

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

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

NOTICE OF INQUIRY

Adopted: October 27, 2022

Released: October 28, 2022

Comment Date: December 12, 2022

Reply Date: January 11, 2023

By the Commission: Chairwoman Rosenworcel and Commissioner Starks issuing separate statements.

TABLE OF CONTENTS

Heading	Paragraph #
I. INTRODUCTION.....	1
II. BACKGROUND.....	2
A. Caller ID Authentication for IP Networks: STIR/SHAKEN.....	3
B. Caller ID Authentication for Non-IP Networks.....	9
III. DISCUSSION.....	15
A. Caller ID Authentication in Non-IP Networks.....	16
1. ATIS Standards.....	20
2. Alternatives.....	32
3. Legal Authority.....	34
B. The IP Transition.....	36
1. Caller ID Authentication and the IP Transition.....	37
2. Actions to Encourage the IP Transition.....	40
IV. PROCEDURAL MATTERS.....	43
V. ORDERING CLAUSE.....	48

I. INTRODUCTION

1. Today, we continue our efforts to protect Americans from illegally spoofed robocalls by launching a broad inquiry on caller ID authentication for non-Internet Protocol (IP) networks. Caller ID authentication combats illegally spoofed robocalls by allowing voice service providers to verify that the caller ID information transmitted with a call matches the caller’s number. Commission rules adopted pursuant to the TRACED Act require voice service providers to implement the caller ID authentication framework known as STIR/SHAKEN on their IP networks.¹ Because STIR/SHAKEN only works on IP networks, the TRACED Act directed the Commission to separately address non-IP networks,² and Commission rules require voice service providers with non-IP network technology to either upgrade their

¹ 47 CFR § 64.6301.

² Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105, § 4(b)(1)(B) (2019) (codified at 47 U.S.C. § 227b(b)(1)(B)) (TRACED Act).

networks to IP or work to develop an authentication solution for non-IP networks.³ In the time since those rules were adopted in September 2020, industry technologists have issued standards for caller ID authentication on non-IP networks,⁴ and we have taken aggressive steps to ensure ubiquitous caller ID authentication implementation across the voice network.⁵ In May 2022, as part of a broader Report and Order and Notice of Proposed Rulemaking addressing robocalls, we sought comment on caller ID authentication for non-IP networks.⁶ The record reflected interest in this subject from a broad array of stakeholders with divergent views on the best path forward. We now issue this Notice of Inquiry to collect more focused comment on this subject and how best to address this remaining gap in our caller ID authentication scheme.

II. BACKGROUND

2. Combatting illegal robocalls continues to be one of the Commission's top consumer protection priorities. Illegal caller ID spoofing is a particularly noxious practice whereby bad actors falsify caller ID information to deceive call recipients into believing the caller is someone they trust. In 2019, recognizing the scope of the problem posed by illegal robocalls and caller ID spoofing, Congress passed the TRACED Act. Among other provisions, the TRACED Act directed the Commission to require voice service providers to implement caller ID authentication technology.⁷ By allowing voice service providers to verify that the caller ID information transmitted with a particular call matches the caller's number, caller ID authentication enables voice service providers to tell their subscribers when the caller ID may be spoofed; offers information that can drive efforts to trace back illegal robocalls to their source; and supplies data to inform blocking decisions voice service providers can make before unwanted calls even reach their subscribers.

A. Caller ID Authentication for IP Networks: STIR/SHAKEN

3. The STIR/SHAKEN framework is a set of technical standards and policies that enable caller ID authentication on IP networks.⁸ At a high level, the operation of STIR/SHAKEN involves two

³ 47 CFR § 64.6303.

⁴ See Press Release, Alliance for Telecommunications Industry Solutions (ATIS), ATIS Addresses Non-IP Call Authentication (Aug. 12, 2021), <https://www.atis.org/press-releases/atis-addresses-non-ip-call-authentication/>.

⁵ See, e.g., *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, Fifth Further Notice of Proposed Rulemaking, FCC 22-37 (May 20, 2022) (*May 2022 Robocalls Order and Further Notice*); *Call Authentication Trust Anchor*, WC Docket No. 17-97, Fourth Report and Order, FCC 21-122 (Dec. 10, 2021) (*Fourth Caller ID Authentication Report and Order*).

