para. 37.

[315] *Fourth Call Blocking Order*, 35 FCC Rcd at 15234, para. 37; *Sixth Call Blocking Order*, 37 FCC Rcd at 6912-13, paras. 116-117; *Seventh Call Blocking Order*, 38 FCC Rcd at 5426, para. 65; *see also* 47 U.S.C. § 154(i).

[316] *Fourth Call Blocking Order*, 35 FCC Rcd at 15234, para. 37; *id*. at 15222, para. 2 n.2 (defining "voice service provider" to include "any entity originating, carrying, or terminating voice calls through . . . Voice over Internet Protocol (VoIP)").

[317] *Fourth Call Blocking Order*, 35 FCC Rcd at 15234, para. 37; *see also Second Caller ID Authentication Order*, 36 FCC Rcd at 1910, para. 99 (concluding "section 251(e) gives us authority to prohibit intermediate providers and voice service providers from accepting traffic from both domestic and foreign voice service providers that do not appear in [the Robocall Mitigation Database]," and noting that its "exclusive jurisdiction over numbering policy provides authority to take action to prevent the fraudulent abuse of NANP resources"); *id.* (observing that "[i]llegally spoofed calls exploit numbering resources whenever they transit any portion of the voice network—including the networks of intermediate providers" and that "preventing such calls from entering an intermediate provider's or terminating voice service provider's network is designed to protect consumers from illegally spoofed calls").

[318] *Fourth Call Blocking Order*, 35 FCC Rcd at 15233-34, para. 37.

[319] TRACED Act § 4(c)(1) (codified at 47 U.S.C. § 227b(c)(1)).

[320] *See* TRACED Act § 7; *Third Call Blocking Order and Further Notice*, 35 FCC Rcd at 7642-43, paras. 88-90.

141. *Proposed caller ID authentication requirements.* We intend to rely on section 4 of the TRACED Act for the STIR/SHAKEN proposals herein.[321] Congress expressly directed the Commission to require voice service providers to implement the STIR/SHAKEN caller ID authentication framework in section 4 of the TRACED Act.[322] We believe that adopting the proposed requirements above, which are designed to ensure the ubiquitous and consistent implementation of STIR/SHAKEN, fits squarely within our authority to require that voice service providers implement STIR/SHAKEN. Assuming we adopt our proposal to read the TRACED Act's "voice service" definition to include intermediate providers consistent with the RAY BAUM'S Act and section 64.1600(r) of the Commission's rules, we believe the TRACED Act gives us authority to apply these requirements to all originating, intermediate, and terminating providers. We also intend to rely on the TRACED Act for authority to adopt our proposals related to the STIR/SHAKEN Governance Authority. These rules will better ensure that providers are held accountable for properly implementing STIR/SHAKEN, thereby enhancing the trust and integrity upon which STIR/SHAKEN relies. We seek comment on this analysis.

142. We also intend to rely on section 251(e) of the Act and the Truth in Caller ID Act, which we believe each provide the Commission with independent authority to exercise the proposed oversight of the Governance Authority, require providers to adopt the enhanced attestation requirements using the STIR/SHAKEN framework, clarify the definitions related to application of the STIR/SHAKEN requirements, and address the remaining loopholes to STIR/SHAKEN implementation.[323] The Commission has consistently relied on these provisions to establish requirements related to STIR/SHAKEN caller ID authentication as a means of preventing the fraudulent abuse of NANP resources as directed in section 251(e) and as directed in the Truth in Caller ID Act deter unlawful spoofing.[324] We seek comment on these views.

143. *Ancillary authority.* While we propose to conclude that our direct sources of authority provide an ample basis to adopt our proposed rules on voice service providers, we intend, as we have with our prior rulemakings addressing illegal calls, to rely on our ancillary authority in section 4(i),[325] which provides an independent basis to adopt rules with respect to voice service providers that have not been classified as common carriers. We seek comment on this view. The Commission has previously relied on its ancillary authority in section 4(i) to apply the existing KYC, KYUP, call blocking requirements to such providers,[326] finding "that it is essential that the rules apply to all voice service providers."[327] We thus likewise believe that the proposed KYUP and call blocking requirements are "reasonably ancillary to the Commission's effective performance of its . . . responsibilities."[328] The Commission may exercise

[321] *Sixth Caller ID Authentication Further Notice*, 38 FCC Rcd at 2624, para. 110; 47 U.S.C. § 227b(b)(1).

[322] 47 U.S.C. § 227b(b)(1)(A). Consistent with the Commission's prior call blocking and caller ID authentication orders, we find that sections 201(b) and 201(a) of the Act, and the Commission's ancillary authority in section 4(i) of the Act, provide us with additional sources of authority to adopt these robocall mitigation requirements. *See, e.g.*, *Sixth Caller ID Authentication Further Notice*, 38 FCC Rcd at 2617-19, paras. 92-95.

[323] *See* 47 U.S.C. §§ 227(e), 251(e).

[324] *See Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12923-24, paras. 43-44, 46; *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2617-18, paras. 91-93; *Gateway Provider Order and Further Notice of Proposed Rulemaking*, 37 FCC Rcd at 6911-13, paras. 113-17; *Second Caller ID Authentication Order*, 36 FCC Rcd at 1931-32, paras. 153-55; *First Caller ID Authentication Order*, 35 FCC Rcd at 3260-62, paras. 42, 44.

[325] 47 U.S.C. § 154(i).

[326] *Fourth Call Blocking Order*, 35 FCC Rcd at 15233-34, paras. 37-38.

[327] *Fourth Call Blocking Order*, 35 FCC Rcd at 15234, para. 37; *see also* 47 U.S.C. § 154(i).

[328] *United States v. Southwestern Cable Co.*, 392 U.S. 157, 178 (1968); *see also, e.g.*, *Rural Call Completion*, WC Docket No. 13-39, Report and Order and Further Notice of Proposed Rulemaking, 28 FCC Rcd 16154, 16562, para. 35 (2013) ("Ancillary authority may be employed, at the Commission's discretion, when the Act covers the

(continued….)

ancillary jurisdiction when two conditions are satisfied: (1) the Commission's general jurisdictional grant under Title I of the Communications Act covers the regulated subject; and (2) the regulations are reasonably ancillary to the Commission's effective performance of its statutorily mandated responsibilities.[329] Specifically, we believe the proposals satisfy the first prong because voice service providers are interconnected with the public switched telephone network, and exchanging IP traffic clearly constitutes "communication by wire or radio" under section 2(a) of the Act.[330] We also believe the proposed requirements are reasonably ancillary to our exercise of authority under sections 201(b) and 202(a), as we do not believe we could ensure that voice service providers that are classified as common carriers comply with obligations to address illegal calls if the same rules did not apply to voice service providers that are not classified as common carriers, and the inability of common carriers to comply with obligations could create a gap that bad actor providers could exploit. Additionally, we believe the proposals are reasonably ancillary to our authority in 251(e) and the Truth in Caller ID Act to combat spoofing and our authority in the TRACED Act to ensure mitigation and blocking of illegal calls using authentication information. We seek comment on this analysis.

144. *Indirect effect on foreign voice service providers.* We propose to conclude that, to the extent any of the rules we seek to adopt today have an effect on foreign voice service providers, that effect is only indirect and therefore consistent with the Commission's authority. In the *Second Caller ID Authentication Order*, the Commission acknowledged its rules would have an indirect effect on foreign providers but concluded that it was permissible under past Commission and court precedent.[331] This includes the authority, pursuant to section 201, for the Commission to require a domestic provider to modify its contracts with a foreign provider with respect to "foreign communication" to ensure that the charges and practices are "just and reasonable."[332] We propose to conclude that the proposed rules do not constitute the exercise of jurisdiction over foreign providers. We seek comment on this and on whether any of our proposed rules exceed the scope of our jurisdiction over foreign communications that enter the United States. We also seek comment on whether any of our proposed rules would be contrary to any of

regulated subject and the assertion of jurisdiction is reasonably ancillary to the effective performance of the Commission's various responsibilities." (internal citations omitted)).

[329] *See*, *e.g.*, *Comcast Corp. v. FCC*, 600 F.3d 642, 646 (D.C. Cir. 2010); *American Library Ass'n v. FCC*, 406 F.3d 689 (D.C. Cir. 2005).

[330] 47 U.S.C. § 152(a).

