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

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Call Authentication Trust Anchor | ) | WC Docket No. 17-97 |

# NOTICE OF PROPOSED RULEMAKING

**Adopted: April 28, 2025** **Released: April 29, 2025**

**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: Chairman Carr issuing a statement.

## TABLE OF CONTENTS



## I. INTRODUCTION

1. Today, we initiate the next step in our efforts to protect Americans from illegally spoofed robocalls by proposing to address the caller ID authentication gap resulting from non-Internet Protocol (IP) networks. Illegal robocalls continue to burden and harm the public. Victims of robocall-based scams lose hundreds to thousands of dollars,[1] with examples of single-instance losses approaching $10,000.[2]

[1] *See* FTC, Consumer Sentinel Network Data Book at 12 (2024), https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf (reporting a median loss by individuals of $1,480); Hiya, State of the Call 2024 at 21 (2024), https://www.hiya.com/state-of-the-call (reporting an average loss of victims of $865).

[2] *See 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 Report and Order and Further Notice of Proposed Rulemaking*).

Collectively, these numbers can reach $850 million annually.[3] Wasted time, nuisance, and fraud altogether drained an estimated $13.5 billion out of the U.S. economy in 2020 alone.[4] Robocalls disrupt Americans' lives more than a dozen times a month on average.[5] The resulting erosion of confidence in the nation's telephone network has spurred the Commission, at the direction of Congress,[6] to combat illegal robocalling campaigns through various means. These include requiring providers to implement the STIR/SHAKEN caller ID authentication framework,[7] establishing the Robocall Mitigation Database and robocall mitigation plan filing requirements,[8] adopting rules to target foreign-originated illegal robocalls,[9] and establishing other robocall mitigation and know-your-customer-style requirements.[10]

---

[3] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, GN Docket No. 17-59, Eighth Report and Order, FCC 25-15, at 2 (Feb. 28, 2025) (*Call Blocking Eighth Report and Order*).

[4] *First Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking*, 35 FCC Rcd at 3263, paras. 47-48.

[5] Hiya, State of the Call 2024 at 6 (2024) (estimating an average number of calls per person of 13); YouMail, *Historical Robocalls by Time*, https://robocallindex.com/history/time (last visited Apr. 23, 2025) (reporting an average number of calls per month and per person of 14.2 so far in 2025).

[6] Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105, § 4(b)(1)(B) (2019) (TRACED Act).

[7] *See, e.g.*, *First Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking*, 35 FCC Rcd at 3243, para. 3 (requiring voice service providers to implement STIR/SHAKEN in their IP networks); *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, Fifth Report and Order, Order on Reconsideration, Order, Seventh Further Notice of Proposed Rulemaking, and Fifth Further Notice of Proposed Rulemaking, 37 FCC Rcd 6865, 6886, para. 51 (2022) (*Gateway Provider Report and Order and Further Notice of Proposed Rulemaking*) (expanding STIR/SHAKEN obligations to gateway providers); *Call Authentication Trust Anchor*, WC Docket No. 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd 2573, 2581, para. 15 (2023) (*Sixth Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking*) (expanding STIR/SHAKEN obligations to non-gateway intermediate providers); *Call Authentication Trust Anchor*, WC Docket No. 17-97, Eighth Report and Order, FCC 24-120 (Nov. 22, 2024) (*Eighth Caller ID Authentication Report and Order*) (establishing defined rules for providers who rely on third parties to satisfy their STIR/SHAKEN implementation obligations).

[8] *See Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, 36 FCC Rcd 1859, 1902, para. 82 (2020) (*Second Caller ID Authentication Report and Order*); *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, FCC 24-135 (Jan. 8, 2025).

[9] *See generally Gateway Provider Report and Order and Further Notice of Proposed Rulemaking*.

[10] *See, e.g.*, *Advanced Methods to Target and Eliminate Unlawful Robocalls, Alarm Industry Communications Committee Petition for Reconsideration, American Dental Association Petition for Reconsideration*, CG Docket No. 17-59, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking, 35 FCC Rcd 7614 (2020) (adopting two call blocking safe harbors and additional protections for lawful callers); *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Fourth Report and Order, 35 FCC Rcd 15211 (2020) (adopting affirmative obligations for providers, including traceback, robocall mitigation, and know-your-customer-style requirements, as well as expanding one blocking safe harbor and adopting enhanced transparency and redress requirements); *Sixth Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking*, 38 FCC Rcd at 2587, para. 26 (instituting additional certification requirements for non-gateway providers related to traceback requests); *Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Seventh Report and Order in CG Docket No. 17-59 and WC Docket No. 17-97, Eighth Further Notice of Proposed Rulemaking in CG Docket No. 17-59, and Third Notice of Inquiry in CG Docket No. 17-59, 38 FCC Rcd 5404, 5405-06, 5412, 5415, 5421, paras. 3, 21, 29, 49 (2023) (modifying the certification requirements established in the *Sixth Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking* and expanding previously adopted requirements to all

(continued….)

2. The STIR/SHAKEN caller ID authentication framework is one of the key tools at the Commission's disposal to combat illegal robocalls. Congress recognized this fact when it passed the TRACED Act, which directs the Commission to work diligently towards ubiquitous deployment of caller ID authentication technology.[11] Over the past five years, industry stakeholders have made great strides towards implementing STIR/SHAKEN across their networks. However, more work remains to achieve ubiquitous caller ID authentication.

3. Because STIR/SHAKEN only works in IP networks, non-IP technology at any point in the call path creates a gap in the caller ID authentication scheme that bad actors can exploit. The loss of STIR/SHAKEN information for calls that traverse non-IP networks significantly undermines the value of the framework as a whole—in many cases negating the value of the investment providers have made to authenticate their calls and leading to improper spam labeling or blocking by downstream providers.[12] Commission rules thus obligate providers to either upgrade their non-IP networks to IP or work toward developing an alternative caller ID authentication solution for non-IP networks.[13]

4. A complete IP transition remains the best solution to achieving ubiquitous caller ID authentication, as it will enable providers to implement STIR/SHAKEN without additional regulatory requirements. Many providers have made progress toward converting their networks to IP in the years since the Commission first promulgated STIR/SHAKEN rules. Progress on completing the IP transition continues to be a priority for the Commission, and we have recently undertaken efforts to reduce burdens for providers working to achieve this goal.[14]

5. While progress on the IP transition is paramount, the ongoing existence of non-IP technology in the phone network leaves the public vulnerable to illegal robocalling campaigns, prompting our efforts to explore whether additional requirements are necessary for providers that have not finished converting to all IP. Over the years, industry has developed and begun to utilize frameworks for authenticating calls on non-IP networks. We initiate this proceeding to evaluate whether any such non-IP caller ID authentication frameworks meet the requirements in the TRACED Act, and whether we should require providers who have not completed their IP transitions to implement one or more of these frameworks in their non-IP networks by a date certain.

## II. BACKGROUND

6. The Commission has long been at the forefront of efforts to protect the American public from illegal robocalls. In December 2019, to advance these efforts, Congress passed the TRACED Act,

(Continued from previous page)
categories of providers); *Call Blocking Eighth Report and Order* at 4-12, paras. 9-25 (expanding the requirement to block using a reasonable do not originate list to all providers in the call path and modifying the commissions requirement to provide immediate notification of blocking based on reasonable analytics to callers).

[11] *See* 47 U.S.C. § 227b(b)(5)(D) ("The Commission shall . . . 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.").

[12] Indeed, by some estimates, as many as 57.2% of calls that may be signed by the originating provider reach their destination unsigned. TransNexus, *STIR/SHAKEN statistics from January 2025* (Mar. 4, 2025), https://transnexus.com/blog/2025/shaken-statistics-february/ (indicating that only 42.8% of calls in the prior six months were signed at termination).

[13] 47 CFR § 64.6303.

[14] *See Technology Transitions*, GN Docket No. 13-5, Order on Clarification, DA 25-250 (Mar. 20, 2025) (*Technology Transitions Order on Clarification*); *Accelerating Wireline Broadband Deployment by Removing Barriers to Infrastructure Investment, Technology* Transitions, WC Docket No. 17-84, GN Docket No. 13-5, Order, DA 25-248 (Mar. 20, 2025) (*Discontinuance Waiver Order*); *Accelerating Wireline Broadband Deployment by Removing Barriers to Infrastructure Investment*, WC Docket No. 17-84, Order, DA 25-251 (Mar. 20, 2025) (*214 Grandfathering Order*); *Accelerating Wireline Broadband Deployment by Removing Barriers to Infrastructure Investment*, WC Docket No. 17-84, Order, DA 25-252 (Mar. 20, 2025) (*Network Change Waiver Order*).

which gave the Commission authority to implement new safeguards to stop robocalls.[15] Among them was a requirement that the Commission mandate that voice service providers institute caller ID authentication technology in their networks.[16] Caller ID authentication reduces fraud by enabling providers to verify that a caller's number matches the caller ID information transmitted with a call. This process informs providers' efforts to identify and block illegal robocalls and gives subscribers trust that callers are who they say they are.

7. For this purpose, Congress required the use of STIR/SHAKEN, a caller ID authentication framework comprised of several different standards and protocols, for IP networks.[17] The Internet Engineering Task Force (IETF), a standards development body that works with Internet users, network operators, and equipment vendors,[18] formed the working group that developed Secure Telephone Identity Revisited (STIR), which defined the protocols for authenticating caller ID information.[19] Because STIR allows for a variety of different implementation methods,[20] the Alliance for Telecommunication Industry Solutions (ATIS), a global technical standards planning and development organization,[21] in conjunction with the SIP Forum,[22] an industry association involved in development of Session Initiation Protocol (SIP) standards, developed Signature-based Handling of Asserted information using toKENs (SHAKEN). SHAKEN standardizes implementation of STIR across the industry.[23] The Commission requires providers obligated to implement STIR/SHAKEN to follow, at a minimum, ATIS-1000074, ATIS-1000080, and ATIS-1000084, and all documents referenced therein.[24] These documents, published and periodically amended by ATIS, establish both: (1) the technical requirements for authenticating calls; and (2) the governance system underlying STIR/SHAKEN.[25]

8. STIR/SHAKEN establishes how voice service providers can transmit encrypted information about a caller and its relationship to the phone number appearing in the caller ID field. When

[15] Section 4 of the TRACED Act, which addresses call authentication, is codified in 47 U.S.C. § 227b.

[16] 47 U.S.C. § 227b(b)(1).

[17] *Id.* § 227b(a)(1); *id.* § 227b(b)(1)(A).

[18] IETF, *Introduction to the IETF*, https://www.ietf.org/about/introduction/ (last visited Apr. 23, 2025).

[19] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1862-63, para. 7.

[20] ATIS, *SHAKEN: Frequently Asked Questions* at 1, https://sti-ga.atis.org/wp-content/uploads/2020/08/shaken-faq.pdf (last visited Apr. 23, 2025).

[21] ATIS, *ATIS Overview 2025* at 9 (2025), https://cdn.atis.org/atis.org/2025/03/13123524/2025-ATIS-Overview-V11-1.pdf.

[22] The SIP Forum is an industry association working to "foster interoperability and adherence to standardization efforts" based on Session Initiation Protocol technology. SIP Forum, *About the SIP Forum*, https://www.sipforum.org/about/mission-scope-and-structure/ (last visited Apr. 23, 2025).

[23] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1862-63, para. 7.

[24] *First Caller ID Authentication Report and 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"); *Gateway Provider Report and Order and Further Notice of Proposed Rulemaking*, 37 FCC Rcd at 6887-88, para. 53 ("Compliance by [gateway providers] with the most current 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."); *Sixth Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking*, 38 FCC Rcd at 2586, para. 22 ("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.").

[25] *Eighth Caller ID Authentication Report and Order* at 7, para. 9.

a subscriber places a call, the originating provider authenticates the call source and number.[26] The provider then adds encrypted identifying information about the caller, as well as the location of a public key used for its decoding, into the "Identity" header of the SIP INVITE, which is the network-level message used to initiate a SIP call.[27] The encrypted information travels with the call from the originating voice service provider, through any intermediate providers, and then to the terminating voice service provider, which can decrypt it, verify the caller ID information, and use that information to protect its subscribers from unwanted and illegal calls.[28] To ensure that providers can prove their identity and trustworthiness to participate in the STIR/SHAKEN framework, the framework also outlines a system of tokens issued and overseen by a neutral governance authority.[29] Under this system, a provider must "sign" the call by including a certificate in the Identity header used to validate its Personal Assertion Token (PASSporT).[30] A PASSporT acts as a digital signature attesting to the provider's identity and right to authenticate caller ID information.[31]

9. While effective,[32] STIR/SHAKEN only works in IP networks.[33] Although many providers exclusively use IP networks, some still rely on non-IP facilities.[34] When a call routes through a non-IP network segment, the STIR/SHAKEN information is stripped out, thereby creating gaps in the caller ID authentication scheme.[35] The TRACED Act therefore directs the Commission to mandate that providers implement STIR/SHAKEN in their IP networks while also requiring providers to "take reasonable measures to implement an effective call authentication framework in [their] non-[IP] networks."[36] Congress established a June 30, 2021 deadline for voice service providers to implement STIR/SHAKEN while simultaneously directing the Commission to provide extensions based on undue

[26] *See id.* at 8, para. 10.

[27] *First Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking*, 35 FCC Rcd at 3244-45, para. 6.

[28] *Call Authentication Trust Anchor*, WC Docket No. 17-97, Notice of Inquiry, 37 FCC Rcd 13451, 13453, para. 4 (2022) (*Notice of Inquiry*); *First Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking*, 35 FCC Rcd at 3244-45, para. 6.

[29] *Eighth Caller ID Authentication Report and Order* at 4-5, paras. 6-7.

[30] *Id.*, para. 7, n.25.

[31] ATIS & SIP Forum, Signature-based Handling of Asserted information using toKENs (SHAKEN), ATIS-1000074 at 6 (2022) (ATIS-1000074), https://access.atis.org/higherlogic/ws/public/download/67436.

[32] FCC, Triennial Report on the Efficacy of the Technologies Used in the STIR/SHAKEN Caller ID Authentication Framework at 9-11 (2022), https://docs.fcc.gov/public/attachments/DOC-390474A1.pdf (Triennial Report).

[33] *First Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking*, 35 FCC Rcd at 3245, para. 7 ("Because the STIR/SHAKEN framework relies on transmission of information in the Identity header of the SIP INVITE, it only operates in the IP portions of a voice service provider's network—that is, those portions served by network technology that is able to initiate, maintain, and terminate SIP calls.").

[34] 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. § 227(b)(1)(B); 47 CFR § 64.6303. Such technology includes time-division multiplexing (TDM) technology, and providers with non-IP network technology may use protocols such as Signaling System No. 7 (SS7) in place of SIP. *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1895, para. 69 (noting that some providers with TDM networks use SS7 technology while others may not).

[35] *Notice of Inquiry*, 37 FCC Rcd at 13454, para. 6.

[36] 47 U.S.C. § 227b(b)(1)(B).

hardship.[37] Nearly all of the implementation extensions granted by the Commission on the basis of undue hardship have since expired.[38] While Congress established the same June 30, 2021 deadline for voice service providers to take "reasonable measures to implement an effective call authentication framework" in non-IP networks, for those providers "materially reli[ant] on a non-[IP] network for the provision of . . . service or calls," section 4(b)(5)(B) of the TRACED Act requires that the Commission "grant a delay of required compliance . . . until a call authentication protocol has been developed for calls delivered over non-[IP] networks and is reasonably available."[39]

10. In 2020, pursuant to the TRACED Act's directive that voice service providers take reasonable measures to implement call authentication in their non-IP networks, the Commission adopted rules that require voice service providers to either upgrade their networks to IP and fully implement STIR/SHAKEN[40] or provide proof of participation in industry efforts to develop a non-IP caller ID authentication solution.[41] In addition, consistent with section 4(b)(5)(B) of the TRACED Act, Commission rules provide that "[t]hose portions of a . . . provider's network that rely on [non-IP] technology" are "deemed subject to a continuing extension" for compliance.[42] The Commission evaluates the extension on an ongoing basis, monitoring industry progress toward a working non-IP caller ID authentication solution.[43]

11. In the May 2022 *Gateway Provider Report and Order and Further Notice of Proposed Rulemaking*, the Commission sought comment on "whether [it] should require all providers to adopt a non-IP caller ID authentication solution."[44] The Commission acknowledged that both ATIS and commenters in previous proceedings had offered specific proposals for authentication over non-IP networks, and solicited comment on whether the Commission should adopt one of these or a modified solution.[45] In response, the Commission received comments urging it to mandate implementation of a

[37] *Id.* § 227b(b)(1), (5)(A)-(B). The TRACED Act directed the Commission to assess burdens or barriers to the implementation of STIR/SHAKEN and granted the Commission discretion to extend the implementation deadline for a "reasonable period of time" based upon a "public finding of undue hardship." *Id.* § 227b(b)(5)(A).