⁶ See *May 2022 Robocalls Order and Further Notice* at 68-69, para. 173.

⁷ TRACED Act § 4(b)(1). In this proceeding, a "voice service provider" refers to a provider of "voice service," which is defined in relevant part in the TRACED Act as "any service that is interconnected with the public switched telephone network and that furnishes voice communications to an end user using resources from the North American Numbering Plan" and includes "without limitation, any service that enables real-time, two-way voice communications, including any service that requires internet protocol-compatible customer premises equipment . . . and permits out-bound calling, whether or not the service is one-way or two-way voice over internet protocol." TRACED Act § 4(a)(2); see also 47 CFR § 64.6300(n)(2)(ii). Commission rules define an intermediate provider, by contrast, as "any entity that carries or processes traffic that traverses or will traverse the PSTN at any point insofar as that entity neither originates nor terminates that traffic." 47 CFR § 64.6300(g).

⁸ 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, 3244, 3258-59, paras. 5, 36 (2020) (*First Caller ID Authentication Report and Order and Further Notice*). See also ATIS & SIP Forum, Joint ATIS/SIP Forum Standard—Signature-Based Handling of Asserted Information Using toKENs (SHAKEN), ATIS-1000074 (2017) (ATIS-1000074); ATIS & SIP Forum, Joint ATIS/SIP Forum Standard -Signature-Based Handling of Asserted

(continued....)

processes: (1) the technical process of authenticating and verifying caller ID information; and (2) the certificate governance process that maintains trust in the caller ID authentication information transmitted along with a call.⁹ Commission rules require almost all types of providers in the potential call chain to implement STIR/SHAKEN on their IP networks.¹⁰

4. *STIR/SHAKEN Overview.* The STIR/SHAKEN technical authentication and verification processes rely on public key cryptography to securely transmit the information that an originating voice service provider knows about the caller and its relationship to the phone number it is using along with the call itself, allowing the terminating voice service provider to verify the information on the other end.¹¹ This encrypted information is contained in a unique part of the Session Initiation Protocol (SIP) message known as the “Identity header field.”¹² After the originating voice service provider authenticates this caller ID information for a particular call and adds this information, it travels along with the call from the originating voice service provider, through any intermediate providers, and then to the terminating voice service provider.¹³ When the terminating voice service provider receives the call with the Identity header attached, it can decrypt it, verify the caller ID information, and then use that information to protect its subscribers from unwanted and illegal calls.¹⁴

5. The STIR/SHAKEN framework relies on the use of digital “certificates” issued through a neutral governance system to maintain trust and accountability among providers.¹⁵ The provider adding the Identity header also includes its assigned certificate to the call, which states, in essence, that the provider is the entity it claims to be and that it has the right to authenticate the caller ID information.¹⁶ This system is overseen by a Governance Authority—a role filled by an entity called the Secure Telephone Identity Governance Authority¹⁷—which establishes the policies and procedures regarding how providers may acquire and maintain certificates.¹⁸ A Policy Administrator applies the rules set by the Governance Authority,¹⁹ and third-party Certification Authorities (themselves subject to Policy

(Continued from previous page) _____

Information Using toKENs (SHAKEN): Governance Model and Certificate Management, ATIS-1000080 (2017) (ATIS-1000080); ATIS & SIP Forum, Joint ATIS/SIP Forum Standard -Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators, ATIS-1000084 (2018) (ATIS-1000084).

⁹ *May 2022 Robocalls Order and Further Notice* at 6, para. 9.

¹⁰ See 47 CFR §§ 64.6301, 64.6302.

¹¹ See *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3244-45, para. 6.

¹² See IETF, *Authenticated Identity Management in the Session Initiation Protocol*, RFC 8224, at 4, (2018), <https://datatracker.ietf.org/doc/rfc8224/>; *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3244-45, para. 6.

¹³ See *Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, 36 FCC Rcd 1859, 1863, para. 8 (2020) (*Second Caller ID Authentication Report and Order*).