[331] *Second Caller ID Authentication Order*, 36 FCC Rcd at 1910 n.370 ("An indirect effect on foreign voice providers, however, 'does not militate against the validity of rules that only operate directly on voice service providers within the United States'") (quoting *International Settlement Rate Benchmarks*, IB Docket No. 96-261, Report and Order, 12 FCC Rcd 19806, 19819, para. 27 (1997)); *see also Cable & Wireless P.L.C. v. FCC*, 166 F.3d 1224, 1230 (D.C. Cir. 1999) (finding that "the Commission does not exceed its authority simply because a regulatory action has extraterritorial consequences"); *see also* 47 CFR §§ 1.767(g)(5), 63.14 (prohibiting carriers from agreeing to access special concessions from a foreign carrier with respect to any U.S. international route where the foreign carrier possesses sufficient market power to adversely affect competition in the U.S. market); *Petition of AT&T for Settlements Stop Payment Order on the U.S.-Tonga Route*, IB Docket No. 09-10, Memorandum Opinion and Order, 29 FCC Rcd 4186, 4196, para. 24 (2014) (*Tonga*) (concluding that "Commission review and interpretation of contracts entered into by U.S. carriers for delivery of traffic to foreign destinations may, as here, be necessary and relevant to the Commission's policy goals of protecting U.S. ratepayers from the effects of anticompetitive actions . . . Thus, the existence of extraterritorial consequences stemming from the Bureau's review of this case does not render the Bureau's actions impermissible").

[332] *See* 47 U.S.C. § 201; *Tonga*, 24 FCC Rcd at 8014-15, para. 24 ("The Act also gives the Commission authority to prescribe just and reasonable charges when it finds that a charge or practice associated with a U.S. carrier providing foreign communications is unlawful.").

our international treaty obligations, other international laws and rules, or create a risk of foreign retaliation.[333]

G. Cost–Benefit Analysis

145. We seek comment on the overall costs and benefits of our proposals above and whether the benefits will outweigh the costs.

146. Consumers continue to be victims of significant fraud, and a substantial amount of the fraud is perpetrated through illegal calls. According to the most recent FTC's Consumer Sentinel Network Data Book by the Federal Trade Commission, 19% of reported fraud was due to phone calls and the median loss to individuals of such fraud was $1500 in 2024 for a total of $948M that year.[334] Hiya's February 2026 State of the Call Report shows reports that consumers receive an average of 7 unwanted calls every week with 15% of respondents saying they lost money to a phone scam in the last year, resulting in an average individual loss of $682 from phone scams in the U.S.[335] We believe that our proposals above will have a meaningful impact on the reducing illegal calls, therefore substantially reducing the harms to consumers that result from these calls. In the long term, we believe more effective KYUP and caller ID authentication will increase trust in the nation's voice networks, yielding positive spillover benefits such as greater consumer willingness to answer legitimate calls, more effective communication between enterprises and their customers, and improved performance of emergency and public-safety calling systems. We seek comment on these views. What portion of providers already follow robust KYUP or STIR/SHAKEN practices, and therefore, to what extent will the benefits be incremental for customers of already-compliant providers? How will increased trust in authenticated voice communications manifest in measurable market or consumer outcomes? We also invite comment on appropriate methods to measure these benefits. How will these rules impact illegal calls? How should the Commission quantify the benefits or estimate the reduction in illegal calls? What data can the Commission use to measure these benefits?

147. We believe that the costs of our proposal will be minimal for providers that already take their KYUP and STIR/SHAKEN obligations seriously, as many of the proposals are designed to codify practices that providers should already be following to meet their obligations. We seek comment on this view. To what extent will the costs differ for different types of providers? What are the costs, and their impact, on small providers specifically? How may we mitigate such costs, if indeed there are any? Do other commenters agree with this assessment? Because our proposals are necessarily aimed at reducing the number of illegal calls that transverse the voice network, we recognize that providers may lose revenue if call volumes shrink. However, we believe these losses will be made up over time by increased call volumes resulting from the restoration of trust by consumers and businesses in voice communications. We seek comment on this assessment.

IV. PROCEDURAL MATTERS

148. *Regulatory Flexibility Act.* The Regulatory Flexibility Act of 1980, as amended (RFA),[336] requires that an agency prepare a regulatory flexibility analysis for notice-and-comment rulemaking proceedings, unless the agency certifies that "the rule will not, if promulgated, have a

---

[333] *Cf.* Comments of BT Americas, WC Docket No. 17-97, at 4-5 (filed Jan. 29, 2021) (arguing that the foreign provider prohibition could implicate foreign tax, privacy and data protection issues and result in retaliation from foreign regulators).

[334] FTC, Consumer Sentinel Network Data Book 2024 at 12 (2025), https://www.ftc.gov/system/files/ftc_gov/pdf/csn-annual-data-book-2024.pdf.

[335] HIYA, State of the Call 2026 at 2, 5 (2026), https://work.hiya.com/hubfs/2026/Hiya_SotC_2026_FINAL.pdf?hsLang=en.

[336] 5 U.S.C. §§ 601 *et seq.*, as amended by the Small Business Regulatory Enforcement and Fairness Act (SBREFA), Pub. L. No. 104-121, 110 Stat. 847 (1996).

significant economic impact on a substantial number of small entities."[337] Accordingly, the Commission has prepared an Initial Regulatory Flexibility Analysis (IRFA) concerning potential rule and policy changes contained in this *Notice of Proposed Rulemaking*. The IRFA is set forth in Appendix B. The Commission invites the general public, in particular small businesses, to comment on the IRFA. Comments must be filed by the deadlines for comments on the *Notice of Proposed Rulemaking* indicated on the first page of this document and must also have a separate and distinct heading designating them as responses to the IRFA.

149. *Paperwork Reduction Act.* This *Notice of Proposed Rulemaking* may contain proposed new or modified information collections. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and the Office of Management and Budget (OMB) to comment on any information collections contained in this document, as required by the Paperwork Reduction Act of 1995, 44 U.S.C. §§ 3501-3521. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, 44 U.S.C. § 3506(c)(4), we seek specific comment on how we might further reduce the information collection burden for small business concerns with fewer than 25 employees.

150. *Providing Accountability Through Transparency Act.* Consistent with the Providing Accountability Through Transparency Act, Public Law 118-9, a summary of this document will be available on https://www.fcc.gov/proposed-rulemakings.

151. *Ex parte presentations—permit-but-disclose.* The proceeding this *Notice of Proposed Rulemaking* initiates shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules.[338] Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with section 1.1206(b) of the Commission's rules. In proceedings governed by section 1.49(f) of the Commission's rules or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must, when feasible, be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (e.g., .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.[339]

152. *Comment filing procedures.* Pursuant to sections 1.415 and 1.419 of the Commission's rules, 47 CFR §§ 1.415, 1.419, interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS).

- *Electronic Filers*: Comments may be filed electronically using the Internet by accessing the ECFS: https://www.fcc.gov/ecfs.
    - *Paper Filers*: Parties who choose to file by paper must file an original and one copy

[337] *Id.* § 605(b).

[338] 47 CFR §§ 1.1206.

[339] *Id.* §§ 1.1200-1216.

of each filing.

- Filings can be sent by hand or messenger delivery, by commercial courier, or by the U.S. Postal Service. **All filings must be addressed to the Secretary, Federal Communications Commission.**
- Hand-delivered or messenger-delivered paper filings for the Commission's Secretary are accepted between 8:00 a.m. and 4:00 p.m. by the FCC's mailing contractor at 9050 Junction Drive, Annapolis Junction, MD 20701. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes and boxes must be disposed of before entering the building.
- Commercial courier deliveries (any deliveries not by the U.S. Postal Service) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701.
- Filings sent by U.S. Postal Service First-Class Mail, Priority Mail, and Priority Mail Express must be sent to 45 L Street NE, Washington, DC 20554.

- *People with Disabilities*: To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530.

153. *Additional information.* For further information about the *Notice of Proposed Rulemaking*, contact Chris Laughlin, Deputy Division Chief, Competition Policy Division, Wireline Competition Bureau, at Chris.Laughlin@fcc.gov.