[38] The STIR/SHAKEN implementation extension for services scheduled for section 214 discontinuance ended on June 30, 2022, and the implementation extensions for non-facilities-based and facilities-based small voice service providers ended on June 30, 2022 and June 30, 2023, respectively. *See* 47 CFR § 64.6304(a)(1), (c). In December 2023, the Wireline Competition Bureau (Bureau) retained implementation extensions for small voice service providers originating calls via satellite and for providers that cannot obtain a service provider token necessary to participate in STIR/SHAKEN. *See Wireline Competition Bureau Performs Required Evaluation Pursuant to Section 64.6304(F) of the Commission's Rules*, WC Docket No. 17-97, Public Notice, 38 FCC Rcd 11912 (2023). These extensions remain in place. *See* 47 CFR § 64.6304(a)(1)(iii), (b).

[39] 47 U.S.C. § 227b(b)(5)(B).

[40] Implementation of STIR/SHAKEN requires its use, which includes: (1) authentication and verification of caller ID information for all SIP calls exclusively transiting a provider's network, 47 CFR § 64.6301(a)(2); (2) authentication and (to the extent feasible) transmission of caller ID information for all SIP calls it originates and exchanges with another provider, *id.* § 64.6301(a)(2); and (3) verification of caller ID information for all SIP calls it receives from another provider which it will terminate and for which the caller ID information has been authenticated, *id.* § 64.6301(a)(3).

[41] *Id.* § 64.6303(a), (b), (c).

[42] *Id.* § 64.6304(d).

[43] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1895, para. 69.

[44] *Gateway Provider Report and Order and Further Notice of Proposed Rulemaking*, 37 FCC Rcd at 6931, para. 173.

[45] *Id.*, para. 173, n.467.

non-IP solution,[46] as well as those arguing that doing so would be premature[47] and that the Commission should instead focus its efforts on promoting the transition of non-IP network technology to IP.[48]

12. In October 2022, recognizing a need to develop a more focused record on closing the non-IP network gap in the STIR/SHAKEN framework, the Commission released a *Notice of Inquiry*.[49] The Commission sought comment generally about caller ID authentication in non-IP networks, the prevalence of non-IP network technology, and the impact such networks have on efforts to stem illegal robocalls.[50] Additionally, the *Notice of Inquiry* asked about the state of the IP transition and whether the Commission should take steps to promote its acceleration.[51] Highlighting the ability of an all IP network to "promote new and innovative product offerings to customers" and the potential for ubiquitous end-to-end implementation of STIR/SHAKEN, the Commission asked whether it should forego requiring implementation of a non-IP caller ID authentication solution and instead mandate a regulatory sunset for non-IP technology.[52]

13. The *Notice of Inquiry* also solicited detailed comment on two non-IP caller ID authentication standards published by ATIS:[53] ATIS-1000095.v002, *Extending STIR/SHAKEN over TDM* (In-Band Authentication),[54] and ATIS-1000096, *Out-of-Band PASSporT Transmission Involving TDM Networks* (Out-of-Band Multiple STI-CPS Authentication).[55] Although they differ in approach, both specifications enable transmission of caller ID authentication information for calls transmitted over non-IP networks.[56]

14. In-Band Authentication allows providers to transmit some of the same information as STIR/SHAKEN, including PASSporTs, with the call over the non-IP portions of the phone network.

---

[46] *See* Credit Union National Association et al. Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 3-5 (rec. Aug. 17, 2022) (Credit Union National Association et al. 2022 FNPRM Comments); TransNexus Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 5-6 (rec. Aug. 17, 2022) (TransNexus 2022 FNPRM Comments); ZipDX Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 7-8 (rec. Aug. 17, 2022) (ZipDX 2022 FNPRM Comments).

[47] *See* ACA Connects Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 9 (rec. Aug. 17, 2022) (ACA Connects 2022 FNPRM Comments); USTelecom Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 17-18 (rec. Aug. 17, 2022) (USTelecom 2022 FNPRM Comments).

[48] *See* NCTA Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 2-3 (rec. Aug. 17, 2022) (NCTA 2022 FNPRM Comments) (arguing that requiring providers "to adopt a *non*-IP call authentication solution . . . would be counterproductive" and would "eliminate incentives for . . . providers to transition to IP-based solutions"); *see also* USTelecom 2022 FNPRM Comments at 17-18 (claiming that "STIR/SHAKEN over TDM solutions raise" various issues and that "devoting resources there may detract from other, more fruitful efforts").

[49] *See Notice of Inquiry*, 37 FCC Rcd at 13451, para. 1.

[50] *See id.* at 13459, paras. 17-19.

[51] *Id.* at 13467-70, paras. 36-42.

[52] *Id.* at 13470, para. 42.

[53] *Id.* at 13456, 59-62, paras. 11, 20-24.

[54] ATIS, Extending STIR/SHAKEN over TDM, ATIS-1000095.v002 (2022), https://access.atis.org/apps/group_public/download.php/67542/ATIS-1000095.v002.pdf (In-Band Authentication (ATIS-1000095.v002)).

[55] ATIS, Signature-based Handling of Asserted information using toKENs (SHAKEN): Out-of-Band PASSporT Transmission Involving TDM Networks, ATIS-1000096 (2021), https://access.atis.org/apps/group_public/download.php/60535/ATIS-1000096.pdf (Out-of-Band Multiple STI-CPS Authentication (ATIS-1000096)).

[56] *Notice of Inquiry*, 37 FCC Rcd at 13456-57, paras. 12-13.

Under this standard, an originating voice service provider "comes to an agreement with the subsequent provider in the call path on how to share . . . information about what it knows about the caller and its right to use the phone number along with the call."[57] Because non-IP calls do not use SIP headers and cannot include the digital token attesting to a provider's trustworthiness, providers implementing the standard instead "guarantee trust through bilateral agreements between providers that exchange calls with one another."[58] The standard is thus reliant on bilateral agreements being in place between every directly connected provider using the standard at each non-IP network-to-network interface (NNI) in a call path.[59] According to ATIS, the In-Band Standard will function even if other providers in the call path employ alternative non-IP caller ID authentication frameworks.[60]

15. Out-of-Band Multiple STI-CPS Authentication allows providers to send the same information about a call as STIR/SHAKEN "on a separate track that is sent in tandem to the non-IP call signaling."[61] Under this standard, when a provider originates a call, it "publishes" STIR/SHAKEN call information, including PASSporTs, to a Secure Telephone Identity Call Placement Service (STI-CPS), which is hosted on the Internet by an entity registered with a governance structure, thereby avoiding loss of the information.[62] The next provider in the call path then "retrieves" the published information from an STI-CPS.[63] The standard envisions more than one STI-CPS, each sharing information with one another, enabling a terminating provider to retrieve call information from an STI-CPS other than the one to which the information was originally published.[64] According to ATIS, Out-of-Band Multiple STI-CPS Authentication, like In-Band Authentication, will function even if other providers in the call path employ alternative non-IP caller ID authentication frameworks.[65]

16. The Commission sought comment in the *Notice of Inquiry* on whether these two standards met the TRACED Act's requirements and inquired generally about the pros and cons of both standards, whether their implementation would impact the IP transition, their compatibility with one another, and how any issues unique to both standards could affect the STIR/SHAKEN caller ID authentication scheme.[66] Although commenters demonstrated a definitive need to address the non-IP gap in the STIR/SHAKEN framework, the record was mixed as to whether In-Band Authentication and Out-of-Band Multiple STI-CPS Authentication were fully developed, commercially available, and effective at that moment in time.

---

[57] *Id.* at 13457, para. 13.

[58] *Id.*

[59] *Id.*

[60] ATIS, Alternatives for Call Authentication for Non-IP Traffic, at 11 (2024), https://access.atis.org/higherlogic/ws/public/download/79507/ATIS-1000097.v003.pdf (ATIS-1000097.v003) (noting that providers could use In-Band Authentication and Out-of-Band Multiple STI-CPS Authentication across different TDM network-to-network interfaces in a call path).

[61] *Notice of Inquiry*, 37 FCC Rcd at 13456, para. 12; *see also* ATIS-1000097.v003 at 15 ("Within the specification, cryptographically signed PASSporT(s) are exchanged out-of-band, that is, separate from the telephone network signaling.").

[62] *Notice of Inquiry*, 37 FCC Rcd at 13456, para. 12; *see also* ATIS-1000097.v003 at 15-16 ("A governance structure is also required to support STI-CPS discovery. . . .").

[63] ATIS-1000097.v003 at 15; Out-of-Band Multiple STI-CPS Authentication (ATIS-1000096) at 6 (describing the PASSporT "publish" and "retrieval" process in greater detail).

[64] *Notice of Inquiry*, 37 FCC Rcd at 13456, para. 12; *see also* ATIS-1000097.v003 at 15 ("An STI-CPS has a standardized interface for service providers to publish and retrieve PASSporT(s).").

[65] ATIS-1000097.v003 at 11.

[66] *Notice of Inquiry*, 37 FCC Rcd at 13459-65, paras. 20-29.

17. In December 2024, following the *Notice of Inquiry*, ATIS published a third non-IP caller ID authentication standard, ATIS-1000105, Out-of-Band PASSporT Transmission Involving TDM Networks (Out-of-Band Agreed STI-CPS Authentication).[67] Like Out-of-Band Multiple STI-CPS Authentication, Out-of-Band Agreed STI-CPS Authentication involves publication and retrieval of STIR/SHAKEN call information, including PASSporTs, out-of-band through an STI-CPS.[68] Unlike Out-of-Band Multiple STI-CPS Authentication, every directly connected provider across each non-IP NNI in the call path must agree on the STI-CPS to be used for publishing and retrieving call information.[69] Additionally, according to ATIS, unlike the two other non-IP standards, all providers that interconnect with non-IP portions of the call path must utilize Out-of-Band Agreed STI-CPS Authentication for the call information to be received intact by the terminating provider.[70]

18. At the same time ATIS approved the Out-of-Band Agreed STI-CPS Authentication standard, it released two technical reports on the three ATIS non-IP standards: (1) ATIS-1000097.v003, *Alternatives for Call Authentication for Non-IP Traffic*, which "identifies non-IP call authentication scenarios and provides a framework to evaluate potential approaches that could provide call authentication even when the call is not SIP end-to-end,"[71] and (2) ATIS-1000106, *Viability of Non-IP Call Authentication Standards*, to help providers understand challenges with implementing the standards.[72]

## III. DISCUSSION

19. We propose to conclude that effective non-IP caller ID authentication frameworks are developed and reasonably available, and therefore propose to mandate that voice service providers, gateway providers, and non-gateway intermediate providers that have not upgraded their networks to IP implement one or more non-IP caller ID authentication frameworks in their non-IP networks by a date certain.[73] Under the TRACED Act, the Commission must mandate that providers that continue to rely on

---

[67] ATIS, Signature-based Handling of Asserted information using Tokens (SHAKEN): Out-of-Band PASSporT Transmission Between Service Providers that Interconnect using TDM (2024), https://access.atis.org/higherlogic/ws/public/download/79509/ATIS-1000105.pdf (Out-of-Band Agreed STI-CPS Authentication (ATIS-1000105)).

[68] *See* ATIS-1000097.v003 at 16 (explaining that Out-of-Band Agreed STI-CPS Authentication utilizes standard PASSporTs, interworks transparently with SHAKEN, does not require changes to SHAKEN-compliant SIP networks that do not use TDM NNIs, fully supports "shaken," "div," "rcd," and "rph" PASSporTs, and should support future PASSporT extensions without changes to standards or functional elements).

[69] Out-of-Band Agreed STI-CPS Authentication (ATIS-1000105) at 6.

[70] ATIS, Viability of Non-IP Call Authentication Standards at 6 (2024), https://access.atis.org/higherlogic/ws/public/download/79510/ATIS-1000106.pdf (ATIS-1000106) ("ATIS-1000105 [Ref 6] must be implemented by every service provider with TDM NNIs in the call path of a given call for the PASSporT(s) associated with that call to be delivered to the terminating service provider.").

[71] ATIS-1000097.v003 at 1.

[72] ATIS-1000106 at 1.

[73] Although section 4(b)(1)(B) of the TRACED Act applies to "provider[s] of voice service" and defines "voice service" to include any service that is "interconnected with the public switched telephone network and that furnishes voice communications to an end user," 47 U.S.C. § 227b(a)(2), the Commission has adopted rules that also apply caller ID authentication obligations to gateway providers and non-gateway intermediate providers, relying on its authority under sections 251(e) and 227(e) of the Communications Act. *See Gateway Provider Report and Order and Further Notice of Proposed Rulemaking*, 37 FCC Rcd at 6893, para. 62; *Sixth Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking*, 38 FCC Rcd at 2587, para. 26; 47 U.S.C. §§ 251(e), 227(e). In this item, we propose amending certain rules that are currently applicable to these three categories of providers. For purposes of this item, we will use the general term "providers" to encompass the three categories of providers covered by our caller ID authentication rules, unless otherwise specified.

non-IP technology "take reasonable measures to implement an effective call authentication framework in [their] non-[IP] networks."[74] To fulfill this "reasonable measures" requirement, the Commission requires that voice service providers either upgrade their entire network to IP or participate in efforts to develop a non-IP caller ID authentication solution, and said that it "will continue to evaluate whether an effective non-IP caller ID authentication framework emerges."[75] The TRACED Act requires the Commission to "grant a delay of required compliance" with the implementation deadline for non-IP caller ID authentication for voice service providers materially reliant on non-IP networks "until a call authentication protocol has been developed for calls delivered over non-[IP] networks and is reasonably available."[76]

20. In light of the record developed in response to the *Notice of Inquiry* and marketplace developments, we propose to conclude that certain non-IP caller ID authentication frameworks meet the TRACED Act's requirements. This proposed conclusion is based upon the application of criteria we propose to establish for evaluating whether a given framework is first, developed and reasonably available, and second, effective.[77] In turn, we propose to repeal the continuing extension from caller ID authentication requirements granted to providers that rely on non-IP technology and modify our rule interpreting the TRACED Act's "reasonable measures" requirement to mandate that providers either upgrade their networks to IP or implement non-IP caller ID authentication frameworks. Continuing to allow providers to complete their IP transitions rather than implement non-IP caller ID authentication frameworks enables them to avoid the additional obligation associated with the new requirement.[78] We propose to give providers a reasonable transition period to either complete their IP transitions or implement one or more non-IP caller ID authentication frameworks in their non-IP networks.[79] We

[74] 47 U.S.C. § 227b(b)(1)(B). We propose to conclude that a "call authentication framework" under section 227b(b)(1)(B) consists of any standards or other structures that define how to authenticate calls. *See* Framework, Collins Online Dictionary, https://www.collinsdictionary.com/dictionary/english/framework (last visited Apr. 23, 2025) (defining "framework" as "a particular set of rules . . . which you use in order to deal with problems or to decide what to do"). This is supported by the TRACED Act's requirement that the Commission mandate implementation of the STIR/SHAKEN framework, which consists of the STIR and SHAKEN standards. 47 U.S.C. § 227b(a)(1); *id.* § 227b(b)(1)(A); *see also supra* Section II (Background) (describing the STIR/SHAKEN framework as comprised of several standards and protocols).

[75] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1874, para. 32; 47 CFR § 64.6303(a). We propose to clarify that the Commission's rules requiring providers with non-IP networks to either upgrade their networks to IP or participate in efforts "to develop a non-IP *solution*," *see, e.g.*, 47 CFR § 64.6303(a), refer to the development of a "call authentication *framework*" for non-IP networks under section 227b(b)(1)(B) of the TRACED Act. This is consistent with the Commission's description when it established these rules in the *First Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking*. There, the Commission made clear that it was implementing the "reasonable measures" requirement in section 227b(b)(1)(B) and it referred to the STIR/SHAKEN framework as a "SIP-based *solution*." *First Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking*, 35 FCC Rcd at 3283 at para. 96 (emphasis added).

[76] 47 U.S.C. § 227b(b)(5)(B). The Commission issued this continuing extension in the *Second Caller ID Authentication Report and Order*. *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1892-93, para. 66; *see also* 47 CFR § 64.6304(d). We propose to conclude, under the best reading of the statute, that the phrase "call authentication protocol" in section 227b(b)(5)(B) refers to the technical procedures underlying the standards or other procedures developed for authenticating calls. *See* Newton's Telecom Dictionary 1068 (Harry Newton and Steve Schoen, eds., 32nd ed. 2021) (defining "protocol" as "a set of rules that govern communications on a network"); *see also supra* Section II (Background) (describing the STIR standard as comprised of various protocols).

[77] 47 U.S.C. § 227b(b)(1)(B), (5)(B).