¹⁴ See *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3244-45, para. 6.

¹⁵ *Id.* at 3245, para. 9.

¹⁶ See *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1864, para. 11.

¹⁷ *Id.* at 1864, para. 11. See also Secure Telephone Identity Governance Authority, *STI Governance Authority*, <https://sti-ga.atis.org/> (last visited Oct. 27, 2022). The Secure Telephone Identity Governance Authority Board of Directors is made up of representatives from around the voice industry. See Secure Telephone Identity Governance Authority, *Leadership*, <https://sti-ga.atis.org/leadership/> (last visited Oct. 27, 2022).

¹⁸ *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1864, para. 11.

¹⁹ iconectiv, *Authenticate*, <https://authenticate.iconectiv.com/> (last visited Oct. 27, 2022) (filling the role of the Policy Administrator).

Administrator approval)²⁰ issue the digital certificates themselves to each provider to use.²¹ This robust system of checks and balances ensures that providers can trust one another based on the certificates transmitted along with STIR/SHAKEN-authenticated calls.

6. The STIR/SHAKEN caller ID authentication framework only works on IP networks—that is, those networks with technology that is able to initiate, maintain, and terminate SIP calls.²² The additional information a provider must add to the SIP message has not been designed to be added to the message of other signaling protocols used to initiate, maintain, and terminate calls, and we refer to networks that use this technology generally as “non-IP.”²³ This means that providers using non-IP technology cannot participate in the STIR/SHAKEN framework for the non-IP portion of their networks.²⁴ Not only that, the STIR/SHAKEN framework fails to work if at any point a call routes over non-IP network technology, even if both the originating and terminating voice service provider have implemented the technology.²⁵ If an authenticated call passes through a non-IP interconnection point or the network of an intermediate provider using non-IP technology, the authentication information accompanying the call will be lost.²⁶ Non-IP technology in the network thus creates a gap in the caller ID authentication scheme that decreases the efficacy of the technology on the network and can be exploited by bad actors.²⁷

7. *Commission Rules.* Commission rules require voice service providers to implement STIR/SHAKEN in the IP portions of their networks.²⁸ They must not only implement the technology, but also use it. Voice service providers must: (1) authenticate and verify caller ID information for all SIP calls that exclusively transit their networks; (2) authenticate caller ID information for all SIP calls originating on their networks that they will pass to another voice service or intermediate provider and, to the extent technically feasible, transmit such calls with authenticated caller ID information to the next provider in the call path; and (3) verify caller ID information for all SIP calls they receive from other

²⁰ iconectiv, *Approved Certification Authorities*, <https://authenticate.iconectiv.com/approved-certification-authorities> (last visited Oct. 27, 2022) (listing the certification authorities that the Policy Administrator has approved for operation within the STIR/SHAKEN framework).

²¹ *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1864, para. 11.

²² *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3245, para. 7. The Session Initiation Protocol (SIP) is “an application-layer control protocol” “for creating, modifying, and terminating sessions” such as Internet Protocol (IP) telephony calls. IETF, *SIP: Session Initiation Protocol*, RFC 3261, at 1 (2002), <https://tools.ietf.org/html/rfc3261>.

²³ The TRACED Act—and the Commission’s rules implementing it—use the general term “non-internet protocol [IP]” to capture networks that use types of technology other than IP. See TRACED Act § 4(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.

²⁴ *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3245, para. 7.

²⁵ See *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1863, para. 9.

²⁶ *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3245, para. 7.

²⁷ See Call Authentication Trust Anchor Working Group, North American Numbering Council, Report on Deployment of STIR/SHAKEN by Small Voice Service Providers § 2.2.4 (2021) (describing non-IP network technology as a barrier to deployment of the STIR/SHAKEN framework) (NANC Oct. 2021 Report); TransNexus Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 6 (rec. Aug. 17, 2022) (TransNexus Comments) (“Many providers have invested in SHAKEN capability, but they don’t get the full benefit. Many signed calls that they originate arrive at their destinations unsigned. Many calls that were sent to them with SHAKEN information arrive with none.”).