V. ORDERING CLAUSES

154. Accordingly, pursuant to sections 4(i), 4(j), 201, 202, 217, 227, 251(e), 303(r), 403, 501, 502, and 503 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 154(i), 154(j), 201, 202, 217, 227, 251(e), 303(r), 403, 501, 502, and 503, and section 4 of the TRACED Act, 47 U.S.C. § 227b, this *Notice of Proposed Rulemaking* IS ADOPTED.[340]

155. IT IS FURTHER ORDERED that the Commission's Office of the Secretary, SHALL SEND a copy of this *Notice of Proposed Rulemaking*, including the Initial Regulatory Flexibility Analysis, to the Chief Counsel for the Small Business Administration (SBA) Office of Advocacy.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

[340] Pursuant to Executive Order 14215, 90 Fed. Reg. 10447 (Feb. 24, 2025), this regulatory action has been determined to be not significant under Executive Order 12866, 58 Fed. Reg. 51735 (Oct. 4, 1993).

APPENDIX A

Proposed Rules

For the reasons discussed in the document, the Federal Communications Commission proposes to amend 47 CFR parts 1 and 64 as follows:

PART 1 – Practice and Procedure

1. The authority citation for part 1 continues to read as follows:

Authority: 47 U.S.C. chs. 2, 5, 9, 13; 28 U.S.C. § 2461 note; 47 U.S.C. § 1754, unless otherwise noted.

2. Amend § 1.80(b)(11) by revising tbl.1 to (b)(11) to read as follows:

(11) * * *

Table 1 to Paragraph (b)(11) - Base Amounts for Section 503 Forfeitures

Forfeitures	**Violation amount**
Misrepresentation/lack of candor	(1)
Failure to file required DODC required forms, and/or filing materially inaccurate or incomplete DODC information	$15,000
Construction and/or operation without an instrument of authorization for the service	10,000
Failure to comply with prescribed lighting and/or marking	10,000
Violation of public file rules	10,000
Submitting inaccurate or false information to the Robocall Mitigation Database (Continuing violation until cured)	10,000
Violation of political rules: Reasonable access, lowest unit charge, equal opportunity, and discrimination	9,000
Unauthorized substantial transfer of control	8,000
Violation of children's television commercialization or programming requirements	8,000
Violations of rules relating to distress and safety frequencies	8,000
False distress communications	8,000
EAS equipment not installed or operational	8,000
Alien ownership violation	8,000
Failure to permit inspection	7,000
Transmission of indecent/obscene materials	7,000
Interference	7,000
Importation or marketing of unauthorized equipment	7,000
Exceeding of authorized antenna height	5,000

Fraud by wire, radio or television	5,000
Unauthorized discontinuance of service	5,000
Use of unauthorized equipment	5,000
Exceeding power limits	4,000
Failure to Respond to Commission communications	4,000
Violation of sponsorship ID requirements	4,000
Unauthorized emissions	4,000
Using unauthorized frequency	4,000
Failure to engage in required frequency coordination	4,000
Construction or operation at unauthorized location	4,000
Violation of requirements pertaining to broadcasting of lotteries or contests	4,000
Violation of transmitter control and metering requirements	3,000
Failure to file required forms or information	3,000
Failure to implement the STIR/SHAKEN authentication framework (continuing violation until cured)	2,500
Per call know an upstream provider violations	2,500
Per call violations of the robocall blocking rules	2,500
Failure to make required measurements or conduct required monitoring	2,000
Failure to provide station ID	1,000
Unauthorized pro forma transfer of control	1,000
Failure to maintain required records	1,000
Failure to update Robocall Mitigation Database within 10 business days (continuing violation until cured)	1,000
Per call caller ID authentication attestation violations	1,000

* * * * *

PART 64 – Miscellaneous Rules Relating to Common Carriers

3. The authority citation for part 64 continues to read as follows:

Authority: 47 U.S.C. §§ 151, 152, 154, 201, 202, 217, 218, 220, 222, 225, 226, 227, 227b, 228, 251(a), 251(e), 254(k), 255, 262, 276, 403(b)(2)(B), (c), 616, 620, 716, 1401-1473, unless otherwise noted; Pub. L. 115-141, Div. P, sec. 503, 132 Stat. 348, 1091; Pub. L. 117-338, 136 Stat. 6156.

4. Amend § 64.1200 by revising paragraph (n) to read as follows:

§ 64.1200 Delivery restrictions.

* * * *

(n) A voice service provider must:

(5) take affirmative, effective measures to prevent any voice service provider directly upstream from it, foreign or domestic, from using its network or services to transmit illegal calls, including knowing its upstream voice service provider. For purposes of this rule, a voice service provider must:

(i) collect directly from the upstream provider general business information, financial information, Internet commercial presence information, ownership and affiliate information, operational information, and service information or an explanation for why the upstream provider cannot produce any such information;

(ii) perform due diligence of the upstream provider's compliance with Commission rules related to the provision of service;

(iii) perform due diligence to verify the validity and authenticity of the upstream provider, the information the provider obtained from or about the upstream provider, and the upstream provider's explanation for any information it could not produce, including:

(a) confirming any phone numbers and email addresses are active;

(b) participating in a verbal communication with one or more human principals, owners, or company leaders;

(c) conducting general research to identify risk factors or contradictory information;

(d) reviewing the upstream provider's Internet commercial presence information to identify risk factors or contradictory information;

(e) conducting a basic comparative analysis of the information to identify inconsistencies among the information and consistencies with information concerning other upstream providers; and

(f) evaluating the upstream provider's financial information to identify risk factors;

(iv) monitor the upstream provider by:

(a) regularly checking the upstream provider's compliance with Commission rules related to the provision of service;

(b) using call analytics on an ongoing basis to identify illegal or suspect calls or call patterns from the upstream provider,

(c) evaluate on a timely basis information or evidence it finds, receives, or is made aware of that the upstream provider is transmitting illegal calls, failing to authenticate calls, or authenticating calls with improper attestations;

(d) evaluating on a timely basis whether any information or evidence it finds, receives, or is made aware presents inconsistencies with other information obtained from or about the upstream provider under this paragraph (n)(5); and

(e) evaluating on a timely basis any other new information or evidence it finds, receives, or is made aware of concerning the upstream provider's reputation.

(v) perform a holistic, totality of the circumstances evaluation of the upstream provider based on the actions taken under this paragraph (n)(5) and implement measures to refuse or discontinue service:

(a) when the results do not form an objectively reasonable basis for concluding that the upstream provider is a valid and authentic entity;

(b) when the results form an objectively reasonable basis for concluding that the upstream provider is likely to use or is using its network or services to transmit illegal calls or enable the transmission of illegal calls;

(c) when the upstream provider does not have a filing in the RMD, does not have an SPC token, is on the Foreign Adversary Control System or the Covered List, has had a Commission license revoked, or has been the subject of any other Commission enforcement actions that deny is ability to provision voice service; or

(d) when the provider finds, receives, or is made aware that the upstream provider does not have mechanisms in place to ensure its customers, upstream providers, clients, employees, and contractors comply with federal and state laws and regulations concerning unlawful calls, including any KYC and KYUP requirements established by the Commission;

(vi) retain the information it collects for the upstream provider for a period of four (4) years; and

(vii) report to the Commission's Enforcement Bureau and the Governance Authority any voice service provider it reasonably believes is or may be transmitting illegal calls or violating KYUP obligations.

(6) block any SIP call it receives from another voice service provider that uses North American Numbering Plan resources in the caller identification field and does not have authenticated caller identification information in accordance with § 64.6301, except that it must:

(i) not block a SIP call if the call is placed to 911 or the 988 Suicide and Crisis Hotline; and

(ii) make all reasonable efforts to ensure that it does not block any call from a public safety answering point or government emergency number.

5. Revise § 64.6300 to read as follows:

§ 64.6300 Definitions.

Authenticate caller identification information. The term "authenticate caller identification information" refers to the process by which a voice service provider attests to the accuracy of caller identification information transmitted with a call.

Caller identification information. The term "caller identification information" has the same meaning given the term "caller identification information" in § 64.1600(c) as it currently exists or may hereafter be amended.

Certificate. The term "certificate" refers to a digital data object obtained from a Certification Authority which is used by a voice service provider to sign and verify caller identification information consistent with the STIR/SHAKEN authentication framework.

Certification Authority. The term "Certification Authority" refers to an entity that issues certificates and vouches for the binding between the data items in a certificate.