[78] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1871, para. 24; 47 CFR § 64.6303(a)(1).

[79] The Cloud Communications Alliance et al. asks that we seek comment on requiring all providers to convert their networks to IP by a date certain. *See* Letter from Joe Marion, Cloud Communications Alliance, et al., to Marlene Dortch, Secretary, FCC, WC Docket No. 17-97 at 2 (filed Apr. 21, 2025) (CCA et al. *Ex Parte*). We support

(continued….)

propose to rely on the TRACED Act and other Commission authority to implement this mandate. Below, we seek comment on these proposals and any other considerations not addressed or specifically asked about herein.

### A. Determining Whether Effective Non-IP Caller ID Authentication Frameworks Exist

21. Below we propose criteria for evaluating whether non-IP caller ID authentication frameworks meet TRACED Act requirements to first, be developed and reasonably available, and second, be effective and, applying that criteria, propose to conclude that certain standards promulgated by ATIS constitute frameworks meeting those requirements. We seek comment on these proposals.

#### 1. Criteria for Evaluating Whether Non-IP Caller ID Authentication Frameworks Meet TRACED Act Requirements

22. We propose to establish criteria for evaluating whether a given non-IP caller ID authentication framework meets the TRACED Act's requirements. Consistent with the TRACED Act, we propose to apply the criteria in two steps. First, the Commission must determine whether any frameworks are "developed" and "reasonably available" to meet the TRACED Act's requirements for repealing the continuing extension from caller ID authentication requirements for providers materially reliant on non-IP networks. Second, the Commission must determine whether any such frameworks meet the TRACED Act's requirement to be "effective," in connection with the TRACED Act's requirement that providers "take reasonable measures to implement an effective call authentication framework" in their non-IP networks.[80] We discuss each step below.

23. *Criteria for repealing the continuing extension for non-IP networks.* We propose to establish criteria, based on the plain meaning of the TRACED Act, for determining whether a given non-IP caller ID authentication framework meets the TRACED Act's requirements for repealing the continuing extension. Section 4(b)(5)(B) of the TRACED Act requires the Commission to provide a continuing extension from implementing non-IP caller ID authentication for providers materially reliant on non-IP networks "until a call authentication protocol has been developed for calls delivered over non-[IP] networks and is reasonably available."[81] The terms "developed," and "available" are not defined in the TRACED Act, so we propose to rely on the ordinary meaning of these terms. "Developed" or "develop" means "starts to exist"[82] or "to make more available or usable," [83] while "available" means "able to be used or obtained"[84] or "usable."[85]

24. Considering these definitions, we propose to retain the two criteria the Commission established in the *Second Caller ID Authentication Report and Order* for evaluating whether a non-IP caller ID authentication framework satisfies the requirements in the TRACED Act for repealing the continuing extension. Specifically, the Commission determined that a framework must be: (1) "fully developed and finalized by industry standards," and (2) reasonably available such that "the underlying equipment and software necessary to implement such protocol is available on the commercial market."[86]

(Continued from previous page)
providers' completing their transition to IP, which is a key goal of the Commission, but this proposal is outside the scope of this proceeding.

[80] 47 U.S.C. § 227b(b)(1)(B).

[81] *Id.* § 227b(b)(5)(B).

[82] Concise Oxford English Dictionary 391 (Catherines Soanes et al. eds., 11th ed. 2008).

[83] The New Merriam-Webster Dictionary 212 (Frederick C Mish ed., 1989).

[84] Concise Oxford English Dictionary 91 (Catherines Soanes et al. eds., 11th ed. 2008).

[85] The New Merriam-Webster Dictionary at 65 (Frederick C Mish ed., 1989).

[86] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1894-95, para. 68; *see also id.* at 1874, para. 32; *Notice of Inquiry*, 37 FCC Rcd at 13456, para. 11.

We believe that these criteria reflect a logical and straightforward understanding of the plain meaning of the statutory text. We seek comment on our proposal and any alternative interpretations of the TRACED Act's requirements. We also propose and seek comment on a set of non-exhaustive factors for each criterion, no one of which is determinative, that we should consider when evaluating whether a given non-IP caller ID authentication framework satisfies those criteria, as well as any other factors we should take into account. We believe these factors will enable the Commission to reach well-reasoned conclusions about whether a framework meets the criteria within the ordinary meaning of the statutory language.

25. For the first criterion, we propose to consider a set of factors to determine whether a framework is "fully developed and finalized by industry standards."[87] Consistent with the *Second Caller ID Authentication Report and Order*, we propose to evaluate whether a framework is standards-based, including whether "all fundamental aspects of the protocol which enable its effectiveness are standardized by industry."[88] Relatedly, we propose to consider whether the technical elements of the framework have been published and are accessible by providers or vendors that make frameworks commercially available. As further consistent with the *Second Caller ID Authentication Report and Order*, we propose to consider whether a framework is "ready for implementation," including whether "the protocol is implementable" by providers.[89] We also propose to consider whether the framework is undergoing further development or improvement.[90] Given that Commission rules obligate providers using non-IP network technology to participate in industry efforts to develop a non-IP caller ID authentication solution,[91] we further propose to consider the extent to which industry was involved in the development and approval of a framework and the standards upon which the framework is based. We seek comment on these factors and whether the Commission should consider any other factors when evaluating whether a framework is fully developed and finalized by industry standards.

26. For the second criterion, we propose to consider a set of factors to determine whether a framework is reasonably available such that "the underlying equipment and software necessary to implement such protocol is available on the commercial market."[92] We propose to consider evidence that a framework is being marketed or otherwise offered to providers. We also propose to consider evidence that a framework has been implemented by providers or whether providers are waiting for the Commission to mandate frameworks before investing in implementing available frameworks. Additionally, we propose to consider a framework's cost and evidence that the cost can be reasonably borne by providers. We also propose to consider the need to set up a governance structure for a framework to operate and whether any changes to Commission process or rules are necessary to implement such a structure. We seek comment on these factors and whether the Commission should consider any other factors when evaluating whether a framework is reasonably available such that the underlying equipment and software necessary to implement such protocol is available on the commercial market. For instance, should we consider the extent to which a framework can scale to serve a greater number of providers, and if so, how important is this factor if we determine that multiple frameworks meet the TRACED Act's requirements? Similarly, how, if at all, should we consider whether products

[87] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1894, para. 68; *see also id.* at 1874, para. 32; *Notice of Inquiry*, 37 FCC Rcd at 13456, para. 11.

[88] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1894, para. 68, n.268.

[89] *Id.*

[90] *See id.* at 1894 para. 68 n.268 ("By 'fully developed' and 'finalized' we do not require that the protocol must have achieved a status whereby no future development or progress is possible. Under that interpretation, the STIR/SHAKEN framework itself would not meet this standard. Instead, our standard does not foreclose the possibility of further development and improvement . . . .").

[91] 47 CFR § 64.6303(a)(2), (b)(2), (c)(2).

[92] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1894-95, para. 68; *see also id.* at 1874, para. 32; *Notice of Inquiry*, 37 FCC Rcd at 13456, para. 11.

implementing a framework are only offered by one or a few vendors? Should we consider whether a product relies on proprietary elements not outlined in the framework and the extent to which a provider must use such proprietary elements for the product to work?

27. *Criteria for modifying the requirement to take reasonable measures to implement effective non-IP caller ID authentication.* We propose to establish criteria, based on the structure and plain meaning of the TRACED Act, for determining whether a given non-IP caller ID authentication framework meets the TRACED Act's requirement to be "effective."[93]

28. First, we propose to conclude that for a framework to be "effective" under the TRACED Act, it must at least satisfy the two requirements for repealing the continuing extension in section 4(b)(5)(B) of the TRACED Act (i.e., "developed" and "reasonably available"). Incorporating these two baseline requirements ensures that providers cannot rely on the continuing extension to avoid implementing frameworks the Commission has concluded are effective.[94] Were we to read the TRACED Act otherwise, the Commission could find that a caller ID authentication framework is effective under section 4(b)(1)(B), but a provider would not have an obligation to implement that framework if the Commission did not also find that the framework satisfies the requirements for removing the continuing extension under section 4(b)(5)(B).[95] The best reading of the statute and its structure therefore ties the continuing extension from complying with the non-IP caller ID authentication obligation to the obligation to implement an effective non-IP caller ID authentication framework. We seek comment on this view and any alternative interpretations.

29. Next, we propose to evaluate effectiveness based on the plain meaning of the text in the TRACED Act. The TRACED Act does not define "effective," and so we propose to rely on the ordinary meaning of the word. "Effective" is defined to mean "producing a desired or intended result,"[96] "operative,"[97] or "performing within the range of normal and expected standards."[98] In applying these definitions, we propose to conclude that an "effective" non-IP caller ID authentication framework must

[93] *See* 47 U.S.C. § 227b(b)(1)(B).

[94] This understanding is also consistent with the *Second Caller ID Authentication Report and Order*, wherein the Commission said it "will consider a non-IP caller ID authentication framework to be effective only if it is: (1) fully developed and finalized by industry standards; and (2) reasonably available such that the underlying equipment and software necessary to implement such protocol is available on the commercial market." *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1874, para. 32; *see also Notice of Inquiry*, 37 FCC Rcd at 13456, para. 10. The Commission acknowledged, however, that while these criteria may be necessary for determining whether a solution is effective, they may not be sufficient. *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1873-74, para. 31 (stating, under the Commission's interpretation at the time, that "significant industry consensus is an important predicate to deeming a non-IP solution 'effective'").

[95] Similarly, the Commission could find that a solution is developed and reasonably available, satisfying the requirements for repealing the continuing extension under section 4(b)(5)(B) and thereby triggering the requirement in section 4(b)(1)(B) for providers to take reasonable measures to implement an effective non-IP caller ID authentication solution. However, a provider would not be able to implement an effective non-IP caller ID authentication solution if the Commission had not determined at the same time or earlier that such a solution exists.

[96] Concise Oxford English Dictionary 456 (Catherines Soanes et al. eds., 11th ed. 2008); *see also* The New Merriam-Webster Dictionary 243 (Frederick C Mish ed., 1989) ("producing a decisive or desired effect"); *Effective*, Black's Law Dictionary (12th ed. 2024) ("Productive; achieving a result").

[97] Concise Oxford English Dictionary 456 (Catherines Soanes et al. eds., 11th ed. 2008); *see also Effective*, Black's Law Dictionary (12th ed. 2024) ("in operation at a given time").

[98] *See Effective*, Black's Law Dictionary (12th ed. 2024).

operate to produce the intended result of authenticating calls as described in the applicable standards.[99] That is, when the standards are properly applied under the conditions specified in the standards, the provider is able to authenticate calls.[100] This meaning is consistent with the Commission's understanding of its requirement under the TRACED Act to assess the efficacy of the technologies used for call authentication frameworks implemented under the statute every three years.[101] In its Triennial Report, "the [Wireline Competition Bureau] assesses the efficacy of the STIR/SHAKEN framework herein based on the proposed standard of how well it effectuates the authentication of caller ID information,"[102] and its finding "is predicated . . . on STIR/SHAKEN technical standards and protocols being executed as required by the three ATIS standards that establish them."[103] Additionally, we believe that interpreting "effective" to mean more than just "developed" and "reasonably available" is consistent with the canon of statutory construction against surplusage, by ensuring that each word is operative.[104] We seek comment on our proposed understanding of "effective," and on any alternative interpretations.

30. We seek comment on whether the best reading of the TRACED Act requires us to consider specific factors for evaluating whether a non-IP caller ID authentication framework is "effective" under the ordinary meaning of the word,[105] and if so, what those factors are.

31. In particular, we invite commenters to address whether we must consider factors

---

[99] *See, e.g.*, American Bankers Association et al. Comments at 5 (arguing that providers should be able to adopt any non-IP standard so long as "the solution has the ability to transmit to the terminating carrier information regarding caller ID authenticity").

[100] We do not believe that "effectiveness" requires that a solution operate to authenticate calls in all instances. We believe our understanding is supported by the TRACED Act requirement that the Commission assess the efficacy of implemented call authentication frameworks every three years. *See* 47 U.S.C. § 227b(4)(b)(4)(B). Because Congress in the TRACED Act required the Commission to mandate that providers use STIR/SHAKEN in their IP networks, *id.* § 227b(b)(1)(A), we believe it is reasonable to conclude that Congress deemed STIR/SHAKEN to be an effective caller ID authentication solution. By requiring the Commission to evaluate the efficacy of call authentication frameworks, including STIR/SHAKEN, we believe Congress acknowledged that even effective caller ID authentication solutions—e.g., STIR/SHAKEN—may not result in perfect call authentication in all instances. Indeed, in conducting the triennial review of the efficacy of call authentication technologies, perfection is not the standard the Commission itself has applied to STIR/SHAKEN. *See* Triennial Report at 9 (noting that one commenter indicated that, "in its experience," STIR/SHAKEN falls just short of successfully authenticating all calls, while another argued that it has been "tremendously successful at authenticating caller ID information for providers that have implemented technology in their networks") (internal citations omitted).

[101] *See* 47 U.S.C. § 227b(4)(b)(4)(B) (requiring the Commission "assess the efficacy of the technologies used for call authentication frameworks implemented under" the TRACED Act every three years); *Efficacy*, Black's Law Dictionary (12th ed. 2024) (defining "efficacy" similar to "effective," as "[t]he power to make an intended result occur").

[102] *See* Triennial Report at 8.

[103] *See id.* at 9.

[104] *See* Congressional Research Service, Valerie C. Brannon, Statutory Interpretation, Theories, Tools, and Trends at 30 (2023), https://www.congress.gov/crs_external_products/R/PDF/R45153/R45153.6.pdf ("The surplusage canon requires courts to give each word and clause of a statute operative effect, if possible. . . . [F]or example, when a court is faced with a statutory list of terms, it generally will reach each term to convey some distinct meaning."); *Bailey v. United States*, 516 U.S. 137, 146 (1995) (assuming "that Congress used two terms because it intended each term to have a particular, nonsuperfluous meaning"); *see also Russello v. U.S.,* 464 U.S. 16, 23 (1983) ("Where Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion.") (internal citations omitted).

[105] *See Notice of Inquiry*, 37 FCC Rcd at 13464, para. 29 (asking whether the Commission should reconsider what it means for a given solution to be "effective" under the TRACED Act and if other factors should be considered).

concerning the feasibility for providers to implement frameworks. For example, must we evaluate the need for providers to enter into bilateral or multilateral agreements to implement certain frameworks?[106] Are we required to consider the extent to which a framework will only work for providers using certain network equipment or facilities, or whether a provider would need to make changes or upgrades to their existing network before implementing a framework?[107] Must we take into account a framework's implementation costs and burdens or its cost effectiveness in determining whether it is effective? If so, how should the Commission evaluate cost-effectiveness? Can a framework still be considered effective if it is not cost-effective for all providers or the cost is burdensome for some providers to implement?[108] Are there other implementation challenges we must or should consider?[109]

32. We also invite commenters to explain whether we are required to evaluate factors concerning the inherent features and functions of each framework. To what extent must we consider technical limitations of a framework that otherwise authenticates calls as described by the standard?[110]

---

[106] *See* ATIS-1000106 at 5 (noting that for In-Band Authentication, "bilateral agreements need to exist between each pair of service providers that interconnect via TDM [network-to-network interfaces] or multilateral agreements need to exist among all providers that interconnect through a given tandem network"); ATIS-1000097.v003 at 13 (stating that a provider implementing Out-of-Band Agreed STI-CPS Authentication needs to enter into bilateral agreements with other providers with which it interconnects in TDM to choose a common STI-CPS); *see also* GCI Reply at 12 (arguing that "the In-Band standard imposes incredible burdens on providers because, as the Commission observed, 'it requires directly connected providers at each link in the call path to have bilateral agreements in place'"); *but see* WTA Comments at 6 (agreeing that this burden exists, but arguing that the Commission should approve the standard because it "may be feasible and economical for some carriers under some circumstances . . .").

[107] *See* ATIS-1000106 at 5 (explaining that [In-Band Authentication] could be implemented on "later-generation TDM-based systems" but that they would "require additional capital and/or operating resources to deploy and support the function" and that "[a]dditional development" of TDM elements that "have been in service for many years and contain older technology . . . may be impractical or vendor support may not be available"); GCI Comments at 12 ("The In-Band Standard simply will not work in remote Alaska" because "[m]any rural end offices . . . do not have SS7 capability . . . ."); ATIS-1000097.v003 at 15 (stating that, for Out-of-Band Multiple STI-CPS Authentication, among other things, "TDM networks may need the same functional elements that IP networks need"); *id.* (stating that for Out-of-Band Multiple STI-CPS Authentication, new functionality is required to be implemented "at the end office level").