²⁸ 47 CFR § 64.6301(a).

providers that they terminate and for which caller ID information has been authenticated.²⁹ Voice service providers were obligated to implement STIR/SHAKEN in the IP portions of their networks by June 30, 2021, subject to certain extensions for undue hardship.³⁰ Many of the extended deadlines have since passed; at this point, extensions remain solely for facilities-based small voice service providers (until June 30, 2023) and providers unable to receive the certificate required to participate in STIR/SHAKEN (until the provider is able to receive the certificate).³¹

8. Commission rules also place obligations on intermediate and gateway providers. Intermediate providers must pass unaltered authenticated caller ID information along with any SIP calls they receive to the next provider in the call path.³² They must also authenticate caller ID information for all unauthenticated calls they receive that will be exchanged with other providers as SIP calls; however, they are freed from this obligation if they participate in traceback efforts.³³ In our *May 2022 Robocalls Order and Further Notice*, we proposed eliminating this alternative path of compliance and simply requiring intermediate providers to authenticate unauthenticated SIP calls that will be exchanged with other providers.³⁴ In that same item, we adopted new rules requiring gateway providers—U.S.-based intermediate providers that receive calls directly from foreign originating or intermediate providers and transmit those calls downstream to another U.S.-based provider³⁵—to implement STIR/SHAKEN and authenticate calls with a U.S. number in the caller ID field that they will exchange with downstream U.S.-based providers as SIP calls.³⁶ As our undue hardship extensions for voice service providers expire, and as we take aggressive steps to expand participation in STIR/SHAKEN by other providers,³⁷ non-IP network technology remains the most prominent gap in our caller ID authentication scheme.

B. Caller ID Authentication for Non-IP Networks

9. Because STIR/SHAKEN only works on IP networks, Congress directed the Commission to separately address caller ID authentication for non-IP networks. The TRACED Act required the Commission to mandate that voice service providers take “reasonable measures” to implement an effective caller ID authentication framework in the non-IP portions of their networks.³⁸ It also directed the Commission to grant an extension 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.”³⁹ The Commission adopted rules implementing this statutory

²⁹ 47 CFR § 64.6301(a)(1)-(3).

³⁰ See 47 CFR §§ 64.6301 (requiring implementation by June 30, 2021), 64.6304 (providing extensions and associated deadlines).

³¹ See 47 CFR § 64.6304.

³² 47 CFR § 64.6302(a). Two exceptions to this rule exist: (1) where doing so would make it impossible to complete the call for technical reasons; and (2) when the intermediate provider reasonably believes that doing so presents an imminent threat to the intermediate provider’s network security. *Id.* § 64.6302(a)(1)-(2).

³³ 47 CFR § 64.6302(b).

³⁴ See *May 2022 Robocalls Order and Further Notice* at 63-67, paras. 160-71.

³⁵ 47 CFR § 64.6300(d).

³⁶ See *May 2022 Robocalls Order and Further Notice* at 22-29, paras. 51-60; 47 CFR § 64.6302(c).

³⁷ See *May 2022 Robocalls Order and Further Notice* at 22-29, paras. 51-60; *Fourth Caller ID Authentication Report and Order* at 7-16, paras. 14-30 (shortening undue hardship extension for small voice service providers most likely to be the source of illegal robocalls); see also 47 CFR §§ 64.6302(c), 64.6304(a)(1)(i)-(ii).

³⁸ TRACED Act § 4(b)(1)(B).

³⁹ TRACED Act § 4(b)(5)(B).

direction and, since those rules were adopted, industry technologists have made progress on standards for non-IP caller ID authentication.