Customer. The term "customer" refers to any individual or entity that purchases voice service from a voice service provider.

Domestic voice service provider. The term "domestic voice service provider" refers to a voice service provider that is not a foreign voice service provider.

Downstream. The term "downstream" refers to a point closer to the destination of a call.

End User. The term "end user" refers to the ultimate consumer of voice service.

Foreign voice service provider. The term "foreign voice service provider" refers to a voice service provider that was created, incorporated, or organized outside of the United States, regardless of whether it has an office, operation, or facilities in the United States.

Gateway provider. The term "gateway provider" means a domestic voice service provider that is an intermediate provider that accepts voice calls directly from a foreign voice service provider before transmitting the call downstream to another domestic voice service provider.

Governance Authority. The term "Governance Authority" refers to the Secure Telephone Identity Governance Authority, which is the entity that establishes and governs the policies regarding the issuance, management, and revocation of Service Provider Code (SPC) tokens to voice service providers.

Improper attestation. The term "improper attestation" means any attestation level that does not conform with ATIS-1000074 and § 64.6301, including any attestation that is inconsistent with the information the voice service provider has, or is required to have, about a call.

Industry traceback consortium. The term "industry traceback consortium" refers to the consortium that conducts private-led efforts to trace back the origin of suspected unlawful robocalls as selected by the Commission pursuant to § 64.1203.

Initiation. The term "initiation" refers to the action performed by a voice service customer in commencing a call, and does not include origination.

Initiating provider. The term "initiating provider" refers to a voice service provider that performs initiation.

Intermediate provider. The term "intermediate provider" means a voice service provider that carries or processes voice traffic but neither performs the origination or termination of that traffic.

Non-gateway intermediate provider. The term "non-gateway intermediate provider" means a voice service provider that is an intermediate provider but is not a gateway provider.

Originating provider. The term "originating provider" refers to a voice service provider that performs the origination of a given call.

Origination. The term "origination" refers to the technological act of placing a customer's outgoing call onto the network using the provider's own facilities.

Policy Administrator. The term "Policy Administrator" refers to a STIR/SHAKEN governance body that applies rules set by the Governance Authority, confirms that Certification Authorities are authorized to issue certificates, and confirms that voice service providers are authorized to request and receive certificates.

Robocall Mitigation Database. The term "Robocall Mitigation Database" refers to a database accessible via the Commission's website that lists all entities that make filings pursuant to § 64.6305(b).

SIP call. The term "SIP call" refers to a call that is initiated, originated, carried, processed, and terminated using the Session Initiation Protocol signaling protocol.

SPC token. The term "SPC token" refers to the Service Provider Code token, which is an authority token validly issued to a voice service provider that allows the provider obtain a certificate from a Certification Authority.

STIR/SHAKEN authentication framework. The term "STIR/SHAKEN authentication framework" means the Secure Telephone Identity Revisited and Signature-based Handling of Asserted information using toKENs standards.

Terminating provider. The term "terminating provider" refers to a voice service provider that performs the termination of a given call.

Termination. The term "termination" refers to the technological act of serving to a customer an incoming call received on a provider's own facilities that are interconnected with the public network.

Upstream. The term "upstream" refers to a point closer to the source of a call.

Verify caller identification information. The term "verify caller identification information" refers to the process by which a terminating provider confirms that the caller identification information transmitted with a call for which it performs termination was properly authenticated.

Voice service. The term "voice service"—

(1) Means any service that is interconnected with the public switched telephone network and that furnishes voice communications to an end user using resources from the North American Numbering Plan or any successor to the North American Numbering Plan adopted by the Commission under section 251(e)(1) of the Communications Act of 1934, as amended; and

(2) Includes—

(i) Transmissions from a telephone facsimile machine, computer, or other device to a telephone facsimile machine; and

(ii) Without limitation, any service that enables real-time, two-way voice communications, including any service that requires Internet Protocol-compatible customer premises equipment and permits out-bound calling, whether or not the service is one-way or two-way Voice over Internet Protocol.

Voice service provider. The term "voice service provider" means any entity that provides voice service for a given call.

6. Revise § 64.6301 to read as follows:

§ 64.6301 Caller ID authentication in IP networks.

(a) ***STIR/SHAKEN implementation.*** Except as provided in § 64.6301(f), each voice service provider shall fully implement the STIR/SHAKEN authentication framework in its Internet Protocol networks in accordance with the STIR/SHAKEN authentication framework standards. To fulfill this obligation:

(1) An originating or intermediate provider shall:

(i) obtain an SPC token from the Secure Telephone Identity Policy Administrator in accordance with the Governance Authority token access policy; and

(ii) use that SPC token to obtain Secure Telephone Identity certificates from a Secure Telephone Identity Certification Authority in accordance with the Governance Authority certificate policy;

(2) An originating provider shall, using the certificates obtained pursuant to paragraph (a)(1)(ii) of this section, authenticate caller identification information consistent with the attestation-level decisions made pursuant to § 64.6301(d) for all SIP calls for which it performs origination that will exclusively transit its own network or that it will exchange with another voice service provider;

(3) A non-gateway intermediate provider shall, using the certificates obtained pursuant to paragraph (a)(1)(ii) of this section, authenticate caller identification information for all calls it receives from a domestic voice service provider that use North American Numbering Plan resources in the caller identification field and that are not SIP calls and which it will exchange with another provider as a SIP call;

(4) A gateway provider shall, using the certificates obtained pursuant to paragraph (a)(1)(ii) of this section, authenticate caller identification information for all calls it receives from a foreign voice service provider that use North American Numbering Plan resources in the caller identification field for which the caller identification information has not been authenticated and

which it will exchange with another provider as a SIP call; and

(5) An intermediate provider shall pass unaltered to the next voice service provider in the call path any authenticated caller identification information it receives with a SIP call, except:

(i) where necessary for technical reasons to complete the call; or

(ii) where the intermediate provider reasonably believes the caller identification authentication information presents an imminent threat to its network security; so long as

(iii) it re-authenticates caller identification information using the certificates obtained pursuant to paragraph (a)(1)(ii) of this section; and

(6) A terminating provider shall verify authenticated caller identification information for all SIP calls for which it performs termination that exclusively transit its own network or that it receives from another voice service provider.

(b) ***Attestation requirements and prohibitions.*** A voice service provider shall not willfully apply attestation levels inconsistent with the following criteria for each level:

(1) ***A-level attestations.*** To authenticate the caller identification information of a call with an A-level attestation, a voice service provider shall, consistent with the STIR/SHAKEN authentication framework:

(i) be responsible for the origination of the call onto the IP network,

(ii) have a direct, authenticated relationship with the customer associated with the call and be able to identify the customer by satisfying the requirements in § 64.1200(n)(4)-(5), and

(iii) establish a verified association between the customer and the telephone number used for a call, which shall presumptively be satisfied if the provider assigned the telephone number to the customer and shall not be satisfied by a business agreement or certification that includes a general statement that the customer will only use numbers with which it has a verified association or when the numbers meet the conditions in § 64.1200(o).

(2) ***B-level attestations.*** To authenticate the caller identification information of a call with a B-level attestation, a voice service provider shall, consistent with the STIR/SHAKEN authentication framework:

(i) be responsible for the origination of the call onto the IP network,

(ii) have a direct, authenticated relationship with the customer associated with the call and be able to identify the customer by satisfying the requirements in § 64.1200(n)(4)-(5), and

(iii) be unable to establish a verified association between the customer and the telephone number used for a call.

(3) ***C-level attestations.*** To authenticate the caller identification information of a call with a C-level attestation, a voice service provider shall, consistent with the STIR/SHAKEN authentication framework:

(i) not be responsible for the origination of a call onto the IP network, or

(ii) not have a direct, authenticated relationship with the customer associated with the call or be able to identify the customer.

(c) ***Third-party authentication.*** An originating or intermediate provider may fulfill its obligations to authenticate caller identification information under paragraphs (a)(2)-(3) of this section by entering into an agreement with a third-party authentication service, provided that the provider:

(1) requires the third party to sign all calls using the certificate obtained by the provider in

accordance with paragraph (a)(1)(ii) of this section;

(2) makes all attestation-level decisions regarding the caller identification information of each call in accordance with paragraph (b);

(3) memorializes the agreement between it and the third party for the authentication service in writing, which must:

(i) specify the tasks that the third-party authentication service will perform on the provider's behalf, and

(ii) confirm that the provider shall make all attestation-level decisions for calls signed pursuant to the agreement, and that all calls shall be signed using the provider's Secure Telephone Identity certificate;

(4) maintains any agreement entered into pursuant to paragraph (d)(3) of this section for as long as any third-party authentication arrangement exists; and

(5) retains a copy of any agreement entered into pursuant to paragraph (d)(3) of this section for a period of two (2) years from the end or termination of the agreement.