[108] *See, e.g.*, TransNexus Comments at 9 (arguing that Out-of-Band Multiple STI-CPS Authentication "is a better choice for most providers that rely on non-IP technology and are not yet ready or able to transition to IP. However, we expect that [In-Band Authentication] may be suitable for some use cases.").

[109] *See* Aureon Comments at 9 (asserting that In-Band Authentication would "give rise to disputes regarding which party is responsible for transporting calls outside the rural LEC's service area"); ATIS-1000097.v003 at 14 (explaining that under Out-of-Band Agreed STI-CPS Authentication, "a given service provider may need to interface with multiple STI-CPSs"); *id.* at 16 (stating that each "TDM entity" also must obtain an "STI certificate"); TransNexus Comments at 11 (stating that Out-of-Band Multiple STI-CPS Authentication "requires software updates"); USTelecom Comments at 11 (claiming that, without additional steps, Out-of-Band Multiple STI-CPS Authentication can only be used in "TDM-in-the-middle" scenarios, not for origination and termination, and therefore is a poor solution for larger providers); *but see* TransNexus Reply at 7 (arguing that the standard is not so limited and noting that "[t]he Out-of-Band standard provides call scenario examples using Out-of-Band with TDM origination and termination"). We note that the Commission recently required all providers with a STIR/SHAKEN obligation to obtain an STI certificate. *See Eighth Caller ID Authentication Report and Order* at 21-22, para. 28.

[110] *See* ATIS-1000097.v003 at 18-19 (noting that In-Band Authentication allows for transmission of certain extensions); TransNexus Comments at 8-9 (stating that certain SHAKEN information, including information "associated with additional features" such as delegate certificates and Rich Call Data, is often too large and "some of the information associated with these features . . . is lost" under In-Band Authentication); USTelecom Comments at 15 (arguing that In-Band Authentication "may require as much as four-times the TDM network interfaces between interconnected carriers" resulting in TDM network inefficiencies and complexity and that the "SS7 UUI parameter" upon which the standard relies is not always available); ATIS-1000097.v003 at 17 (explaining that there may be scenarios for Out-of-Band Multiple STI-CPS Authentication where providers would be required to "reconstruct any

(continued….)

For example, must we evaluate whether and the extent to which a framework's ability to authenticate calls provides functional parity with STIR/SHAKEN?[111] Is it necessary to consider whether a framework is technically futureproof, including whether it would continue to function and be able to incorporate additional functionality as providers make changes and upgrades to their networks?[112] To what extent must we consider the security of a framework and whether it may enable bad actors to transmit false authentication information or otherwise undermine the effectiveness of STIR/SHAKEN?[113] Must we consider a framework's resilience to Denial of Service attacks aimed at different components of the framework? Are we required to consider whether there are single-points-of-failure embedded within the design of certain frameworks and their impact? We also seek comment on whether we must consider any impacts that these frameworks' implementation may have on E911 and emergency services, and their bearing on the frameworks' effectiveness.[114]

33. We seek comment on whether the best reading of the statute requires us to take into account any other factors when evaluating a framework's effectiveness. For example, in the *Second Caller ID Authentication Report and Order*, the Commission said that "significant industry consensus is an important predicate to deeming a non-IP framework 'effective,' given that cross-network exchange of

(Continued from previous page)
SIP headers that were lost in the conversion from SIP to TDM back to SIP"); ATIS-1000106 at 5 (explaining that in some scenarios for Out-of-Band Multiple STI-CPS Authentication, "call setup time may be increased" and, as a result, an authenticated call may appear "as if it was unauthenticated . . .").

[111] *See* TransNexus Comments at 15-16 (arguing that in those use cases where In-Band Authentication "cannot relay all of the SHAKEN information it receives," the standard would not meet the TRACED Act requirements); American Bankers Association et al. Comments at 5 (arguing that providers should be able to adopt any non-IP standard so long as "the solution has the ability to transmit to the terminating carrier information regarding caller ID authenticity").

[112] *See, e.g.*, ATIS-1000097.v003 at 13 (appearing to show that, like Out-of-Band Multiple STI-CPS Authentication, Out-of-Band Agreed STI-CPS Authentication appears to support any PASSporT extension and any likely future PASSporT extensions).

[113] *See, e.g., id.* at 15-17 (explaining that "[d]ue to the security considerations with [Out-of-Band Multiple STI-CPS Authentication] . . . use of [Out-of-Band Agreed STI-CPS Authentication] may be preferrable" and discussing some of these security issues in greater detail, such as possible vulnerability to "replay attacks" and that calling patterns of every provider using the standard can be visible to every STI-CPS); USTelecom Reply at 4 (arguing that at least Out-of-Band Multiple STI-CPS Authentication should not be adopted until the ATIS Non-IP Call Authentication (NIPCA) Task Force addresses questions, including those "related to security and governance"); CTIA Reply at 3-4 (arguing that Out-of-Band Multiple STI-CPS Authentication "presents security risks at a large scale" including CPNI risks); NTCA Comments at 15-16 (arguing any CPNI vulnerabilities with Out-of-Band Multiple STI-CPS Authentication were addressed in the standard, and that it is "misleading to assert that 'security' concerns have not been . . . properly addressed," and noting that any security concerns are comparable to those for calls carried over the PSTN); Wabash Reply at 1-2 (arguing that "[w]hile some have raised 'security' concerns with respect to non-IP SHAKEN, the issues are no different than current issues being discussed for IP-SHAKEN used today" and noting that "security issues will be inherently ongoing to live-production IP-SHAKEN and SHAKEN as a whole" for as long as there are bad actors); ATIS-1000097.v003 at 19 (suggesting that In-Band Authentication is secure because it "does not introduce additional concerns about information leakage pertaining to calling patterns since no information is exposed to entities which are not already in the call signaling path").

[114] ATIS released two reports concerning the impact of non-IP standards on 911 services. The first, ATIS-0500046, Analysis of Non-IP Call Authentication Mechanisms in Support of Emergency Services, "discusses call authentication [including In-Band Authentication and Out-of-Band Multiple STI-CPS Authentication] in the context of emergency services" using "legacy" E911, while ATIS-1000097.v003, Appendix B describes a broader set of issues related to all three non-IP standards and their interaction with different types of 911 systems. *See* ATIS-1000097.v003 at 20 (describing ATIS-0500046, Analysis of Non-IP Call Authentication Mechanisms in Support of Emergency Services); *id.* at 20-25 (discussing additional considerations); *see also* ANSI Webstore, Analysis of Non-IP Call Authentication Mechanisms in Support of Emergency Services, ATIS-0500046 (2022), https://webstore.ansi.org/standards/atis/atis0500046.

authenticated caller ID information is a central component to caller ID authentication."[115] Must we consider whether and the extent to which industry consensus exists on the merits of a framework and the standards upon which the framework is based?[116] Does presence or lack of consensus bear on a framework's effectiveness? If so, how should we evaluate whether there is sufficient consensus? Should we consider whether any industry participants are withholding such consensus for reasons other than the effectiveness of the framework, such as an unwillingness to compromise on which frameworks are best or a desire to avoid having to invest in implementing a framework?

### 2. Evaluation of Non-IP Caller ID Authentication Frameworks

34. In this section, we propose to conclude that frameworks using two of the three ATIS-adopted non-IP caller ID authentication standards satisfy the TRACED Act's requirement using the Commission's proposed criteria for evaluating non-IP frameworks. Specifically, we propose to conclude that In-Band Authentication (ATIS-1000095.v002) and Out-of-Band Multiple STI-CPS Authentication (ATIS-1000096) are both developed and reasonably available, and therefore satisfy the requirements for repealing the non-IP caller ID authentication continuing extension. We also propose to conclude that these two standards are effective, and therefore satisfy the requirement for providers to take reasonable measures to implement effective non-IP caller ID authentication. We seek comment on whether the newest standard, Out-of-Band Agreed STI-CPS Authentication (ATIS-1000105) also satisfies the TRACED Act's requirements using the criteria. We also seek comment on whether any other non-IP frameworks have been developed that meet the TRACED Act's requirements using the criteria. Additionally, we propose a streamlined process for evaluating non-IP caller ID authentication frameworks in the future.

#### a. Developed and Reasonably Available Frameworks

35. We propose to conclude that frameworks using all three ATIS non-IP standards meet the first criterion for repealing the continuing extension because they are "fully developed and finalized by industry standards."[117] Specifically, we propose to conclude that because ATIS is a well-established standards development organization, frameworks using all three standards are standards-based and their fundamental aspects are standardized.[118] We propose to recognize that the technical elements of all three frameworks have been published and are accessible by providers and vendors that make frameworks commercially available.[119] We further propose to conclude that there is consensus within the industry that all three frameworks are developed, given that final versions of all three standards have been approved by ATIS, an industry standards organization.[120] Additionally, we propose to conclude that because record evidence indicates that both In-Band Authentication and Out-of-Band Multiple STI-CPS Authentication

[115] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1874, para. 31.

[116] *Id.* at 1873-74, para. 31 (stating, under the Commission's interpretation at the time, that "significant industry consensus is an important predicate to deeming a non-IP solution 'effective'").

[117] *Id.* at 1874, para. 32.

[118] *See, e.g.*, Wabash Reply at 3 ("There certainly can't be any argument that multiple Non-IP standards were recently adopted and published through ATIS, and there's no contest about Non-IP SHAKEN in live-production today, and its availability."); *but see* GGI Reply at 2 ("[M]ultiple commenters agree that the ATIS Standards do not meet the thresholds — 'fully developed and finalized by industry standards' and 'reasonably available'—that would trigger mandatory implementation under the TRACED Act . . . .").

[119] *See* In-Band Authentication (ATIS-1000095.v002); Out-of-Band Multiple STI-CPS Authentication (ATIS-1000096); Out-of-Band Agreed STI-CPS Authentication (ATIS-1000105).

[120] In-Band Authentication (ATIS-1000095.v002) at 1 (noting that this version of the standard was approved Aug. 26, 2022); Out-of-Band Multiple STI-CPS Authentication (ATIS-1000096) at i. (noting that the standard was approved on July 15, 2021); Out-of-Band Agreed STI-CPS Authentication (ATIS-1000105) at i. (noting that the standard was approved Dec. 2, 2024).

have been implemented by at least some providers, they qualify as fully developed and finalized.[121] We seek comment on these proposed conclusions. We also seek comment on whether Out-of-Band Agreed STI-CPS Authentication is ready for implementation, and whether it has been implemented by any providers. We seek comment on whether there are any ongoing efforts to further develop or improve any of the standards either inside or outside of ATIS.[122] If so, what are the substance of such revisions and what problems or shortcomings in the standards are they designed to solve? What progress is industry making to complete any further development? Have all fundamental aspects of each standard which enable their effectiveness been standardized by industry? Are there any other factors we should consider when evaluating whether each of the standards is fully developed and finalized by industry standards?

36. Next, we propose to conclude that frameworks using In-Band Authentication and Out-of-Band Multiple STI-CPS Authentication are reasonably available such that the underlying equipment and software necessary to implement those frameworks are commercially available, and therefore meet the second criterion for repealing the continuing extension. Record evidence (from December 2022 and January 2023) indicates that frameworks using In-Band Authentication and Out-of-Band Multiple STI-CPS Authentication have been implemented by some providers, which suggests that the necessary equipment and software is commercially available. For instance, we note that TelcoBridges explained it "offers technology solutions for both" standards.[123] Regarding In-Band Authentication, NCTA noted that at least two providers "have successfully demonstrated an in-band band solution."[124] With respect to Out-of-Band Multiple STI-CPS Authentication, the Cloud Communications Alliance stated that Neustar "offers an out-of-band solution"[125] and its members "have undertaken the expense of enabling out-of-band solutions for their networks. . . ."[126] TransNexus explained that it knows "of about 50 providers currently using Out-of-Band [Multiple STI-CPS],"[127] and appears to continue to offer an out-of-band solution,[128] as does TransUnion.[129] We seek additional information concerning the commercial availability, marketing, and deployment of frameworks based on these standards. Have there been increases or decreases in deployments of such frameworks since the *Notice of Inquiry*? If so, are such increases or decreases relevant to their "commercial availability"? We also seek comment on whether some or all current in-band and out-of-band deployments rely on proprietary elements not outlined in the standard and whether the use of or need to use proprietary elements bear on whether we should conclude that frameworks based on either standard are reasonably available.[130] Are any of the frameworks or associated standards subject

[121] *See, e.g.*, TelcoBridges Comments at 5; NTCA Reply at 12; Cloud Communications Alliance at 3, 5; TransNexus Reply at 2 n.5.

[122] WTA explained in 2022 that it believes that "there is no open or ongoing ATIS proceeding regarding further refinement or revision of the In-Band standard . . . ." WTA Comments at 6.

[123] TelcoBridges Comments at 4.

[124] NTCA Reply at 12 ("As the Cloud Communications Alliance states, TelcoBridges . . . and TransNexus, have successfully demonstrated an in-band solution based on the ATIS-1000095v.002 standard.") (internal citations omitted).

[125] Cloud Communications Alliance Comments at 3.

[126] *Id.* at 5.

[127] TransNexus Reply at 2 n.5.

[128] TransNexus, *Out-of-Band Shaken*, https://transnexus.com/whitepapers/out-of-band-shaken/ (last visited Apr. 23, 2025) ("We offer STIR/SHAKEN and robocall mitigation solutions in our ClearIP and NexOSS software platforms. These platforms fully support Out-of-Band Shaken.").

[129] TransUnion, *Enhancing Call Authentication: Unraveling the Impact of STIR/SHAKEN* (Aug. 21, 2023), https://www.transunion.com/blog/enhancing-call-authentication-unraveling-the-impact-of-stir-shak?atvy=%7B"264995"%3A"Experience+B"%7D.

[130] *See* USTelecom Comments at 16 (implying that the solutions implementing Out-of-Band Multiple STI-CPS Authentication were "limited" and "proprietary" and not consistent with the published standard); NCTA Reply at 2 (continued….)

to patents or other intellectual property restrictions? We propose to conclude that the governance structure required by Out-of-Band Multiple STI-CPS Authentication does not affect our proposed conclusion that frameworks using this standard are reasonably available.[131] We believe that existing governance structures utilized under STIR/SHAKEN can be expanded to fulfill Out-of-Band Multiple STI-CPS Authentication requirements without unreasonable burden on the existing governance structures or the Commission.[132] We seek comment on this proposed conclusion. Additionally, we seek comment on the cost and burdens of implementing these frameworks, including whether they can be reasonably borne by providers and their relevance to a framework's "commercial availability."[133] Does the reasonability depend on the size and type of provider and structure and location of its network?[134] How many voice service providers with 100,000 or fewer voice service subscriber lines have implemented frameworks using each of these standards?[135] If a framework is not cost effective in some cases or for some providers, can it still be considered reasonably available? Should the Commission consider any other factors when evaluating whether a framework is reasonably available?

37. We seek comment on whether frameworks using Out-of-Band Agreed STI-CPS Authentication are reasonably available such that the underlying equipment and software necessary to implement them are commercially available, as we do not believe we have sufficient information yet to evaluate their availability. In particular, we seek comment on any pending or current implementation of frameworks using Out-of-Band Agreed STI-CPS Authentication by vendors or providers. Have vendors

(Continued from previous page)
(citing USTelecom's statement and saying that TransNexus' and Neustar's out-of-band deployments are proprietary); TransNexus Comments at 4, 13 (noting that it built its own Call Placement Service, which the published standard assumes would be subject to a governance authority); *but see id.* at 15 (stating that it knows that at least two vendors, itself and netnumber, offer out-of-band solutions based on the ATIS standard).

[131] *See* ATIS-1000097.v003 at 15-17 (stating that the Out-of-Band Multiple STI-CPS Authentication requires a "governance authority and policy administrator" that involves an "STI-CPS mesh across all participating service providers with each having access to at least one STI-CPS," necessary "to support STI-CPS discovery and issue STI-certificates to the STI-CPS"); TransNexus Comments at 13 (stating that the mesh network connects multiple STI-CPSs managed through a "governance structure").

[132] *See* NTCA Reply at 15 (arguing that the STI-GA is capable of taking over governance and that USTelecom's arguments to the contrary are merely stalling tactics meant to delay approval of the standard); Wabash Reply at 2 (agreeing that the STA-GA can take on the task and noting that "the STI-GA has consistently taken on additional responsibilities directly related to SHAKEN"); TransNexus Comments at 13, n.25 (arguing the STI-PA should provide the STI-CPS list).

[133] *See* TelcoBridges Comments at 4 (asserting that the "gateway device" that some providers may need for interconnection to IP networks "range from approximately $1,000 to $40,000 depending on size and capacity"); TransNexus Comments at 11 (saying that the gateway devices "start at about $7,000 each" with more expensive "[h]igher-capacity units capable of handling larger call volumes . . ."); USTelecom Reply at 7 (stating that "at least one USTelecom member indicated that it could cost the company hundreds of millions of dollars to implement certain of these solutions as it may be necessary to either add equipment at virtually every TDM switch or build new TDM trunks to every TDM switch").