10. *Commission Rules.* Commission rules require voice service providers with non-IP network technology to do one of two things. They must either: (1) upgrade their entire network to IP and implement STIR/SHAKEN;⁴⁰ or (2) participate (directly or via a representative) in industry efforts to develop a non-IP caller ID authentication solution.⁴¹ Consistent with the TRACED Act, the Commission established that voice service providers that rely on non-IP technology “are deemed subject to a continuing extension” and are thus subject to the robocall mitigation obligations on providers with an extension.⁴² The Commission explained that “we will continue to evaluate whether an effective non-IP caller ID authentication framework emerges” and that, consistent with the TRACED Act, “we 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.”⁴³ It further stated that “[we] may revisit our approach . . . if we find that industry has failed to make sufficient progress in either transitioning to IP or developing a consensus non-IP authentication solution.”⁴⁴

11. *Non-IP Standards.* Since the Commission adopted these rules, industry technologists have made progress on caller ID authentication for non-IP networks. In May 2020, ATIS established the Non-IP Call Authentication Task Force to develop solutions for non-IP networks. In August 2021, this Task Force published two standards for the exchange of authenticated caller ID information on non-IP networks: ATIS-1000096, Signature-based Handling of Asserted information using toKENs (SHAKEN): Out-of-Band PASSporT Transmission Involving TDM Networks; and ATIS-1000095, Extending STIR/SHAKEN over TDM, the latter of which was updated with a second version released in August 2022.⁴⁵ These two standards address the problem of STIR/SHAKEN information not being designed for the signaling messages of non-IP calls in different ways, though they can be used in conjunction with one another, by the same provider, or by different providers.⁴⁶

12. The ATIS-1000096 standard allows a non-IP originating voice service provider to send the same information as in STIR/SHAKEN by transmitting that information on a separate track that is

⁴⁰ 47 CFR § 64.6303(a)(1).

⁴¹ 47 CFR § 64.6303(a)(2). In the *May 2022 Robocalls Order and Further Notice*, we adopted rules requiring gateway providers to meet these same two requirements not later June 30, 2023. *See May 2022 Robocalls Order and Further Notice* at 29-30, paras. 62-63; 47 CFR § 64.6303(b)(1)-(2). Compliance by gateway providers with these new rules is not required until the Office of Management and Budget (OMB) completes its review of these requirements under the Paperwork Reduction Act and notice of OMB’s approval is published in the Federal Register. *See* 47 CFR § 64.6303(b)(3).

⁴² 47 CFR § 64.6304(d); *see also id.* § 64.6305(a)(1) (establishing robocall mitigation requirements for providers subject to extension).

⁴³ *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1874, para. 32.

⁴⁴ *Id.*

⁴⁵ *See* ATIS & SIP Forum, Extending STIR/SHAKEN over TDM, ATIS-1000095.v002 (2022), https://access.atis.org/apps/group_public/download.php/67542/ATIS-1000095.v002.pdf (ATIS-1000095.v002); ATIS & SIP Forum, Signature-based Handling of Asserted information using toKENs (SHAKEN): Out-of-Band PASSporT Transmission Involving TDM Networks, ATIS-1000096, (July 2021), https://access.atis.org/apps/group_public/download.php/60535/ATIS-1000096.pdf (ATIS-1000096; *see also* ATIS & SIP Forum, Technical Report on Alternatives for Call Authentication for Non-IP Traffic, ATIS-1000097.v002 (2022), https://access.atis.org/apps/group_public/download.php/67654/ATIS-1000097.v002.pdf (ATIS-1000097.v002) (report evaluating these different approaches to caller ID authentication on non-IP networks).

⁴⁶ *See* ATIS-1000097.v002 § 6 (noting that both approaches can be used in the call path of a single call).

sent in tandem to the non-IP call signaling.⁴⁷ In this “Out-of-Band” approach, the STIR/SHAKEN caller ID information that in the IP context is contained “in-band” (i.e., within an IP call’s SIP message) is instead transmitted over the Internet, “out-of-band”—that is, separate from the network signaling used to transmit the call itself.⁴⁸ In the most obvious example, the originating voice service provider places the information in a secure location on the Internet—one that is hosted by an entity registered with the Policy Administrator and referred to in the standard as a Secure Telephone Identity Call Placement Service (STI-CPS)—when it originates the call; the terminating voice service provider can then retrieve the information to verify the caller ID information when it terminates the call.⁴⁹ The standard envisions that multiple STI-CPSs could exist and that providers may choose to work with different STI-CPSs, each of which must be able to share information with one another.⁵⁰ While this example is illustrative, under the standard any provider in the call path can insert or retrieve STIR/SHAKEN information to or from an STI-CPS. If an intermediate provider’s network is non-IP and it has received an authenticated SIP call, it can place the STIR/SHAKEN information in an STI-CPS when it converts the call to non-IP.⁵¹ Similarly, if an intermediate provider’s network is IP and it has received a non-IP call, it can retrieve the authentication information from an STI-CPS and insert it back into the Identity header field of the call when it converts the call signaling to SIP.⁵² The standard can thus support a variety of call scenarios where non-IP technology is present in the call path without sacrificing the full scope of information available in STIR/SHAKEN.⁵³