(d) ***Attestation requirements for voice service providers serving end users directly.*** A voice service provider that serves end users directly shall make all attestation-level decisions regarding the caller identification information of each of its end users' SIP calls consistent with paragraph (b) of this section, regardless of whether it has a STIR/SHAKEN implementation obligation.

(e) ***Prohibition on elective non-IP routing.*** A voice service provider shall not intentionally cause a call to be routed over a network that does not support the transmission of authenticated caller identification information when it has the technical ability to cause the call to be routed over a network that does support the transmission of authenticated caller identification information.

(f) ***Implementation extensions and exemptions.***

(1) ***Annual review of undue hardship extensions.*** The Wireline Competition Bureau shall, in conjunction with an assessment of burdens and barriers to implementation of caller identification authentication technology, annually review the scope of all previously granted undue hardship extensions and, after issuing a Public Notice seeking comment, may extend or decline to extend each such extension, and may decrease the scope of entities subject to a further extension.

(2) ***Non-IP networks extension.*** Those portions of a voice service provider's network that rely on technology that cannot initiate, maintain, carry, process, and terminate SIP calls are deemed subject to a continuing extension. A voice service provider subject to the foregoing extension shall comply with the requirements of § 64.6303(a) as to the portion of its network subject to the extension.

(3) ***Non-facilities-based provider exemption.*** A voice service provider is exempt from implementing the STIR/SHAKEN authentication framework as described in paragraph (a) of this section to the extent that it is a non-facilities-based provider for a given call.

7. Remove and reserve § 64.6302.
8. Revise § 64.6303 to read as follows:

§ 64.6303 Caller ID authentication in non-IP networks.

(a) A voice service provider shall either:

(1) Upgrade its entire network to allow for the origination, carrying, processing and termination, as applicable, of SIP calls and fully implement the STIR/SHAKEN authentication framework as required in § 64.6301 throughout its network; or

(2) Maintain and be ready to provide the Commission on request with documented proof that it is

participating, either on its own or through a representative, including third party representatives, as a member of a working group, industry standards group, or consortium that is working to develop a non-Internet Protocol caller identification authentication solution, or actively testing such a solution.

9. Remove and reserve § 64.6304.

10. Amend § 64.6305 to read as follows:

§ 64.6305 Robocall mitigation and certification.

(a) ***Robocall mitigation program requirements.*** Each voice service provider shall implement an appropriate robocall mitigation program that shall include:

(1) reasonable steps to prevent its network or services from being used to transmit illegal robocalls; and

(2) a commitment:

(i) to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium; and

(ii) to cooperate with such entities in investigating and stopping any person or entity from using the voice service provider's network or services to transmit illegal robocalls.

(b) ***Certification in the Robocall Mitigation Database.***

(1) A voice service provider shall certify that all of the calls its network or services transmit are subject to a robocall mitigation program consistent with paragraph (a) of this section, that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission.

(2) A facilities-based voice service provider shall certify to one of the following:

(i) It has fully implemented the STIR/SHAKEN authentication framework across its entire network and services and all calls it transmits are compliant with § 64.6301;

(ii) It has implemented the STIR/SHAKEN authentication framework on a portion of its network and services and all calls it transmits on that portion of its network are compliant with § 64.6301; or

(iii) It has not implemented the STIR/SHAKEN authentication framework on any portion of its network.

(3) A voice service provider that serves end users directly shall certify that it is compliant with the attestation requirements in § 64.6301(b) for all calls it transmits on its services.

(4) A voice service provider shall include the following information in its certification in English or with a certified English translation:

(i) If it is has certified that it has not implemented the STIR/SHAKEN authentication framework on any portion of its network pursuant to paragraphs (b)(2)(i) or (b)(2)(ii) of this section, identification of the exemption(s) or extension(s) the voice service provider received under § 64.6301(f) for the that portion of the network, if the voice service provider is not a foreign voice service provider, and the basis for the exemption(s) or extension(s);

(ii) The specific reasonable steps the voice service provider has taken to prevent its network or services from being used to transmit illegal robocalls as part of its robocall mitigation program, including a description of how it complies with its obligation to know its customers and/or know its upstream providers, as applicable, pursuant to § 64.1200(n)(4)-(5), the analytics system(s) it uses to identify and block illegal traffic, including whether it uses any third-party analytics vendor(s) and the name(s) of such vendor(s);

(iii) A statement of the voice service provider's commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its network or services to transmit illegal robocalls; and

(iv) State whether, at any time in the prior two years, the filing entity (and/or any entity for which the filing entity shares common ownership, management, directors, or control) has been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description; and, if so, provide a description of any such action or investigation, including all law enforcement or regulatory agencies involved, the date that any action or investigation was commenced, the current status of the action or investigation, a summary of the findings of wrongdoing made in connection with the action or investigation, and whether any final determinations have been issued.

(6) A voice service provider filing a certification pursuant to paragraph (b) of this section shall submit the following information in the Robocall Mitigation Database:

(i) The voice service provider’s business name(s) and primary address;

(ii) Other business names in use by the voice service provider;

(iii) All business names previously used by the voice service provider;

(iv) Whether the voice service provider is a foreign voice service provider;

(v) The name, title, department, business address, telephone number, and email address of one person within the company responsible for addressing robocall mitigation-related issues;

(vi) Whether or not the voice service provider has a STIR/SHAKEN authentication framework implementation obligation;

(vii) Whether the voice service provider:

(A) Is a facilities-based provider that:

(*1*) Is an originating or terminating voice service provider directly serving end users;

(*2*) Is an originating or terminating provider acting as a wholesale provider originating or terminating calls on behalf of another provider or providers;

(*3*) Is a gateway provider; and/or

(*4*) Is a non-gateway intermediate provider; or

(B) Is a non-facilities-based provider; and

(viii) The voice service provider’s OCN, if it has one.

(5) All certifications made and information submitted pursuant to paragraph (b) of this section shall:

(i) Be filed in the Robocall Mitigation Database; and

(ii) Be signed by an officer in conformity with § 1.16.

(7) A voice service provider shall update its filings within ten (10) business days of any change to the information it must provide pursuant to paragraph (b) of this section.

(i) A voice service provider that has been aggrieved by a Governance Authority decision to revoke that voice service provider's SPC token need not update its filing on the basis of that revocation until the sixty (60)-day period to request Commission review pursuant to § 64.6308(b)(1), following completion of the Governance Authority's formal review process, expires or, if the aggrieved voice service provider files an appeal, until ten (10) business days after the Wireline Competition Bureau releases a final decision pursuant to § 64.6308(d)(1).

(ii) If a voice service provider elects not to file a formal appeal of the Governance Authority decision to revoke that voice service provider's SPC token, the provider need not update its filing on the basis of that revocation until the thirty (30) day period to file a formal appeal with the Governance Authority Board expires.

(c) ***Intermediate and terminating voice service provider obligations —***

(1) ***Accepting calls from domestic voice service providers.*** Intermediate and terminating providers shall accept calls directly from a domestic voice service provider only if that domestic voice service provider's filing appears in the Robocall Mitigation Database in accordance with paragraph (b) of this section, showing that the voice service provider has affirmatively submitted the filing, and that filing has not been de-listed pursuant to an enforcement action.

(2) ***Accepting calls from foreign voice service providers.*** Intermediate and terminating providers shall accept calls directly from a foreign voice service provider that uses North American Numbering Plan resources in the caller identification field to send voice calls to residential or business subscribers in the United States, only if that foreign voice service provider's filing appears in the Robocall Mitigation Database in accordance with paragraph (b) of this section, showing that the foreign voice service provider has affirmatively submitted the filing, and that filing has not been de-listed pursuant to an enforcement action.