[134] *See, e.g.*, Aureon Comments at 8 (explaining how Out-of-Band Multiple STI-CPS Authentication is more cost effective for small and rural providers than In-Band Authentication); TelcoBridges Comments at 4-5 ("The cost [of a non-IP software solution] depends on the size and capacity of the gateway device; those that handle greater call volumes are more expensive. . . . The time to implement an out-of-band or in-band solution varies depending on the functionalities existing in the network.").

[135] *See* 47 CFR § 64.6304(a)(2) (defining a small voice service provider as "a provider that has 100,000 or fewer voice service subscriber lines (counting the total of all business and residential fixed subscriber lines and mobile phones and aggregated over all of the provider's affiliates)"); *see also* Letter from Dave Frigen, Chief Operating Officer, Wabash Communications, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 17-97, at 2-3 (filed Aug. 17, 2021) (noting that it has been using Out-of-Band Multiple STI-CPS Authentication "for over a year . . . and it works very well").

and providers had sufficient time to develop software and equipment based on the standard? If not, do they plan to do so and how long will it take? Do vendors and providers believe that it will be easier or more difficult than the other non-IP standards to implement frameworks based on Out-of-Band Agreed STI-CPS Authentication in their equipment and networks? If frameworks based on Out-of-Band Agreed STI-CPS Authentication have been developed, are there any proprietary elements to any such frameworks? Is the standard or any associated frameworks subject to patents or other intellectual property restrictions? Are frameworks being offered and marketed to providers? What are the costs of these frameworks and can those costs be reasonably borne by providers?

**b. Effective Frameworks**

38. We propose to conclude that frameworks using In-Band Authentication and Out-of-Band Multiple STI-CPS Authentication satisfy the proposed criteria for determining whether a non-IP caller ID authentication framework is effective. First, we propose to conclude that these frameworks satisfy the first two criteria of effectiveness—developed and reasonably available—based on our proposed conclusion above that they satisfy these TRACED Act requirements. Second, we propose to conclude that these frameworks are effective under the plain meaning of the TRACED Act because they operate to produce the intended result of authenticating calls as described in the applicable standard. We believe that record evidence of deployments of In-Band Authentication and Out-of-Band Multiple STI-CPS Authentication frameworks in the marketplace are *prima facie* evidence that these frameworks are in fact operating to authenticate calls as described in each standard, as providers would otherwise be unlikely to implement them in the absence of a mandate.[136] We also note record evidence indicating that the two standards are interoperable, i.e., that they will continue to operate to authenticate calls even if other providers in the call path are using frameworks based on the other standard.[137] We seek comment on our proposed conclusion. Do commenters have additional evidence concerning testing or real-world deployments showing whether these frameworks, when implemented as designed, successfully authenticate calls? What is the experience of those who have implemented these two types of frameworks? Are there any other bases for concluding that frameworks using In-Band Authentication and Out-of-Band Multiple STI-CPS Authentication do or do not authenticate calls as intended under the standards based on the plain meaning of the TRACED Act?

39. We also seek comment regarding whether frameworks using Out-of-Band Agreed STI-CPS Authentication are effective under the TRACED Act. We note that we propose to conclude above that, although we believe frameworks using Out-of-Band Agreed STI-CPS Authentication are developed, we do not have sufficient evidence to determine whether they are reasonably available, and we sought comment on that criterion. We similarly do not believe we have sufficient evidence to determine whether these frameworks are effective under the ordinary meaning of the word, and seek comment on that criterion. Is there any evidence of testing or marketplace deployments that would show that Out-of-Band Agreed STI-CPS Authentication frameworks operate to produce the intended result of authenticating calls as described in the standard? Will Out-of-Band Agreed STI-CPS Authentication undermine the effectiveness of frameworks based on the other standards or will use of those other frameworks impact the effectiveness of Out-of-Band Agreed STI-CPS Authentication? Are there other factors relevant under the plain meaning of the TRACED Act that we should consider? Can and should we preclude use of certain frameworks even if a framework is otherwise effective in order to prevent interoperability issues?

---

[136] *See, e.g.*, TelcoBridges Comments at 5; NTCA Reply at 12, Cloud Communications Alliance at 3, 5; TransNexus Reply at 2 n.5.

[137] ATIS-1000097.v003 at 11 (concluding that STIR/SHAKEN Over TDM and Out-of-Band Multiple STI-CPS Authentication "may be used independently by different service providers in the call path . . ."); *id.* ("At minimum, service providers need to support configuration of approach per TDM interface and implement an approach that is supported by the service providers they interconnect with. This may require some service providers to implement more than one approach for call authentication to be transmitted end-to-end.").

40. *Other non-IP caller ID Authentication frameworks.* We seek comment on whether there are any other non-IP frameworks that we should evaluate using our criteria. For instance, are there any other standards either ratified or in development by ATIS, IETF, or any other standards organization that we should consider? Are there proprietary frameworks that we should consider or be aware of that might meet the TRACED Act requirements? For example, the Commission noted in the *Notice of Inquiry* that AB Handshake has previously submitted a proprietary solution for consideration.[138] At least two commenters explained that the AB Handshake solution, "meets the Commission's standards for effectiveness."[139] Should we consider AB Handshake or other providers' solutions?[140] We also note that IETF appears to be developing a new out-of-band standard.[141] We seek comment on its development status and how it may differ from the three ATIS standards discussed above. If there are other frameworks that commenters believe we should consider, we seek comment on the application of the criteria and factors described above to those frameworks, as well as other considerations we should take into account when evaluating the frameworks.[142]

41. *Streamlined evaluation process.* We propose to create a streamlined process the Commission can use going forward to determine whether other non-IP caller ID authentication frameworks are "effective" under the criteria we propose to adopt today. Specifically, we propose to delegate to the Wireline Competition Bureau the authority to seek comment on whether a non-IP caller ID authentication framework is effective under the Commission-established criteria, evaluate the framework using the criteria, and make final determinations about a framework's effectiveness. We believe this approach will ensure that providers can rapidly take advantage of such frameworks. We seek comment on this proposal, including any implementation issues we should consider.[143] We also propose, consistent with the approach we took with STIR/SHAKEN,[144] to permit providers continuing to rely on non-IP networks to adopt improved versions of any approved standards or frameworks as they become available in the future.

### B. Mandating Implementation of Non-IP Caller ID Authentication

42. We propose to conclude that the development and availability of effective non-IP caller

[138] *See Notice of Inquiry*, 37 FCC Rcd at 13645, paras. 3, 32 n.108 (describing the AB Handshake solution).

[139] Aureon Reply at 8; *see also* Cloud Communications Alliance Comments at 4, 6-7.

[140] *See, e.g.*, TransNexus Comments at 16 ("We discourage the Commission from launching a search for other alternative approaches. Considerable time and effort have gone into producing these non-IP standards.").

[141] *See* IETF, *Out-of-Band STIR for Service Providers*, https://datatracker.ietf.org/doc/draft-ietf-stir-servprovider-oob/ (last visited Apr. 23, 2025).

[142] Some commenters responding to the *Notice of Inquiry* discussed alternative IP voice traffic delivery methods, such as transmission over the public Internet. *See, e.g.*, Verizon Comments at 3 (noting the 2022 SIP Interconnection Working Group Report on, among other things, internet-delivered IP voice traffic, and describing the development of its own such products). We do not believe these alternatives bear on whether non-IP caller ID authentication solutions meet the TRACED Act's requirements and warrant mandating non-IP caller ID authentication, but commenters are invited to provide information otherwise.

[143] We note that the Commission previously delegated to the Bureau the authority to seek comment on requiring providers to comply with new versions of the existing STIR/SHAKEN standards and to require use of such standards. *See Sixth Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking*, 38 FCC Rcd at 6876, para. 25.

[144] *See First Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking*, 35 FCC Rcd at 3258-59, para. 36 (requiring, at a minimum, compliance with the most recent versions of ATIS-1000074, ATIS-1000080, and ATIS-1000084); *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1927, para. 142 (explaining that the Commission encourages "innovation and improvement to the STIR/SHAKEN framework, so long as any changes or additions do not compromise the baseline call authentication functionality envisioned" by the three ATIS STIR/SHAKEN standards).

ID authentication frameworks warrants mandating that providers that continue to maintain non-IP infrastructure to either upgrade their networks to IP or to implement one or more non-IP caller ID authentication frameworks in their non-IP networks. To effectuate this mandate, we believe the Commission must, pursuant to the TRACED Act, repeal the continuing extension from caller ID authentication obligations for providers relying on non-IP network infrastructure in section 64.6304(d) of our rules and modify section 64.6303 (the "reasonable measures" rule) to require that such providers either upgrade their networks to IP or implement one or more non-IP caller ID authentication solutions. We seek comment on this proposed conclusion. Below we discuss and seek comment on repeal of the continuing extension and modification of the "reasonable measures" rule. We also propose and seek comment on conforming modifications to the rules governing Robocall Mitigation Database filing requirements to account for the proposed non-IP caller ID authentication mandate.

43. *Repealing the continuing extension.* In connection with our proposed determination above that non-IP caller ID authentication frameworks are developed and reasonably available, we propose to repeal the continuing extension from robocall mitigation obligations granted to providers that rely on non-IP technology.[145] Section 4(b)(5)(B) of the TRACED Act requires the Commission to "grant a delay of required compliance" with the implementation deadline for non-IP caller ID authentication for voice service providers materially reliant on non-IP networks "until a call authentication protocol has been developed for calls delivered over non-[IP] networks and is reasonably available."[146] Providers reliant on non-IP technology therefore "are deemed subject to a continuing extension" under the Commission's rules.[147] As explained above, we believe that frameworks based on certain ATIS standards qualify as developed and reasonably available and therefore justify repeal of the continuing extension. Are there other factors the Commission must or should consider before repealing the continuing extension? If the Commission determines that non-IP caller ID authentication frameworks have been developed and are reasonably available, does it have any discretion under the TRACED Act to maintain the continuing extension?

44. *Modifying the "reasonable measures" rule.* In connection with our proposed determination above that available non-IP caller ID authentication frameworks are effective, we propose to modify section 64.6303 of our rules, which implements the TRACED Act's "reasonable measures" requirement, to mandate that providers either upgrade their networks to IP or implement one or more non-IP caller ID authentication frameworks. Under section 4(b)(1)(B) of the TRACED Act, voice service providers must "take reasonable measures to implement an effective call authentication framework in [their] non-internet protocol networks."[148] In the *Second Caller ID Authentication Report and Order*, the Commission concluded that "[a] voice service provider satisfies this obligation by either (1) completely

[145] *See* 47 CFR § 64.6304(d). We also propose additional changes to our caller ID authentication rules to remove obsolete rules and make non-substantive corrections. First, we propose to delete rules in section 64.6304 that pertain to extensions for small voice service providers (except for small voice service providers that originate calls via satellite using North American Numbering Plan numbers), services scheduled for section 214 discontinuance, and provider-specific extensions, as those extensions were time-limited and have since expired. *See* Appendix A. Second, we propose to delete all of section 64.6306, which we do not believe is necessary any longer, as it implemented the TRACED Act's requirement to provide an exemption from call authentication obligations for providers who certified by a date that has since passed that they were implementing call authentication. *See id.* Third, we propose to make a non-substantive correction to section 64.6302 concerning intermediate providers' attestation-level decisions regarding the caller ID information of each SIP call they receive. *See id.* We seek comment on these proposals.

[146] 47 U.S.C. § 227b(b)(5)(B). The Commission issued this continuing extension in the *Second Caller ID Authentication Report and Order*. *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1892-96, paras. 66-70; *see also* 47 CFR § 64.6304(d).

[147] 47 CFR § 64.6304(d).

[148] 47 U.S.C. § 227b(b)(1)(B).

upgrading its non-IP networks to IP and implementing the STIR/SHAKEN authentication framework on its entire network, or (2) working to develop a non-IP authentication solution."[149] At the time, the Commission stated that "[i]f and when we identify an effective framework, we expect to revisit our 'reasonable measures' requirement and shift it from focusing on development to focusing on implementation."[150] Since we propose to conclude that available non-IP caller ID authentication frameworks are effective, we propose to modify this rule to state that a provider with a non-IP network satisfies the "reasonable measures" requirement by either (1) completely upgrading its non-IP networks to IP and implementing the STIR/SHAKEN authentication framework on its entire network, or (2) implementing one or more effective non-IP caller ID authentication frameworks. We propose to make similar modifications in section 64.6303 for gateway providers and non-gateway intermediate providers receiving calls directly from an originating provider. We believe this approach would continue to promote the IP transition, which is the most effective method for achieving caller ID authentication on phone networks and obviates the need for providers to implement non-IP caller ID authentication frameworks. Additionally, we propose to add a provision in section 64.6303 to make clear that intermediate providers, including gateway providers, must pass unaltered to the subsequent intermediate provider or voice service provider in the call path any non-IP caller ID authentication information it receives, except where necessary for technical reasons to complete the call and where the intermediate provider reasonably believes the non-IP caller ID authentication information presents an imminent threat to its network security, mirroring the requirement on intermediate providers for STIR/SHAKEN authentication information.[151] We seek comment on whether additional rule revisions are necessary to ensure that both STIR/SHAKEN and non-IP caller ID authentication information are passed to the next provider in the call path regardless of whether the network is IP or non-IP. We also propose to add a definition for "effective non-IP caller ID authentication framework" in section 64.6300, to mean a non-Internet Protocol caller identification authentication framework that the Commission has determined to be effective under 47 U.S.C. § 227b(b)(1)(B).

45. We seek comment on these proposals and their implications. What are the costs and benefits of requiring providers to either complete their IP transitions or implement a non-IP caller ID authentication framework? Would removing the option allowing providers to meet the "reasonable measures" requirement by working to develop a non-IP caller ID authentication solution disincentivize providers from participating in efforts to develop other non-IP caller ID authentication solutions that may be more effective or to improve the non-IP caller ID authentication solutions that have already been developed so that they are more effective? Should we require that providers who do not upgrade their networks to IP both implement non-IP caller ID authentication frameworks and continue to work to develop or improve non-IP caller ID authentication solutions? Are there any other issues or alternative approaches we should consider?

46. *Conforming Robocall Mitigation Database rules.* We propose changes to the Commission's Robocall Mitigation Database rules to conform them with the proposed non-IP caller ID authentication mandate. Specifically, we propose a new requirement for providers to certify in the Robocall Mitigation Database whether they have implemented a non-IP caller ID authentication framework in their non-IP networks. We seek comment on this proposal and whether we should take a different approach implementing the requirement in our rules. Should we further require such providers to certify which Commission-approved non-IP caller ID authentication frameworks they have implemented? What would be the benefits and costs of such additional requirement? We also seek comment on whether and to what extent we should modify any other Robocall Mitigation Database filing

[149] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1871, para. 24; *see also* 47 CFR § 64.6303(a).

[150] *See id.* at 1874, para. 32.

[151] *See* 47 CFR § 64.6302(a); *see also* CCA et al. *Ex Parte* at 2 (requesting that we ensure the proposed non-IP caller ID authentication requirements apply to all intermediate providers in the call path).

requirements or rules to account for our non-IP caller ID authentication requirement. In providing such feedback, we encourage providers to consider how we would implement any rule changes in the Robocall Mitigation Database submission form.

### C. Compliance Deadline

47. We propose a two-year timeline for providers that continue to maintain non-IP infrastructure to either complete their IP transitions or fully implement one or more of the available non-IP caller ID authentication frameworks in their non-IP networks.[152] We seek comment on this proposal. In the *Notice of Inquiry*, the Commission sought comment on a reasonable implementation timeline for deployment of one or both non-IP caller ID authentication frameworks.[153] Several commenters agreed the Commission should set a deadline for providers to implement a non-IP framework if they have not completed their IP transition by that date,[154] and others proposed a specific date, which has since passed.[155]

48. In the TRACED Act, Congress made clear its intention for all calls to be authenticated, and that it did not intend for the non-IP implementation extension to last indefinitely.[156] Four years have passed since caller ID authentication obligations have been in effect, during which time advancements in the IP transition have occurred while providers continuing to rely on non-IP technology have certified that they have participated in efforts to develop non-IP caller ID authentication solutions.[157] As proposed above, we believe there are now non-IP caller ID authentication frameworks that meet the requirements in the TRACED Act and Commission rules. Given subsequent industry progress in the IP transition and in the development and deployment of non-IP frameworks, we believe that a two-year compliance timeline appropriately balances the strong public interest in closing the non-IP caller ID authentication gap as soon as possible with the need for providers to have sufficient time to implement the approach that makes the most sense for their networks and business models.[158] We seek comment on this proposed compliance

---

[152] Under our proposal, the two-year timeline would commence from the effective date of any implementing rules we adopt.