13. The ATIS-1000095 standard, by contrast, provides a method to convey some caller ID authentication information over the non-IP portions of the phone network in-band along with the call.⁵⁴ In this “Non-IP In-Band” approach, the originating voice service provider comes to an agreement with the subsequent provider in the call path on how to share, within the components of a non-IP call, information about what it knows about the caller and its right to use the phone number along with the call.⁵⁵ However, the originating voice service provider cannot use an Identity header field as in a SIP call, nor can it insert the trust information captured by the certificate used in STIR/SHAKEN.⁵⁶ Instead, providers guarantee trust through bilateral agreements between providers that exchange calls with one another.⁵⁷ To work, it requires directly connected providers at each link in the call path to have bilateral agreements in place; without these agreements, a terminating voice service provider cannot have confidence that the additional information provided pursuant to this standard is not itself falsified.⁵⁸ Similar to the Out-of-Band

⁴⁷ This standard builds off of similar work underway by the Internet Engineering Task Force (IETF). See IETF, *Out-of-Band STIR for Service Providers*, Draft (2022), <https://datatracker.ietf.org/doc/draft-ietf-stir-servprovider-ooob/02/>; see also ATIS-1000096 § 2.2 (identifying IETF Out-of-Band STIR draft as an “informative reference”).

⁴⁸ See ATIS-1000096 § 1.1; ATIS-1000097.v002 § A.1.

⁴⁹ ATIS-1000096 § 4.

⁵⁰ *Id.* (noting that the method by which this information would be shared among all registered STI-CPSs in the ecosystem is outside the scope of ATIS-1000096).

⁵¹ *Id.*

⁵² *Id.*

⁵³ See ATIS-1000096 § 8.

⁵⁴ ATIS-1000095.v002 § 1; ATIS-1000097.v002 § A.2.

⁵⁵ See ATIS-1000095.v002 § 4.2 (describing how a provider can encode this information in a non-IP call’s signaling or convey a call’s attestation level by sending traffic over particular trunk groups).

⁵⁶ See ATIS-1000095.v002 § 4.1.

⁵⁷ *Id.*

⁵⁸ See *id.*

approach, an intermediate provider that converts a call to or from IP could translate STIR/SHAKEN information to the Non-IP In-Band information.⁵⁹

14. *May 2022 Robocalls Order and Further Notice.* In our *May 2022 Robocalls Order and Further Notice*, we sought comment on “whether we should require all providers to adopt a non-IP caller ID authentication solution.”⁶⁰ We acknowledged that both ATIS and commenters in previous proceedings had offered specific proposals for authentication over non-IP networks, and solicited comment on whether we should adopt one of these or a modified solution.⁶¹ In response, we received comments urging us to mandate implementation of a non-IP solution,⁶² as well as comments to the contrary arguing that doing so would be premature.⁶³ Commenters opposed to a mandate also argued that we should instead focus our efforts on promoting the transition of non-IP network technology to IP.⁶⁴

III. DISCUSSION

15. In light of the record developed in response to our *May 2022 Robocalls Order and Further Notice*, we now seek comment on caller ID authentication in non-IP networks. We open this inquiry to gain comment on how best to address this gap in our caller ID authentication scheme and carry out the TRACED Act’s directive to require voice service providers “to take reasonable measures to implement an effective call authentication framework in the non-internet protocol networks of the provider of voice service.”⁶⁵ When the Commission adopted the caller ID authentication rules for non-IP networks in the *Second Caller ID Authentication Report and Order*, it explained that it would revisit these rules to account for industry progress—or lack thereof—toward the development of non-IP caller ID authentication technology and provider progress in transitioning their non-IP networks to IP technology.⁶⁶ As such, we seek comment on industry progress toward developing a caller ID authentication framework for non-IP networks, and on the pair of standards ATIS adopted on this subject. We further seek comment on the status of providers in transitioning to a fully IP network and whether, as some commenters have suggested, our efforts can and should be focused on encouraging the IP transition instead of or in addition to promoting caller ID authentication for non-IP networks.