(3) ***Public safety safeguards.*** Notwithstanding paragraph (c)(1) and (2):

(i) A provider may not block a voice call under any circumstances if the call is an emergency call placed to 911; and

(ii) A provider must make all reasonable efforts to ensure that it does not block any calls from public safety answering points and government emergency numbers.

(d) ***Annual Recertification Requirement.*** In accordance with this section and § 1.16, all providers shall certify annually, on or before March 1, that any information submitted to the Robocall Mitigation Database is true and correct.

11. Remove and reserve § 64.6306.

12. Revise § 64.6307 to read as follows:

§ 64.6307 Line item charges.

(a) Voice service providers are prohibited from adding any additional line item charges to consumer or small business customer subscribers for the effective caller identification authentication technology required by § 64.6301 and § 64.6303.

(1) For purposes of this section, "consumer subscribers" means residential mass-market subscribers.

(2) For purposes of this section, "small business customer subscribers" means subscribers that are business entities that meet the size standards established in 13 CFR part 121, subpart A.

13. Revise § 64.6308 to read as follows:

§ 64.6308 Review of Governance Authority Decision to Revoke an SPC Token.

(a) ***Parties permitted to seek review of Governance Authority decision.***

(1) Any voice service provider aggrieved by a Governance Authority decision to revoke that voice service provider's SPC token, must seek review from the Governance Authority and complete the appeals process established by the Governance Authority prior to seeking Commission review.

(2) Any voice service provider aggrieved by an action to revoke its SPC token taken by the Governance Authority, after exhausting the appeals process provided by the Governance Authority, may then seek review from the Commission, as set forth in this section.

(b) ***Filing deadlines.***

(1) A voice service provider requesting Commission review of a Governance Authority decision to revoke that voice service provider's SPC token by the Commission, shall file such a request electronically in the Electronic Comment Filing System (ECFS) in WC Docket No. 21-291, Appeals of the STIR/SHAKEN Governance Authority Token Revocation Decisions within sixty (60) days from the date the Governance Authority upholds it token revocation decision.

(2) Parties shall adhere to the time periods for filing oppositions and replies set forth in § 1.45.

(c) ***Filing requirements.***

(1) A request for review of a Governance Authority decision to revoke a voice service provider's SPC token by the Commission shall be filed in WC Docket No. 21-291, Appeals of the STIR/SHAKEN Governance Authority Token Revocation Decisions, in the Electronic Comment Filing System (ECFS). The request for review shall be captioned "In the matter of Request for Review by (name of party seeking review) of Decision of the Governance Authority to Revoke an SPC Token."

(2) A request for review shall contain:

(i) A statement setting forth the voice service provider's asserted basis for appealing the Governance Authority's decision to revoke the SPC token;

(ii) A full statement of relevant, material facts with supporting affidavits and documentation, including any background information the voice service provider deems useful to the Commission's review; and

(iii) The question presented for review, with reference, where appropriate, to any underlying Commission rule or Governance Authority policy.

(3) A copy of a request for review that is submitted to the Commission shall be served on the Governance Authority by the voice service provider requesting Commission review via *sti-ga@atis.org* or in accordance with any alternative delivery mechanism the Governance Authority may establish in its operating procedures.

(d) ***Review by the Wireline Competition Bureau.***

(1) Except in extraordinary circumstances, final action on a request for review of a Governance Authority decision to revoke a voice service provider's SPC token should be expected no later than one hundred and eighty (180) days from the date the request for review is filed in the Electronic Comment Filing System (ECFS) pursuant to § 64.6308(b)(1). The Wireline Competition Bureau shall have the discretion to pause the one hundred and eighty (180)-day review period in situations where actions outside the Wireline Competition Bureau's control are responsible for delaying review of a request for review.

(2) An affected party may seek review of a decision issued under delegated authority by the

Wireline Competition Bureau pursuant to the rules set forth in § 1.115.

(e) ***Standard of review.*** The Wireline Competition Bureau shall conduct *de novo* review of Governance Authority decisions to revoke a voice service provider's SPC token.

(f) ***Status during pendency of a request for review and a Governance Authority decision.***

(1) A voice service provider shall not be considered to be in violation of the Commission's caller identification authentication rules under § 64.6301 after revocation of its SPC token by the Governance Authority until the thirty (30) day period to file a formal appeal with the Governance Authority Board expires, or during the pendency of any formal appeal to the Governance Authority Board.

(2) A voice service provider shall not be considered to be in violation of the Commission's caller identification authentication rules under § 64.6301 after the Governance Authority Board upholds the Governance Authority's SPC token revocation decision until the sixty (60) day period to file a request for review with the Commission expires.

(3) When a voice service provider has sought timely Commission review of a Governance Authority decision to revoke a voice service provider's SPC token under this section, the voice service provider shall not be considered to be in violation of the Commission's caller identification authentication rules under § 64.6301 until and unless the Wireline Competition Bureau, pursuant to paragraph (d)(1) of this section, has upheld or otherwise decided not to overturn the Governance Authority's decision.

(4) In accordance with §§ 1.102(b) and 1.106(n), the effective date of any action pursuant to paragraph (d) of this section shall not be stayed absent order by the Wireline Competition Bureau or the Commission.

14. Add § 64.6309 to read as follows:

§ 64.6309 Governance Authority Policies

(a) ***SPC Token Issuance and Revocations Policies.***

(1) The Governance Authority shall adopt a policy that includes affirmative, effective measures to prevent voice service providers that are issued SPC tokens from transmitting calls that are not in compliance with the STIR/SHAKEN authentication framework, the Commission's STIR/SHAKEN rules, or the Governance Authority's policies, including the requirements in § 64.1200(n)(5)(i)-(iii).

(2) The Governance Authority shall adopt a policy to review all information it receives concerning an SPC token holder and its conduct, further investigate the SPC token holder and its conduct when there is a reasonable basis for believing the SPC token holder is not or is unlikely to be in compliance with the STIR/SHAKEN authentication framework, the Commission's STIR/SHAKEN rules, and/or the Governance Authority's policies, and deny or revoke an SPC token when it concludes that the SPC token is not in compliance or is not likely to comply with such requirements.

(b) ***Selection of Secure Telephone Identity Certification Authorities.***

(1) The Governance Authority shall adopt a policy that includes affirmative, effective measures to prevent Certification Authorities from failing to comply with the STIR/SHAKEN authentication framework, the Commission's STIR/SHAKEN rules, or the Governance Authority's policies, including the requirements in § 64.1200(n)(5)(i)-(iii).

(2) The Governance Authority shall adopt a policy to review all information it receives concerning a Certification Authority and its conduct, further investigate the Certification Authority and its conduct when there is a reasonable basis for believing the Certification Authority has violated or may violate the STIR/SHAKEN authentication framework, the

Commission's STIR/SHAKEN rules, and/or the Governance Authority's policies, and deny or remove the Certification Authority when it concludes that the Certification Authority holder is not in compliance or is not likely to comply with such requirements.

(c) ***Information Collection.*** The Governance Authority shall establish measures to regularly obtain from the industry traceback consortium and call analytics providers information about SPC token holder and Certification Authority conduct.

(d) ***Reporting.*** The Governance Authority shall report to the Commission on no less than a quarterly basis information about its enforcement activity, including complaints it has received, investigations it has initiated and concluded, and decisions concerning SPC token revocations and Certification Authority removals, including any reports documenting the Governance Authority's final determinations.