[153] *Notice of Inquiry*, 37 FCC Rcd at 13464, para. 30.

[154] *See* American Bankers Association et al. Reply at 3-4; Cloud Communications Alliance Reply at 1, 5.

[155] Carolina Digital Phone Comments at 1 (proposing a June 30, 2023 deadline); *accord* Cloud Communications Alliance Comments at 5; *see also* Freshphone comments at 1 ("We ask the FCC to require any non-IP carrier to be in full compliance with STIR/SHAKEN by June 2023."); MDU1 Comments at 1 (accord); TRACI.net Comments at 1 (accord); WTA Comments at 1 ("June 30, 2023 . . . would appear to be a reasonable time for at least beginning the phase-out of the non-IP network extension.").

[156] *See* 47 U.S.C. § 227b(b)(5)(B) (directing the Commission to grant a delay of required compliance for voice service providers that "materially rel[y] on a non-[IP] network . . . until a call[er ID] authentication protocol has been developed for calls delivered over non-[IP] networks and is reasonably available"); S. Rep. No. 116-41, 116th Cong., 1st Sess., at 5 ("[I]t is necessary to implement call authentication technologies to reduce robocalls . . . . [T]he TRACED Act would help to ensure the speedy implementation of these authentication technologies and protect consumers.").

[157] *See, e.g.*, Competitive Carriers Association Comments at 2 ("Many CCA members have upgraded their networks to be fully IP-based, and others continue to upgrade significant parts of their networks."); 47 CFR §§ 64.6304(d), 64.6303(a) (requiring providers claiming the STIR/SHAKEN implementation extension for non-IP networks to either upgrade their entire networks to allow for the initiation, maintenance, and termination of SIP calls, or be working to develop a non-IP caller identification authentication solution, or actively testing such a solution); *see generally* FCC, *Robocall Mitigation Database*, https://www.fcc.gov/robocall-mitigation-database (last visited Apr. 23, 2025).

[158] Congress directed the Commission in the TRACED Act to "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." 47 U.S.C. § 227b(b)(5)(D).

timeline.

49. Specifically, we ask that commenters address how any remaining technical, financial, or other obstacles may affect the time needed to implement any of the discussed non-IP caller ID authentication frameworks. We note that the Commission previously adopted compliance timelines of roughly 15 months for voice service providers, 13 months for gateway providers, and 10 months for certain non-gateway intermediate providers to implement STIR/SHAKEN in their IP networks,[159] and providers were generally able to meet those deadlines.[160] Accordingly, would the significantly longer two-year compliance timeline we propose here be necessary to reasonably account for any additional burdens providers may face in implementing one of the non-IP frameworks?[161] Is a shorter timeline warranted given that some providers have already begun to implement one or both of the commercially available non-IP frameworks?[162] Is two years adequate time for providers to make adjustments to any existing contractual arrangements that may be impacted by implementing one or more of the non-IP frameworks? Are there any technical or operational hurdles unique to the non-IP caller ID authentication frameworks that require additional time for providers to comply? If commenters believe that more or less time is needed to implement one or more of the commercially available non-IP caller ID authentication frameworks, they should discuss specific reasons why our proposed two-year timeline is insufficient or too long, propose an alternative timeline, and provide detail on why their proposed alternative is appropriate.

50. Above, we seek comment on whether the costs and operational hurdles associated with implementing non-IP frameworks vary depending on the size and type of provider and the structure and location of a provider's network. If they do, should we modify our proposed timeline for certain classes of providers? Or would doing so undermine the value of any requirements we adopt? For example, the Commission previously granted an extension of the STIR/SHAKEN implementation deadline for voice service providers with 100,000 or fewer subscriber lines, including small rural providers,[163] and subsequently accelerated the extended deadline by one year for non-facilities-based small voice service

[159] *See generally First Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking* (adopted on March 31, 2020, and requiring voice service providers to implement STIR/SHAKEN by June 30, 2021); *Gateway Provider Report and Order and Further Notice of Proposed Rulemaking* (adopted May 19, 2022, and requiring gateway providers to apply STIR/SHAKEN to all unauthenticated foreign-originated SIP calls with U.S. North American Numbering Plan numbers by June 30, 2023); *Sixth Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking* (adopted March 16, 2023, and requiring non-gateway intermediate providers that receive unauthenticated SIP calls directly from an originating provider to use STIR/SHAKEN to authenticate those calls by December 31, 2023).

[160] *See, e.g.*, Cloud Communications Alliance Comments at 2 ("The telecommunications industry, including members of the Alliance, have invested substantial capital and human resources to implement the STIR/SHAKEN framework . . . [in part] as a matter of regulatory compliance . . . ."). Our rules adopted pursuant to the TRACED Act granted certain providers extensions from this deadline and permitted providers to request exemptions. *See* 47 CFR § 64.6304 (granting extensions to various classes of providers); *id.* § 64.6306 (establishing a process to obtain an exemption).

[161] Both TransNexus and TelcoBridges say that deployment time depends on the existing network capabilities, but can be as short as a few days. *See* TelcoBridges Comments at 4-5; TransNexus Comments at 11-12.

[162] *See, e.g.*, TransNexus Comments at 4 ("We currently have about fifty service provider customers using our STIR/SHAKEN software with Out-of-Band enabled.").

[163] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1877-82, paras. 40-48 (adopting a two-year STIR/SHAKEN implementation extension until June 30, 2023, for small voice service providers); 47 CFR § 64.6304(a)(1).

providers.[164] Should we similarly adopt an extension for small providers to implement a non-IP caller ID authentication framework? If so, should we adopt different extensions for facilities and non-facilities-based small providers? Do certain classes of small providers, such as rural or intermediate providers, face unique challenges to implementing non-IP caller ID authentication? For purposes of the STIR/SHAKEN implementation extension for small voice service providers, the Commission considers a "small voice service provider" to be "a provider that has 100,000 or fewer voice service subscriber lines (counting the total of all business and residential fixed subscriber lines and mobile phones and aggregated over all of the provider's affiliates)."[165] Would a similar approach be appropriate in the non-IP caller ID authentication context, or should we adopt a different threshold? If so, why? Are there certain gateway and non-gateway intermediate providers that warrant an extension, such that the extension should not be tied to the number of subscriber lines? If so, how should we determine the class or classes of such providers subject to an extension? If we grant an extension to some providers, how much additional time would be appropriate in light of the public interest in promptly closing the non-IP caller ID authentication gap? How would any extension account for the importance of ubiquitous caller ID authentication? Instead of a categorical approach, should we instead rely on individualized waiver requests pursuant to the Commission's longstanding waiver standard?[166]

51. We invite commenters to address how our proposed compliance timeline relates to providers' efforts to transition their networks to IP technology. In the *Notice of Inquiry*, we sought comment on the status of providers' efforts to fully transition their networks to all-IP technology and the effect that a non-IP caller ID authentication requirement would have on the IP transition's progress.[167] We seek additional comment on this issue in light of our proposed mandate of non-IP caller ID authentication and the Commission's recent efforts to ease regulatory barriers to IP transitions.[168] For example, should any compliance timeline take into account providers' assertions about the time it would take to transition their networks to all IP? Do providers opting to fully upgrade their networks to IP face unique challenges that counsel for a longer compliance timeline? Would two years give providers adequate time to adjust existing contractual arrangements, or to negotiate new ones, as a result of upgrading their networks to all IP? What, if any, technical or financial circumstances affect providers' ability to transition to all-IP technology that our proposed timeline does not account for? To the extent that providers believe that transitioning their networks to IP warrants a longer compliance timeline, they should propose a specific alternative compliance timeline, and discuss in detail the reasons that such providers need additional time to comply.

### D. Cost-Benefit Considerations

52. We seek comment on the costs and benefits associated with requiring providers to implement a non-IP caller ID authentication framework. As explained above, the TRACED Act requires that the Commission provide a continuing extension from implementing a non-IP caller ID authentication framework to providers materially reliant on non-IP networks "until a call authentication protocol has

---

[164] *See generally Call Authentication Trust Anchor*, WC Docket No. 17-97, Fourth Report and Order, 36 FCC Rcd 17840 (2021) (accelerating the STIR/SHAKEN implementation extension for small voice service providers by one year to June 30, 2022, for non-facilities-based small voice service providers); 47 CFR § 64.6304(a)(1)(i).

[165] 47 CFR § 64.6304(a)(2).

[166] The Commission may exercise its discretion to waive a rule where the particular facts at issue make strict compliance inconsistent with the public interest. *Northeast Cellular Tel. Co. v. FCC*, 897 F.2d 1164, 1166 (D.C. Cir. 1990). In considering whether to grant a waiver, the Commission may take into account considerations of hardship, equity, or more effective implementation of overall policy on an individual basis. *WAIT Radio v. FCC*, 418 F.2d 1153, 1159 (D.C. Cir. 1969).

[167] *Notice of Inquiry*, 37 FCC Rcd at 13467-69, paras. 37-39.

[168] *See generally Technology Transitions Order on Clarification*; *Discontinuance Waiver Order*; *214 Grandfathering Order*; *Network Change Waiver Order*.

been developed for calls delivered over non-[IP] networks and is reasonably available."[169] Thereafter, providers must take reasonable measures to implement an effective caller ID authentication framework in their non-IP networks,[170] which we propose to mean implementing a non-IP caller ID authentication framework for providers that continue to rely on non-IP networks by the end of the proposed two-year transition period. Because implementation of a non-IP framework and its accompanying costs must be incurred at some point, we propose to focus our cost-effectiveness analysis on timing, rather than the implementation requirement. Under that proposed focus, we believe the Commission must weigh the costs and benefits of imminent action versus further delay.

53. We believe that the potential cost of mandating one or more non-IP caller ID authentication frameworks at a particular point in time is that a more effective or efficient framework meeting the TRACED Act's requirements could become available after providers have already incurred implementation costs for any approved frameworks. Given that we propose that two commercially available non-IP caller ID authentication frameworks meet the TRACED Act's requirements, propose to allow providers to use later versions of those frameworks if any are released, and propose a streamlined process for the Bureau to evaluate going forward whether other non-IP caller ID authentication frameworks meet the TRACED Act's requirements, we believe that this potential cost is small. We seek comment on the size of this potential cost and on measures we might adopt to avoid or minimize this cost. Additionally, we seek comment on the nature and magnitude of other possible costs of requiring implementation of non-IP caller ID authentication frameworks on the timeline we propose.

54. We believe that the benefits of mandating implementation of non-IP caller ID authentication frameworks on the timeline we propose are vast. Reducing the billions of dollars robocalls cost from wasted time, nuisance, and fraud, which totaled $13.5 billion in 2020 alone,[171] hinges on closing loopholes that enable robocallers to evade detection. Some large portion of that savings must be attributed to closing the non-IP caller ID authentication gap. Moreover, the Commission previously estimated that unchecked robocalls could reduce public welfare by billions of dollars annually, meaning even a small percentage reduction in those calls could confer tens of millions in benefits annually.[172] Each type of benefit is lost every year the Commission delays implementing a non-IP fix. To better refine our benefits estimate, we seek comment on the magnitude—in both absolute and relative terms—of robocall volume originating on or transiting non-IP networks. More broadly, we seek comment on our benefit estimates and the data and methods underlying those estimates, as well as additional information that may inform our estimates. We seek comment on the nature and magnitude of any possible benefits not included in our analysis.

### E. Legal Authority

55. We seek comment on the Commission's legal authority to adopt the proposals outlined above. In particular, we propose that the TRACED Act, the Truth in Caller ID Act, and section 251(e) of the Communications Act provide the Commission with ample authority to adopt the rules implementing the proposals discussed herein. We note that the Commission has long invoked these same statutory provisions to adopt caller ID authentication obligations.[173] We seek comment on this proposal, and on

[169] 47 U.S.C. § 227b(b)(5)(B).

[170] *Id.* § 227b(b)(1)(B).

[171] *See First Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking*, 35 FCC Rcd at 3263, paras. 47-48.

[172] *See Call Blocking Eighth Report and Order* at 14, para. 32 (observing, in the call blocking context, that "eliminat[ing] a small share of unwanted and illegal calls" would "save millions annually in avoided fraud, aggravation, inconvenience, and mistrust").

[173] For example, in the *Second Caller ID Authentication Report and Order*, the Commission found that the text of the TRACED Act provided authority to adopt rules implementing section 4(b)(1)(B) for originating and terminating providers, while section 251(e) and the Truth in Caller ID Act provided further, independent sources of authority for (continued….)

any alternative sources of legal authority upon which we could rely.

56. As the Commission observed in the *Notice of Inquiry*, section 4(b)(1)(B) of the TRACED Act directs the Commission to require voice service providers to take "reasonable measures to implement" a non-IP caller ID authentication framework in their non-IP networks.[174] This language appears to contemplate Commission rules requiring voice service providers to implement one or more non-IP caller ID authentication frameworks. Do the statutory provisions discussed above continue to provide us authority to require voice service providers to implement one or more non-IP caller ID authentication frameworks? Do commenters read the language of section 4(b)(1)(B) as containing any limits on our ability to mandate implementation of a non-IP caller ID authentication framework by voice service providers?[175] Are there other potential sources of authority we should consider?

57. In addition to its authority under the TRACED Act, the Commission has consistently found independent authority for caller ID authentication requirements, including those applicable to intermediate providers, in section 251(e) of the Act and the Truth in Caller ID Act.[176] As the Commission explained in the *First Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking*, section 251(e) provides the Commission with exclusive, independent jurisdiction over numbering issues in the United States and "enables us to act flexibly and expeditiously with regard to important numbering matters[,]" including "[w]hen bad actors unlawfully spoof the caller ID that appears on a subscriber's phone[.]"[177] The Truth in Caller ID Act provides us with further authority to adopt rules that are "necessary to . . . protect voice service subscribers from scammers and bad actors."[178] Beginning with the *Second Caller ID Authentication Report and Order*, the Commission has repeatedly found both provisions to provide authority to impose caller ID authentication obligations on voice service providers and intermediate providers alike.[179] We seek comment on whether these provisions grant us sufficient authority to require intermediate providers to adopt a non-IP caller ID authentication framework.

## IV. PROCEDURAL MATTERS

58. *Regulatory Flexibility Act.* The Regulatory Flexibility Act of 1980, as amended (RFA),[180] requires that an agency prepare a regulatory flexibility analysis for notice-and-comment

(Continued from previous page)
rules applying to intermediate providers, as well as originating and terminating providers. *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1875, paras. 33-35; 47 U.S.C. §§ 227(e), 227b, 251(e).

[174] 47 U.S.C. § 227b(b)(1)(B) (stating that the Commission "shall . . . require a provider of voice service to take reasonable measures to implement an effective call authentication framework in the non-internet protocol networks of the provider of voice service").

[175] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1875, paras. 33-35; 47 U.S.C. §§ 227(e), 227b, 251(e).

[176] *See* 47 U.S.C. §§ 227(e), 251(e); *Sixth Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking*, 38 FCC Rcd at 2617, para. 91 (*citing First Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking*, 35 FCC Rcd at 3262, para. 44 and *Gateway Provider Report and Order and Further Notice of Proposed Rulemaking*, 37 FCC Rcd at 6911-12, para. 113).

[177] *First Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking*, 35 FCC Rcd at 3260-61, para. 42; *see* 47 U.S.C. § 251(e).

[178] *First Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking*, 35 FCC Rcd at 3262, para. 44; *see* 47 U.S.C. § 227(e).

[179] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1931-32, paras. 153-55; *see also Gateway Provider Report and Order and Further Notice of Proposed Rulemaking*, 37 FCC Rcd at 6911-12, para. 113; *Sixth Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking*, 38 FCC Rcd at 2617, para. 91.

[180] 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).

rulemaking proceedings, unless the agency certifies that "the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities."[181] 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 have a separate and distinct heading designating them as responses to the IRFA.

59. *Paperwork Reduction Act.* This *Notice of Proposed Rulemaking* may contain proposed new and revised information collection requirements. 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 the information collection requirements contained in this document, as required by the Paperwork Reduction Act of 1995, Public Law 104-13. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, *see* 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.

60. *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.

61. *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.[182] 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.[183]

62. *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

[181] *Id.* § 605(b).

[182] 47 CFR §§ 1.1206.

[183] *Id.* §§ 1.1200-1216.

ECFS: https://www.fcc.gov/ecfs/.

- Paper Filers: Parties who choose to file by paper must file an original and one copy 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.

63. *Accessible formats.* 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 (voice).