APPENDIX B

Initial Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[1] the Federal Communications Commission (Commission) has prepared this Initial Regulatory Flexibility Analysis (IRFA) of the policies and rules proposed in the *Further Notice of Proposed Rulemaking* (*FNPRM*) assessing the possible significant economic impact on a substantial number of small entities. The Commission requests written public comments on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments specified on the first page of the *FNPRM*. The Commission will send a copy of the *FNPRM*, including this IRFA, to the Chief Counsel for the Small Business Administration (SBA) Office of Advocacy.[2] In addition, the *FNPRM* and IRFA (or summaries thereof) will be published in the Federal Register.[3]

A. Need for, and Objectives of, the Proposed Rules

2. The Commission has adopted a number of tools aimed at stopping unlawful and fraudulent calls, but these tools rely on proper implementation by responsible providers in the ecosystem. In furtherance of the Commission's mission to bring consumers meaningful relief from illegal calls and restore trust in voice communications, the *FNPRM* proposes measures to ensure all voice service providers are fulfilling their obligations to protect consumers from illegal calls through their implementation of the STIR/SHAKEN authentication framework. The STIR/SHAKEN framework, which is designed to deter number spoofing and supports other tools to combat illegal calls, is built on an expectation that providers will properly authenticate calls. Available evidence suggests that some providers have not implemented the framework consistently. We propose measures to address implementation issues, and thereby enhance STIR/SHAKEN, by preventing providers from transmitting calls when they fail to properly implement the framework, ensuring providers properly attest calls using the framework, and closing loopholes that are preventing ubiquitous and consistent deployment of the framework in providers' IP networks. Specifically, we: (1) propose that providers follow baseline measures to fulfill their obligation to know their upstream providers and that the STIR/SHAKEN Governance Authority improve its policies for authorizing providers to authenticate calls using the framework;[4] (2) propose to require that providers follow know-your-customer (KYC) and know-your-upstream-provider (KYUP) requirements when making attestation-level decisions and prohibit improper attestations;[5] (3) propose to close implementation loopholes by clarifying definitions, repealing implementation exemptions, requiring voice service providers closest to end users to authenticate calls, and implementing measures to increase the number of calls that arrive at terminating providers with caller ID authentication information;[6] (4) seek comment on how these and other measures will address illegal foreign-originated calls;[7] (5) propose and seek comment on how to hold providers accountable to these proposed requirements and any existing requirements;[8] and (6) propose steps to ease providers'

[1] 5 U.S.C. §§ 601 *et seq*., as amended by the Small Business Regulatory Enforcement and Fairness Act (SBREFA), Pub. L. No. 104-121, 110 Stat. 847 (1996).

[2] *Id.* § 603(a).

[3] *Id*.

[4] *See supra* Section III.A.

[5] *See supra* Section III.B.

[6] *See supra* Section III.C.

[7] *See supra* Section III.D.2.

[8] *See supra* Section III.E.1.

compliance with the Commission's caller ID authentication rules and improve their administrability.[9]

B. Legal Basis

3. The proposed action is authorized pursuant to sections 4(i), 4(j), 201, 202, 217, 227, 227b, 251(e), 303(r), 403, 501, 502, and 503 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 154(i), 154(j), 201, 202, 217, 227, 227b, 251(e), 303(r), 403, 501, 502, and 503.

C. Description and Estimate of the Number of Small Entities to Which the Proposed Rules Will Apply

4. The RFA directs agencies to provide a description of and, where feasible, an estimate of the number of small entities that may be affected by the proposed rules, if adopted.[10] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[11] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act.[12] A "small business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.[13] The SBA establishes small business size standards that agencies are required to use when promulgating regulations relating to small businesses; agencies may establish alternative size standards for use in such programs, but must consult and obtain approval from SBA before doing so.[14]

5. Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe three broad groups of small entities that could be directly affected by our actions.[15] In general, a small business is an independent business having fewer than 500 employees.[16] These types of small businesses represent 99.9% of all businesses in the United States, which translates to 34.75 million businesses.[17] Next, "small organizations" are not-for-profit enterprises that are independently owned and operated and not dominant in their field.[18] While we do not have data regarding the number of non-profits that meet that criteria, over 99 percent of nonprofits have fewer than 500 employees.[19] Finally, "small governmental jurisdictions" are defined as cities, counties, towns, townships, villages, school districts, or special districts with populations of less than fifty thousand.[20] Based on the 2022 U.S.

---

[9] *See supra* Section III.E.3.

[10] 5 U.S.C. § 603(b)(3).

[11] *Id*. § 601(6).

[12] *Id*. § 601(3) (incorporating by reference the definition of "small-business concern" in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register."

[13] 15 U.S.C. § 632.

[14] 13 CFR § 121.903.

[15] 5 U.S.C. § 601(3)-(6).

[16] *See* SBA, Office of Advocacy, *Frequently Asked Questions About Small Business* (July 23, 2024), https://advocacy.sba.gov/wp-content/uploads/2024/12/Frequently-Asked-Questions-About-Small-Business_2024-508.pdf.

[17] *Id*.

[18] 5 U.S.C. § 601(4).

[19] *See* SBA, Office of Advocacy, *Small Business Facts, Spotlight on Nonprofits* (July 2019), https://advocacy.sba.gov/2019/07/25/small-business-facts-spotlight-on-nonprofits/.

[20] 5 U.S.C. § 601(5).

Census of Governments data, we estimate that at least 48,724 out of 90,835 local government jurisdictions have a population of less than 50,000.[21]

6. The rules proposed in the *FNPRM* will apply to small entities in the industries identified in the chart below by their six-digit North American Industry Classification System (NAICS)[22] codes and corresponding SBA size standard.[23] Where available, we also provide additional information regarding the number of potentially affected entities in the industries identified below.

Table 1. 2022 U.S. Census Bureau Data by NAICS Code

Regulated Industry (Footnotes specify potentially affected entities within a regulated industry where applicable)	NAICS Code	SBA Size Standard	Total Firms[24]	Total Small Firms[25]	% Small Firms
Wired Telecommunications Carriers[26]	517111	1,500 employees	3,403	3,027	88.95%
Wireless Telecommunications Carriers (except Satellite)[27]	517112	1,500 employees	1,184	1,081	91.30%
Telecommunications Resellers[28]	517121	1,500 employees	955	847	88.69%
Satellite Telecommunications	517410	$44 million	332	195	58.73%

[21] *See* U.S. Census Bureau, 2022 Census of Governments –Organization, https://www.census.gov/data/tables/2022/econ/gus/2022-governments.html, tables 1-11.

[22] The North American Industry Classification System (NAICS) is the standard used by Federal statistical agencies in classifying business establishments for the purpose of collecting, analyzing, and publishing statistical data related to the U.S. business economy. *See* www.census.gov/NAICS for further details regarding the NAICS codes identified in this chart.

[23] The size standards in this chart are set forth in 13 CFR § 121.201, by six digit North American Industrial Classification System (NAICS) code.

[24] *U.S. Census Bureau*, "*Selected Sectors: Employment Size of Firms for the U.S.: 2022*." Economic Census, ECN Core Statistics Economic Census: Establishment and Firm Size Statistics for the U.S., Table EC2200SIZEEMPFIRM, 2025, *and* "*Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2022*." Economic Census, ECN Core Statistics Economic Census: Establishment and Firm Size Statistics for the U.S., Table EC2200SIZEREVFIRM, 2025.

[25] *Id.*

[26] Affected Entities in this industry include Carrier RespOrgs, Competitive Access Providers, Cable System Operators (Telecom Act Standard), Competitive Local Exchange Carriers (CLECs), Competitive Local Service Providers, Facilities-Based Carriers (International Telecom Carriers), Incumbent Local Exchange Carriers (Incumbent LECs), Interexchange Carriers (IXCs), and Local Exchange Carriers (LECs).

[27] Affected Entities in this industry include Carrier RespOrgs, Wireless Carriers and Service Providers, and Wireless Telephony.

[28] Affected Entities in this industry include Carrier RespOrgs, Local Resellers, Prepaid Calling Card Providers, Toll Resellers, and Wireless Resellers.

Regulated Industry (Footnotes specify potentially affected entities within a regulated industry where applicable)	NAICS Code	SBA Size Standard	Total Firms[24]	Total Small Firms[25]	% Small Firms
All Other Telecommunications[29]	517810	$40 million	1,673	1,007	60.19%

Table 2. Telecommunications Service Provider Data

2024 Universal Service Monitoring Report Telecommunications Service Provider Data [30] (Data as of December 2023)	SBA Size Standard (1500 Employees)		
Affected Entity	**Total # FCC Form 499A Filers**	**Small Firms**	**% Small Entities**
Competitive Local Exchange Carriers (CLECs)[31]	3,729	3,576	95.90
Incumbent Local Exchange Carriers (Incumbent LECs)	1,175	917	78.04
Interexchange Carriers (IXCs)	113	95	84.07
Local Exchange Carriers (LECs)[32]	4,904	4,493	91.62
Local Resellers	222	217	97.75
Toll Resellers	411	398	96.84
Telecommunications Resellers	633	615	97.16
Wired Telecommunications Carriers[33]	4,682	4,276	91.33
Wireless Telecommunications Carriers (except Satellite)[34]	585	498	85.13

[29] Affected Entities in this industry include Non-Carrier RespOrgs and Telecommunications Relay Service (TRS) Providers.

[30] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2024), https://docs.fcc.gov/public/attachments/DOC-408848A1.pdf.

[31] Affected Entities in this industry include all reporting local competitive service providers.

[32] Affected Entities in this industry include all reporting fixed local service providers (CLECs & ILECs).

[33] Local Resellers fall into another U.S. Census Bureau industry (Telecommunications Resellers) and therefore data for these providers is not included in this industry.

[34] Affected Entities in this industry include all reporting wireless carriers and service providers.

2024 Universal Service Monitoring Report Telecommunications Service Provider Data [30] **(Data as of December 2023)**	**SBA Size Standard (1500 Employees)**		
Affected Entity	**Total # FCC Form 499A Filers**	**Small Firms**	**% Small Entities**
Wireless Telephony[35]	326	247	75.77

Table 3. Cable Entities Data

Cable Entities	Size Standard	Total Firms	Small Firms	% Small Firms in Industry
Cable System Operators (Telecom Act Standard) Small Cable Operator	Serves fewer than 498,000 subscribers, either directly or through affiliates[36] [37]	530[38]	524[39]	98.87%

D. Description of Economic Impact and Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

7. The RFA directs agencies to describe the economic impact of proposed rules on small entities, as well as projected reporting, recordkeeping, and other compliance requirements, including an estimate of the classes of small entities which will be subject to the requirements and the type of professional skills necessary for preparation of the report or record.[40]

8. The *FNPRM* proposes measures that may involve new or additional compliance and recordkeeping requirements for small and other providers. Specifically, we propose to require that providers adopt specific measures to fulfill their existing KYUP obligations, including onboarding, due diligence, compliance review, monitoring, and remediation measures.[41] Upon the effective date of the rules, providers would be required to comply with these obligations with respect to new and renewing

[35] Affected Entities in this industry include Cellular/PCS/SMR - Specialized Mobile Radio Licensees and SMR (Dispatch).

[36] Pursuant to 47 U.S.C. § 543(m)(2) of the Communications Act of 1934, as amended, the size standard for a "small cable operator," is a cable operator that, directly or through an affiliate, serves in the aggregate fewer than 1% of all U.S. subscribers and has no affiliation with entities with gross annual aggregate revenues exceed $250,000,000.

[37] *FCC Announces Updated Subscriber Threshold for the Definition of Small Cable Operator*, Public Notice, DA 23-906 (MB 2023) (*2023 Subscriber Threshold PN*). In the Public Notice, the Commission determined that there were approximately 49.8 million cable subscribers in the United States at that time using the most reliable source publicly available. This threshold will remain in effect until the Commission issues a superseding Public Notice. *See* 47 CFR § 76.901(e)(1).

[38] Based on Commission staff review of S&P Global Market Intelligence, S&P Capital IQ Pro, U.S., *Broadband & Video Subscribers by Geography Q3-2025(June 2025)* data. (last visited Sept. 15, 2025).

[39] *Id.*

[40] 5 U.S.C. § 603(b)(4).

[41] *See supra* Section III.A.1.

upstream providers, and would have an additional 6 months after the effective date of the rules to complete the KYUP onboarding review for existing upstream providers.[42] We further propose that providers retain the information they collect in connection with this requirement for four years and that they report to the Commission and STIR/SHAKEN Governance Authority any upstream provider they believe may be using their network or services to transmit illegal calls.[43] We propose requiring providers use KYC and KYUP information to attest the calls they authenticate using the STIR/SHAKEN framework, and prohibit them from improperly authenticating calls.[44] Additionally, we propose to require that all intermediate providers authenticate any unauthenticated SIP calls they receive,[45] which is a capability that most intermediate providers should already have; propose to prohibit providers from originating or routing calls over non-IP networks with the intent thereby to strip caller ID authentication information;[46] and propose to require that providers block unauthenticated SIP calls.[47]

9. In the *FNPRM*, we seek comment on the costs and benefits of its proposals and inquiries, with specific regard to any potential compliance costs and burdens on small providers, including costs associated with collecting additional information, increasing monitoring, data retention, independent audits, or other operational costs that may result from these proposals. We believe some of these measures will have an economic impact on certain providers by reducing their revenue as result of the reduction in the number of unlawful calls that transverse the voice network, but that those costs may be made up by legitimate callers who regain trust in the voice network. We do not believe the the KYUP requirements costs will not be unreasonably burdensome for most small providers that are good actors who likely collect some of this information as part of their existing obligations. We believe that small providers in most cases either serve end users directly and therefore will not have to perform the KYUP requirements, or interconnect directly with large providers that are easily able to demonstrate their legitimacy. The proposed measures are largely geared toward clarifying and enhancing the compliance expectations that providers already have under existing rules, which should minimize the costs and burdens on providers that have already implemented existing requirements properly or meaningfully. We believe that certain KYC requirements will only apply to small and other providers that choose to enter into certain business relationships and that the burden is reasonable relative to the potential benefits in deterring illegal calls. We also propose to codify a base forfeiture amounts of $2,500 per call for calls resulting from a failure to follow KYUP requirements, $1,000 on a per call basis for violations of rules involving improper call attestations and an unauthenticated calls; and $2,500, on a continuing violation basis, for providers who have failed to implement STIR/SHAKEN and are not subject to any exemption. Small providers that have not already implemented adequate measures to know their upstream providers, or who need to develop procedures for retaining and reporting such information, may need to hire professionals, such as consultants, attorneys, or third parties to comply with these requirements.

10. With regard to the STIR/SHAKEN implementation exemptions, we propose to repeal the two remaining exemptions for small and other providers, and seek comment on potential hardship exemptions.[48] We believe all voice providers are able to obtain SPC tokens without undue hardship, and propose to repeal the extension for providers to obtain this token. Further, we believe small providers that originate calls via satellite using North American Numbering Plan (NANP) numbers are able to implement STIR/SHAKEN without undue hardship, and propose to repeal the extension for such providers. We seek comment on whether undue hardship extensions should be granted for

[42] *See supra* Section III.A.1.

[43] *See supra* Section III.A.2.

[44] *See supra* Section III.B.

[45] *See supra* Section III.C.4.

[46] *See supra* Section III.C.4.

[47] *See supra* Section III.C.4.

[48] *See supra* Section III.C.2.

telecommunications relay service (TRS) providers if they satisfy the definition of "voice service provider."[49] We believe that the burden on intermediate providers authenticating calls will be minimal because most of these providers should already have the ability to authenticate calls. We also believe our proposal to prohibit intentional stripping of authentication information should not affect lawful providers. Additionally, we believe providers should already have the ability to block unauthenticated calls, as they are already required to block other calls under certain circumstances. To the extent the reduction of illegal calls has an impact on providers, we believe these losses will be made up by increased trust and use of the voice network.

E. Discussion of Significant Alternatives Considered That Minimize the Significant Economic Impact on Small Entities

11. The RFA directs agencies to provide a description of any significant alternatives to the proposed rules that would accomplish the stated objectives of applicable statutes, and minimize any significant economic impact on small entities.[50] The discussion is required to include alternatives such as: "(1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the rule for such small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof, for such small entities."[51]

12. We seek comment in the *FNPRM* on alternatives that may accomplish the Commission's objectives of stopping unlawful and fraudulent calls, while potentially minimizing the economic impact on small providers. Specifically, we seek comment on whether we should reduce the KYUP requirements, or whether there are alternatives to the proposed information collection, compliance review, information verification, and monitoring obligations that would allow small providers flexibility to identify bad actors.[52] This includes whether to direct providers to adopt KYUP best practices based on existing resources, or give them a safe harbor for such adoption, instead of requiring them to adopt detailed obligations that small and other providers must follow. We also seek comment on whether we should allow for the use of third-party KYUP services, and if so, whether they would help reduce compliance burdens for small providers.[53] Small entities are encouraged to bring to the Commission's attention any specific concerns they may have with the proposals detailed in the *FNPRM* and outline any additional alternatives that would accomplish the objectives of this proceeding.

F. Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rules

13. None.

---

[49] *See supra* Section III.D.

[50] 5 U.S.C. § 603(c).

[51] *Id.* § 603(c)(1)-(4).

[52] *See supra* Section III.A.1.

[53] *See supra* Section III.A.1.