64. *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

65. Accordingly, pursuant to sections 4(i), 4(j), 201, 202, 217, 227, 227b, 251(e), 303(r), and 403 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), and 403, this *Notice of Proposed Rulemaking* IS ADOPTED.

66. 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 Advocacy of the Small Business Administration.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

## APPENDIX A

## Proposed Rules

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

**PART 64 – Miscellaneous Rules Relating to Common Carriers**

1. 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.

**Subpart HH – Caller ID Authentication**

2. Amend § 64.6300 by redesignating paragraphs (c) through (o) as (d) through (p) and adding paragraph (c).

**§ 64.6300 Definitions.**

* * * * *

(c) *Effective non-IP caller ID authentication framework.* The term "Effective non-IP caller ID authentication framework" means a non-Internet Protocol caller identification authentication framework that the Commission has determined to be effective under 47 U.S.C. § 227b(b)(1)(B).

* * * * *

3. Amend § 64.6302 by revising paragraph (f)(2) to read as follows:

**§ 64.6302 Caller ID authentication by intermediate providers.**

* * * * *

(f) * * *

* * * * *

(2) Makes all attestation-level decisions regarding the caller identification information of each SIP call it receives;

* * * * *

4. Amend § 64.6303 by revising the introductory text of paragraphs (a) through (c), revising paragraphs (a)(2), (b)(2), and (c)(2), and adding paragraph (d) to read as follows:

**§ 64.6303 Caller ID authentication in non-IP networks.**

(a) Not later than [[2 years after effective date]], a voice service provider with a network that relies on technology that cannot initiate, maintain, carry, process, and terminate SIP calls shall either:

* * * * *

(2) Implement one or more effective non-IP caller ID authentication frameworks in its non-Internet Protocol networks.

(b) Not later than [[2 years after effective date]], a gateway provider with a network that relies on technology that cannot initiate, maintain, carry, process, and terminate SIP calls shall either:

* * * * *

(2) Implement one or more effective non-IP caller ID authentication frameworks in its non-Internet Protocol networks.

(c) Not later than [[2 years after effective date]], a non-gateway intermediate provider receiving a call directly from an originating provider with a network that relies on technology that cannot initiate, maintain, carry, process, and terminate SIP calls shall either:

* * * * *

(2) Implement one or more effective non-IP caller ID authentication frameworks in its non-Internet Protocol networks.

(d) Except as provided in § 64.6304, not later than [[2 years after effective date]], an intermediate provider with a network that relies on technology that cannot initiate, maintain, carry, process, and terminate SIP calls shall pass unaltered to the subsequent intermediate provider or voice service provider in the call path any non-IP caller identification authentication information it receives with a call, subject to the following exceptions under which it may remove the authenticated caller identification information:

(1) Where necessary for technical reasons to complete the call; or

(2) Where the intermediate provider reasonably believes the caller identification authentication information presents an imminent threat to its network security.

5. Amend § 64.6304 by revising paragraph (a)(1), removing paragraphs (c), (d), and (e), and redesignating paragraph (f) as (c) to read as follows:

**§ 64.6304 Extension of implementation deadline.**

(a) *Small voice service providers.*

(1) Small voice service providers that originate calls via satellite using North American Numbering Plan numbers are deemed subject to a continuing extension of § 64.6301.

* * * * *

6. Amend § 64.6305 by redesignating paragraphs (d)(2) through (d)(5) as (d)(3) through (d)(6), (e)(2) through (e)(5) as (e)(3) through (e)(6), and (f)(2) through (f)(5) as (f)(3) through (f)(6), adding paragraphs (d)(2), (e)(2), and (f)(2), and revising redesignated paragraphs (d)(4) through (d)(6), (e)(4) through (e)(6), (f)(4) through (f)(6) to read as follows:

**§ 64.6305 Robocall mitigation and certification.**

* * * * *

(d) * * *

* * * * *

(2) A voice service provider relying on non-Internet Protocol networks shall certify that it has implemented one or more effective non-IP caller ID authentication frameworks in its non-Internet Protocol networks and all calls it originates on its non-Internet Protocol networks are compliant with § 64.6303(a).

* * * * *

(4) All certifications made pursuant to paragraphs (d)(1), (2), and (3) of this section shall:

* * * * *

(5) * * *

* * * * *

(vi) * * *

* * * * *

(C) A voice service provider without a STIR/SHAKEN implementation

obligation;

(vii) Whether the voice service provider is a voice service provider relying on non-Internet Protocol networks that has deployed one or more effective non-IP caller ID authentication frameworks; and

(viii) * * *

(6) A voice service provider shall update its filings within 10 business days of any change to the information it must provide pursuant to paragraphs (d)(1) through (5) of this section.

* * * * *

(e) * * *

* * * * *

(2) A gateway provider relying on non-Internet Protocol networks shall certify that it has implemented one or more effective non-IP caller ID authentication frameworks in its non-Internet Protocol networks and all calls it carries or processes its non-Internet Protocol networks are compliant with § 64.6303(b).

* * * * *

(4) All certifications made pursuant to paragraphs (e)(1), (2), and (3) of this section shall:

* * * * *

(5) * * *

* * * * *

(vi) * * *

* * * * *

(B) A gateway provider without a STIR/SHAKEN implementation obligation;

(vii) Whether the gateway provider is a gateway provider relying on non-Internet Protocol networks that has deployed one or more non-Internet Protocol caller identification authentication frameworks; and

(viii) * * *

(6) A gateway provider shall update its filings within 10 business days to the information it must provide pursuant to paragraphs (e)(1) through (5) of this section, subject to the conditions set forth in paragraphs (d)(6)(i) and (ii) of this section.

* * * * *

(f) * * *

* * * * *

(2) A non-gateway intermediate provider relying on non-Internet Protocol networks shall certify that it has implemented one or more effective non-IP caller ID authentication frameworks in its non-Internet Protocol networks and all calls it carries or processes its non-Internet Protocol networks are compliant with § 64.6303(c).

* * * * *

(4) All certifications made pursuant to paragraphs (f)(1), (2), and (3) of this section shall:

* * * * *

(5) * * *

* * * * *

(vi) * * *

* * * * *

(B) A non-gateway intermediate provider without a STIR/SHAKEN implementation obligation;

(vii) Whether the non-gateway intermediate provider is a non-gateway intermediate provider relying on non-Internet Protocol networks that has deployed one or more non-Internet Protocol caller identification authentication frameworks; and

(viii) * * *

(6) A non-gateway intermediate provider shall update its filings within 10 business days of any change to the information it must provide pursuant to this paragraph (f) subject to the conditions set forth in paragraphs (d)(6)(i) and (ii) of this section.

* * * * *

7. Remove and reserve § 64.6306.

**§ 64.6306 [Removed and Reserved]**

## 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 *Notice of Proposed Rulemaking* (*NPRM*) 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 *NPRM*. The Commission will send a copy of the *NPRM*, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).[2] In addition, the *NPRM* and IRFA (or summaries thereof) will be published in the Federal Register.[3]

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

2. To protect the American public from illegally spoofed robocalls, the *NPRM* seeks comment on proposals that would address gaps in the STIR/SHAKEN caller ID authentication framework, which works to provide trust that a calling party is who they claim to be. Although the STIR/SHAKEN framework mandated by Congress is effective, it relies on IP technology, resulting in critical information being stripped out when a call path includes non-IP networks.[4] To address this problem, the Commission proposes to: conclude that effective non-IP caller ID authentication frameworks have been developed and are reasonably available;[5] repeal the continuing extension from caller ID authentication requirements granted to providers that rely on non-IP technology;[6] modify our rules concerning providers' obligation to take reasonable measures to implement effective caller ID authentication in their non-IP networks to require that providers implement one or more non-IP caller ID authentication frameworks;[7] and require that providers certify in the Robocall Mitigation Database that they have implemented a non-IP caller ID authentication framework.[8] The Commission proposes to give providers a two-year transition period to implement one or more non-IP caller ID authentication frameworks in their non-IP networks, with a possible extension of this transition period for providers with 100,000 or fewer voice service subscriber lines.[9] The Commission proposes to rely on the TRACED Act and other Commission authority to implement these mandates.[10]

### 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), and 403 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), and 403.

---

[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] 5 U.S.C. § 603(a).

[3] *Id.*

[4] *NPRM* Section II.B.

[5] *Id.* Section III.A.

[6] *Id.* Section III.B.

[7] *Id.*

[8] *Id.*

[9] *Id.* Section III.C.

[10] *Id.* Section III.D.

### 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.[11] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[12] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act."[13] 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.[14]

5. *Small Businesses, Small Organizations, Small Governmental Jurisdictions.* Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe, at the outset, three broad groups of small entities that could be directly affected herein.[15] First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, according to data from the Small Business Administration's (SBA) Office of Advocacy, 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]

6. Next, the type of small entity described as a "small organization" is generally "any not-for-profit enterprise which is independently owned and operated and is not dominant in its field."[18] The Internal Revenue Service (IRS) uses a revenue benchmark of $50,000 or less to delineate its annual electronic filing requirements for small exempt organizations.[19] Nationwide, for tax year 2022, there were approximately 530,109 small exempt organizations in the U.S. reporting revenues of $50,000 or less

---

[11] 47 U.S.C. § 603(b)(3).

[12] *Id.* § 601(6).

[13] *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."

[14] 15 U.S.C. § 632.

[15] 5 U.S.C. § 601(3)-(6).

[16] *See* SBA, Office of Advocacy, *Frequently Asked Questions About Small Business* 1 (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] The IRS benchmark is similar to the population of less than 50,000 benchmark in 5 U.S.C § 601(5) that is used to define a small governmental jurisdiction. Therefore, the IRS benchmark has been used to estimate the number of small organizations in this small entity description. *See* Annual Electronic Filing Requirement for Small Exempt Organizations – Form 990-N (e-Postcard), "Who must file," https://www.irs.gov/charities-non-profits/annual-electronic-filing-requirement-for-small-exempt-organizations-form-990-n-e-postcard. We note that the IRS data does not provide information on whether a small exempt organization is independently owned and operated or dominant in its field.

according to the registration and tax data for exempt organizations available from the IRS.[20]

7. Finally, the small entity described as a "small governmental jurisdiction" is defined generally as "governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand."[21] U.S. Census Bureau data from the 2022 Census of Governments[22] indicate there were 90,837 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States.[23] Of this number, there were 36,845 general purpose governments (county,[24] municipal, and town or township[25]) with populations of less than 50,000 and 11,879 special purpose governments (independent school districts[26]) with enrollment populations of less than 50,000.[27] Accordingly, based on the 2022 U.S. Census of Governments data, we estimate that at least 48,724 entities fall into the category of "small governmental jurisdictions."[28]

---

[20] *See* Exempt Organizations Business Master File Extract (EO BMF), "CSV Files by Region," https://www.irs.gov/charities-non-profits/exempt-organizations-business-master-file-extract-eo-bmf. The IRS Exempt Organization Business Master File (EO BMF) Extract provides information on all registered tax-exempt/non-profit organizations. The data utilized for purposes of this description was extracted from the IRS EO BMF data for businesses for the tax year 2022 with revenue less than or equal to $50,000 for Region 1-Northeast Area (71,897), Region 2-Mid-Atlantic and Great Lakes Areas (197,296), and Region 3-Gulf Coast and Pacific Coast Areas (260,447) that includes the continental U.S., Alaska, and Hawaii. This data includes information for Puerto Rico (469).

[21] 5 U.S.C. § 601(5).

[22] 13 U.S.C. § 161. The Census of Governments survey is conducted every five (5) years compiling data for years ending with "2" and "7". *See also* Census of Governments, https://www.census.gov/programs-surveys/economic-census/year/2022/about.html.

[23] *See* U.S. Census Bureau, 2022 Census of Governments – Organization Table 2. Local Governments by Type and State: 2022 [CG2200ORG02], https://www.census.gov/data/tables/2022/econ/gus/2022-governments.html. Local governmental jurisdictions are made up of general purpose governments (county, municipal and town or township) and special purpose governments (special districts and independent school districts). *See also* tbl.2. CG2200ORG02 Table Notes_Local Governments by Type and State_2022.

[24] *See id.* at tbl.5. County Governments by Population-Size Group and State: 2022 [CG2200ORG05], https://www.census.gov/data/tables/2022/econ/gus/2022-governments.html. There were 2,097 county governments with populations less than 50,000. This category does not include subcounty (municipal and township) governments.

[25] *See id.* at tbl.6. Subcounty General-Purpose Governments by Population-Size Group and State: 2022 [CG2200ORG06], https://www.census.gov/data/tables/2022/econ/gus/2022-governments.html. There were 18,693 municipal and 16,055 town and township governments with populations less than 50,000.

[26] *See id.* at tbl.10. Elementary and Secondary School Systems by Enrollment-Size Group and State: 2022 [CG2200ORG10], https://www.census.gov/data/tables/2022/econ/gus/2022-governments.html. There were 11,879 independent school districts with enrollment populations less than 50,000. *See also* tbl.4. Special-Purpose Local Governments by State Census Years 1942 to 2022 [CG2200ORG04], CG2200ORG04 Table Notes_Special Purpose Local Governments by State_Census Years 1942 to 2022.

[27] While the special purpose governments category also includes local special district governments, the 2022 Census of Governments data does not provide data aggregated based on population size for the special purpose governments category. Therefore, only data from independent school districts is included in the special purpose governments category.

[28] This total is derived from the sum of the number of general purpose governments (county, municipal and town or township) with populations of less than 50,000 (36,845) and the number of special purpose governments - independent school districts with enrollment populations of less than 50,000 (11,879), from the 2022 Census of Governments - Organizations tbls. 5, 6 & 10.

8. *Cable System Operators (Telecom Act Standard).* The Communications Act of 1934, as amended, contains a size standard for a "small cable operator," which is "a cable operator that, directly or through an affiliate, serves in the aggregate fewer than one percent of all subscribers in the United States and is not affiliated with any entity or entities whose gross annual revenues in the aggregate exceed $250,000,000."[29] For purposes of the Telecom Act Standard, the Commission determined that a cable system operator that serves fewer than 498,000 subscribers, either directly or through affiliates, will meet the definition of a small cable operator.[30] Based on industry data, only six cable system operators have more than 498,000 subscribers.[31] Accordingly, the Commission estimates that the majority of cable system operators are small under this size standard. We note however, that the Commission neither requests nor collects information on whether cable system operators are affiliated with entities whose gross annual revenues exceed $250 million.[32] Therefore, we are unable at this time to estimate with greater precision the number of cable system operators that would qualify as small cable operators under the definition in the Communications Act.

9. *Competitive Local Exchange Carriers (CLECs).* Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. Providers of these services include several types of competitive local exchange service providers.[33] Wired Telecommunications Carriers[34] is the closest industry with a SBA small business size standard. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[35] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[36] Of this number, 2,964 firms operated with fewer than 250 employees.[37] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 3,378 providers that reported they were competitive local

[29] 47 U.S.C. § 543(m)(2).

[30] *FCC Announces Updated Subscriber Threshold for the Definition of Small Cable Operator*, Public Notice, DA 23-906 (MB 2023) (*2023 Subscriber Threshold PN*). In this 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. *Id.* This threshold will remain in effect until the Commission issues a superseding Public Notice. *See* 47 CFR § 76.901(e)(1).

[31] S&P Global Market Intelligence, S&P Capital IQ Pro, *Top Cable MSOs 06/23Q* (last visited Sept. 27, 2023); S&P Global Market Intelligence, Multichannel Video Subscriptions, Top 10 (April 2022).

[32] The Commission does receive such information on a case-by-case basis if a cable operator appeals a local franchise authority's finding that the operator does not qualify as a small cable operator pursuant to § 76.901(e) of the Commission's rules. *See* 47 CFR § 76.910(b).

[33] Competitive Local Exchange Service Providers include the following types of providers: Competitive Access Providers (CAPs) and Competitive Local Exchange Carriers (CLECs), Cable/Coax CLECs, Interconnected VOIP Providers, Non-Interconnected VOIP Providers, Shared-Tenant Service Providers, Audio Bridge Service Providers, Local Resellers, and Other Local Service Providers.

[34] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[35] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[36] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false. At this time, the 2022 Economic Census data is not available.

[37] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

service providers.[38] Of these providers, the Commission estimates that 3,230 providers have 1,500 or fewer employees.[39] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

10. *Incumbent Local Exchange Carriers (Incumbent LECs).* Neither the Commission nor the SBA have developed a small business size standard specifically for incumbent local exchange carriers. Wired Telecommunications Carriers[40] is the closest industry with an SBA small business size standard.[41] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[42] U.S. Census Bureau data for 2017 show that there were 3,054 firms in this industry that operated for the entire year.[43] Of this number, 2,964 firms operated with fewer than 250 employees.[44] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 1,212 providers that reported they were incumbent local exchange service providers.[45] Of these providers, the Commission estimates that 916 providers have 1,500 or fewer employees.[46] Consequently, using the SBA's small business size standard, the Commission estimates that the majority of incumbent local exchange carriers can be considered small entities.

11. *Interexchange Carriers (IXCs).* Neither the Commission nor the SBA have developed a small business size standard specifically for Interexchange Carriers. Wired Telecommunications Carriers[47] is the closest industry with a SBA small business size standard.[48] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[49] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[50] Of this number, 2,964 firms operated with fewer than 250 employees.[51]

---

[38] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[39] *Id.*

[40] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[41] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[42] *Id.*

[43] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false. At this time, the 2022 Economic Census data is not available.

[44] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[45] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[46] *Id.*

[47] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[48] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[49] *Id.*

[50] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311,

(continued….)

Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 127 providers that reported they were engaged in the provision of interexchange services. Of these providers, the Commission estimates that 109 providers have 1,500 or fewer employees.[52] Consequently, using the SBA's small business size standard, the Commission estimates that the majority of providers in this industry can be considered small entities.

12. *Local Exchange Carriers (LECs).* Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. Providers of these services include both incumbent and competitive local exchange service providers. Wired Telecommunications Carriers[53] is the closest industry with an SBA small business size standard.[54] Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.[55] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[56] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[57] Of this number, 2,964 firms operated with fewer than 250 employees.[58] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 4,590 providers that reported they were fixed local exchange service providers.[59] Of these providers, the Commission estimates that 4,146 providers have 1,500 or fewer employees.[60] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

13. *Local Resellers.* Neither the Commission nor the SBA have developed a small business size standard specifically for Local Resellers. Telecommunications Resellers is the closest industry with

(Continued from previous page)
https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false. At this time, the 2022 Economic Census data is not available.

[51] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[52] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[53] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[54] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[55] Fixed Local Exchange Service Providers include the following types of providers: Incumbent Local Exchange Carriers (ILECs), Competitive Access Providers (CAPs) and Competitive Local Exchange Carriers (CLECs), Cable/Coax CLECs, Interconnected VOIP Providers, Non-Interconnected VOIP Providers, Shared-Tenant Service Providers, Audio Bridge Service Providers, Local Resellers, and Other Local Service Providers.

[56] *Id.*

[57] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false. At this time, the 2022 Economic Census data is not available.

[58] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[59] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[60] *Id.*

a SBA small business size standard.[61] The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households.[62] Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure.[63] Mobile virtual network operators (MVNOs) are included in this industry.[64] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[65] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[66] Of that number, 1,375 firms operated with fewer than 250 employees.[67] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 207 providers that reported they were engaged in the provision of local resale services.[68] Of these providers, the Commission estimates that 202 providers have 1,500 or fewer employees.[69] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

14. *Other Toll Carriers.* Neither the Commission nor the SBA has developed a definition for small businesses specifically applicable to Other Toll Carriers. This category includes toll carriers that do not fall within the categories of interexchange carriers, operator service providers, prepaid calling card providers, satellite service carriers, or toll resellers. Wired Telecommunications Carriers[70] is the closest industry with a SBA small business size standard.[71] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[72] U.S. Census Bureau data for 2017 show that there were 3,054 firms in this industry that operated for the entire year.[73]

---

[61] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517911 Telecommunications Resellers*," https://www.census.gov/naics/?input=517911&year=2017&details=517911.

[62] *Id.*

[63] *Id.*

[64] *Id.*

[65] *See* 13 CFR § 121.201, NAICS Code 517911 (as of 10/1/22, NAICS Code 517121).

[66] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEEMPFIRM, NAICS Code 517911, https://data.census.gov/cedsci/table?y=2017&n=517911&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false. At this time, the 2022 Economic Census data is not available.

[67] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[68] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[69] *Id.*

[70] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[71] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[72] *Id.*

[73] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false. At this time, the 2022 Economic Census data is not available.

Of this number, 2,964 firms operated with fewer than 250 employees.[74] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 90 providers that reported they were engaged in the provision of other toll services.[75] Of these providers, the Commission estimates that 87 providers have 1,500 or fewer employees.[76] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

15. *Prepaid Calling Card Providers.* Neither the Commission nor the SBA has developed a small business size standard specifically for prepaid calling card providers. Telecommunications Resellers[77] is the closest industry with a SBA small business size standard. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure.[78] Mobile virtual network operators (MVNOs) are included in this industry.[79] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[80] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[81] Of that number, 1,375 firms operated with fewer than 250 employees.[82] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 62 providers that reported they were engaged in the provision of prepaid card services.[83] Of these providers, the Commission estimates that 61 providers have 1,500 or fewer employees.[84] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

16. *Satellite Telecommunications.* This industry comprises firms "primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or

---

[74] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[75] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[76] *Id.*

[77] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517911 Telecommunications Resellers*," https://www.census.gov/naics/?input=517911&year=2017&details=517911.

[78] *Id.*

[79] *Id.*

[80] *See* 13 CFR § 121.201, NAICS Code 517911 (as of 10/1/22, NAICS Code 517121).

[81] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEEMPFIRM, NAICS Code 517911, https://data.census.gov/cedsci/table?y=2017&n=517911&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false. At this time, the 2022 Economic Census data is not available.

[82] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[83] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[84] *Id.*

reselling satellite telecommunications."[85] Satellite telecommunications service providers include satellite and earth station operators. The SBA small business size standard for this industry classifies a business with $44 million or less in annual receipts as small.[86] U.S. Census Bureau data for 2017 show that 275 firms in this industry operated for the entire year.[87] Of this number, 242 firms had revenue of less than $25 million.[88] Consequently, using the SBA's small business size standard most satellite telecommunications service providers can be considered small entities. The Commission notes however, that the SBA's revenue small business size standard is applicable to a broad scope of satellite telecommunications providers included in the U.S. Census Bureau's Satellite Telecommunications industry definition. Additionally, the Commission neither requests nor collects annual revenue information from satellite telecommunications providers, and is therefore unable to more accurately estimate the number of satellite telecommunications providers that would be classified as a small business under the SBA size standard.

17. *Toll Resellers.* Neither the Commission nor the SBA have developed a small business size standard specifically for Toll Resellers. Telecommunications Resellers[89] is the closest industry with a SBA small business size standard. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure.[90] Mobile virtual network operators (MVNOs) are included in this industry.[91] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[92] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[93] Of that number, 1,375 firms operated with fewer than 250 employees.[94] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 457 providers that reported

[85] *See* U.S. Census Bureau, *2017 NAICS Definition, "517410 Satellite Telecommunications*," https://www.census.gov/naics/?input=517410&year=2017&details=517410.

[86] *See* 13 CFR § 121.201, NAICS Code 517410.

[87] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEREVFIRM, NAICS Code 517410, https://data.census.gov/cedsci/table?y=2017&n=517410&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false. At this time, the 2022 Economic Census data is not available.

[88] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[89] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517911 Telecommunications Resellers*," https://www.census.gov/naics/?input=517911&year=2017&details=517911.

[90] *Id.*

[91] *Id.*

[92] *See* 13 CFR § 121.201, NAICS Code 517911 (as of 10/1/22, NAICS Code 517121).

[93] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEEMPFIRM, NAICS Code 517911, https://data.census.gov/cedsci/table?y=2017&n=517911&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false. At this time, the 2022 Economic Census data is not available.

[94] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

they were engaged in the provision of toll services.[95] Of these providers, the Commission estimates that 438 providers have 1,500 or fewer employees.[96] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

18. *Wired Telecommunications Carriers.* The U.S. Census Bureau defines this industry as establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks.[97] Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband Internet services.[98] By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry.[99] Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.[100]

19. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[101] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[102] Of this number, 2,964 firms operated with fewer than 250 employees.[103] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 4,590 providers that reported they were engaged in the provision of fixed local services.[104] Of these providers, the Commission estimates that 4,146 providers have 1,500 or fewer employees.[105] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

20. *Wireless Telecommunications Carriers (except Satellite).* This industry comprises

---

[95] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[96] *Id.*

[97] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[98] *Id.*

[99] *Id.*

[100] Fixed Local Service Providers include the following types of providers: Incumbent Local Exchange Carriers (ILECs), Competitive Access Providers (CAPs) and Competitive Local Exchange Carriers (CLECs), Cable/Coax CLECs, Interconnected VOIP Providers, Non-Interconnected VOIP Providers, Shared-Tenant Service Providers, Audio Bridge Service Providers, and Other Local Service Providers. Local Resellers fall into another U.S. Census Bureau industry group and therefore data for these providers is not included in this industry.

[101] *See* 13 CFR § 121.201, NAICS Code 517311 (as of 10/1/22, NAICS Code 517111).

[102] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false. At this time, the 2022 Economic Census data is not available.

[103] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[104] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[105] *Id.*

establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves.[106] Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular services, paging services, wireless Internet access, and wireless video services.[107] The SBA size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[108] U.S. Census Bureau data for 2017 show that there were 2,893 firms in this industry that operated for the entire year.[109] Of that number, 2,837 firms employed fewer than 250 employees.[110] Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 594 providers that reported they were engaged in the provision of wireless services.[111] Of these providers, the Commission estimates that 511 providers have 1,500 or fewer employees.[112] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

21. *All Other Telecommunications*. This industry is comprised of establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation.[113] This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems.[114] Providers of Internet services (e.g. dial-up ISPs) or Voice over Internet Protocol (VoIP) services, via client-supplied telecommunications connections are also included in this industry.[115] The SBA small business size standard for this industry classifies firms with annual receipts of $40 million or less as small.[116] U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year.[117] Of those firms, 1,039 had revenue of less than $25 million.[118] Based

---

[106] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers (except Satellite)," https://www.census.gov/naics/?input=517312&year=2017&details=517312*.

[107] *Id.*

[108] *See* 13 CFR § 121.201, NAICS Code 517312 (as of 10/1/22, NAICS Code 517112).

[109] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false. At this time, the 2022 Economic Census data is not available.

[110] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.

[111] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2022), https://docs.fcc.gov/public/attachments/DOC-391070A1.pdf.

[112] *Id.*

[113] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517919 All Other Telecommunications*," https://www.census.gov/naics/?input=517919&year=2017&details=517919.

[114] *Id.*

[115] *Id.*

[116] *See* 13 CFR § 121.201, NAICS Code 517919 (as of 10/1/22, NAICS Code 517810).

[117] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017*, Table ID: EC1700SIZEREVFIRM, NAICS Code 517919, https://data.census.gov/cedsci/table?y=2017&n=517919&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false. At this time, the 2022 Economic Census data is not available.

on this data, the Commission estimates that the majority of "All Other Telecommunications" firms can be considered small.

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

22. 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.[119]

23. In the *NPRM*, the Commission proposes and seeks comment on imposing reporting, recordkeeping and compliance obligations on various providers, many of whom may be small entities. Specifically, the Commission proposes introducing a new requirement for providers to certify in the Robocall Mitigation Database whether they have implemented a non-IP caller ID authentication framework in their non-IP networks.[120] Additionally, the Commission proposes to require all providers using non-IP technology in their networks to implement one or more non-IP caller ID authentication frameworks within two years,[121] and seeks comment on whether additional time for compliance should be allowed for providers that have 100,000 or fewer voice service subscriber lines.[122] The Commission proposes that these frameworks be based on two non-IP caller ID authentication standards promulgated by the Alliance for Telecommunication Industry Solutions (ATIS):[123] In-Band Authentication (ATIS-1000095.v002) and Out-of-Band Multiple STI-CPS Authentication (ATIS-1000096).[124] The *NPRM* seeks comment on whether frameworks based on a third ATIS standard, Out-of-Band Agreed STI-CPS Authentication (ATIS-1000105), or other non-IP caller ID authentication frameworks satisfy the proposed criteria to meet the TRACED Act's requirements to first, be developed and reasonably available, and second, to be "effective."[125]

24. The *NPRM* seeks comment on the costs and benefits of its proposals and inquiries, which we anticipate will help the Commission identify and evaluate relevant compliance matters for small entities, including compliance costs and other burdens that may result from the proposals and inquiries. Specifically, the Commission proposes an analysis of the costs and benefits with respect to the timing of any mandate in the *NPRM* and seeks comment thereon.[126] Further, the *NPRM* specifically seeks comment on the costs of requiring providers to either implement a non-IP caller ID authentication framework or upgrade their networks to all IP,[127] the costs for providers to actually implement a non-IP caller ID

(Continued from previous page)

[118] *Id.* The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[119] 5 U.S.C. § 603(b)(4).

[120] *NPRM* Section III.B.

[121] *Id.* Section III.C.

[122] *Id.*

[123] *Id.* Section III.A.2.

[124] *Id.* Section III.A.1.

[125] *Id.* Section III.A.2.

[126] *Id.* Section III.D.

[127] *Id.* Section III.A.2.

authentication framework in their networks,[128] and the costs for the providers to certify that they have implemented a non-IP caller ID authentication framework in the Robocall Mitigation Database.[129] The *NPRM* also seeks comment on how many small voice service providers have implemented each of these frameworks.[130] We seek comment from small and other entities about these costs.[131]

### E. Discussion of Significant Alternatives Considered That Minimize the Significant Economic Impact on Small Entities

25. 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.[132] 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."[133]

26. The *NPRM* seeks comment on proposals and alternatives that may have a significant impact on small entities. In particular, it seeks comment on the benefits and burdens of requiring all providers, including small and other entities, to implement a non-IP caller ID authentication framework.[134] The *NPRM* specifically asks about frameworks based on standards promulgated by ATIS, as well as whether alternative non-IP caller ID authentication frameworks exist that satisfy the TRACED Act's requirements to first, be "developed" and "reasonably available," and second, be "effective."[135] This includes whether the Commission should use proposed criteria to evaluate whether non-IP caller ID authentication frameworks meet the TRACED Act's requirements, or if any alternative criteria for how to evaluate any such frameworks should be considered.[136] Additionally, the *NPRM* seeks comment on whether providers, including small and other entities, possess the resources necessary to implement these changes in the proposed two-year timeframe.[137] The *NPRM* also solicits comment on whether additional time may be needed to implement these frameworks, or whether extensions should be granted for certain providers including providers that have 100,000 or fewer voice service subscriber lines.[138] Finally, the Commission seeks comment on the proposed analysis of the costs and benefits with respect to the timing of any mandate and any alternatives that may avoid or minimize those costs.[139]

---

[128] *Id.* Section III.B.

[129] *Id.*

[130] *Id.*

[131] *Id.*

[132] 5 U.S.C. § 603(c).

[133] *Id.* § 603(c)(1) - (4).

[134] *NPRM* Section III.B.

[135] *Id.* Section III.A.2.

[136] *Id.* Section III.A.1.

[137] *Id.* Section III.C.

[138] *Id.*

[139] *Id.* Section III.D.

### F. Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rules

27. None.

**STATEMENT OF**
**CHAIRMAN BRENDAN CARR**

Re: *Call Authentication Trust Anchor*, Notice of Proposed Rulemaking, WC Docket No.17-97 (April 28, 2025).

Over the years, the Commission's efforts to crack down on illegal robocalls have often been described as a game of whack-a-mole. We tackle one challenge and then another one pops up.

But FCC leaders, including Chairman Pai and Chairwoman Rosenworcel before me, have also worked on a more comprehensive solution—a call authentication framework known by its very James Bond sounding acronym of STIR/SHAKEN.

Even there, though, some gaps remain. While STIR/SHAKEN is one of our most effective tools for combatting illegal robocalls, it only applies to calls that travel exclusively over modern, Internet Protocol networks. If non-IP technology is used at any point in the call path, STIR/SHAKEN won't catch those robocalls, which bad actors can and have taken advantage of.

Congress anticipated this issue back in 2018 when it passed the TRACED Act. In that law, Congress established a June 2021 deadline for carriers to take "reasonable measures to implement" an authentication framework that could work for non-IP calls. Specifically, Congress directed the Commission to grant a delay of the non-IP compliance date if caller authentication solutions for those networks were not readily available.

Flash forward to today, and the FCC has been granting waivers for a number of years now. But technology has continued to evolve at the same time. So I think it is appropriate for the Commission to look at requiring even the non-IP components of networks to meet the standards laid out in the TRACED Act.

As we do so, we will be mindful of the pace and nature of the transition to all IP networks. In fact, I think there is much more the FCC can and should be doing to accelerate that transition.

So we are proceeding today with an open mind. Whether it's through a faster IP transition or through the adoption and implementation of caller ID authentication solutions for non-IP networks, it is time for the FCC to examine this gap in our robocall defenses.

For my part, I want to thank in particular Erik Beith, Jesse Goodwin, Trent Harkrader, Chris Laughlin, Jonathan Lechter, Jodie May, Zach Ross, and Cara Voth for their great work on this item.