A. Caller ID Authentication in Non-IP Networks

16. We first seek comment on caller ID authentication in non-IP networks. Commission rules implementing the TRACED Act require voice service providers with non-IP network technology either to upgrade their networks to IP or to work to develop a non-IP solution; and when adopting those rules the Commission stated it would “continue to evaluate whether an effective non-IP caller ID

⁵⁹ *See id.*

⁶⁰ *May 2022 Robocalls Order and Further Notice* at 67, para. 173.

⁶¹ *Id.* at 67-68, para. 173 & n.467.

⁶² *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. Comments); TransNexus Comments at 5-6; ZipDX Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 7-8 (rec. Aug. 17, 2022) (ZipDX Comments).

⁶³ *See* ACA Connects Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 9 (rec. Aug. 17, 2022) (ACA Connects Comments at 9); USTelecom Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 17-18 (rec. Aug. 17, 2022) (USTelecom Comments).

⁶⁴ *See* NCTA Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 2-3 (rec. Aug. 17, 2022) (NCTA 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 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.”).

⁶⁵ TRACED Act § 4(b)(1)(B).

⁶⁶ *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1874, para. 32.

authentication framework emerges from the ongoing work that we require.”⁶⁷ The Commission established a threshold, consistent with the TRACED Act, for when it would consider a framework effective: when it is both “fully developed and finalized by industry standards” and “reasonably available . . . on the commercial market.”⁶⁸ Two years have passed since the Commission adopted these rules, and in that time an industry standards group has developed the two standards discussed above. We now seek comment on the state of these new standards, whether we should require implementation of one or both of them, and, if so, the specifics of how we should do so. We further seek comment on any alternative solutions that exist or whether we should address authentication in non-IP networks another way, and on our legal authority for any Commission action to address this issue.

17. As an initial matter, we seek comment on non-IP network technology generally. How prevalent is non-IP network technology across the entire voice network? Are there provider types (e.g., voice service providers vs. intermediate providers), sizes, or business models where non-IP technology is used at a greater or lesser rate? What types of non-IP technology continue to be used? Are there other types of network technology in the phone network that would be considered “non-IP” other than time division multiplexing (TDM) technology in wireline networks and code-division multiple access (CDMA) in wireless networks? How prevalent are any other non-IP technologies? We seek comment on what percentage of calls originate on non-IP networks and whether this share is rising or falling, and at what rate. If providers have increased installation of non-IP technology in their networks in recent years, we seek comment on the reasons why. Should we consider requiring providers to submit data on the percentage of TDM traffic that they originate, exchange, or terminate, as one commenter to our *May 2022 Robocalls Order and Further Notice* suggests?⁶⁹ How specifically would we design such a collection?

18. We further seek comment on the impact of non-IP network technology on the problem of illegal robocalls. Do robocalls disproportionately originate, transit, or terminate on non-IP networks? As STIR/SHAKEN has been implemented on IP networks, have robocalls migrated to non-IP networks? If they have not yet, is it likely that they will? Or are there technological or economic reasons that would make it difficult to leverage non-IP technology for purposes of illegal robocalling? Is the presence of non-IP network technology undermining the efficacy of STIR/SHAKEN and, if so, how significantly? In response to the *May 2022 Robocalls Order and Further Notice*, TransNexus provided data showing that, while more providers have implemented STIR/SHAKEN, “the percentage of calls received at termination with SHAKEN information has not increased,” an outcome it attributes to the notion that “SHAKEN information is not surviving transit across the network because of” non-IP technology.⁷⁰ We seek comment on this data and conclusion.

19. Finally, we seek comment on the pervasiveness of non-IP technology within the networks of originating and terminating providers. Are there cases where non-IP technology is only used at the edge of a provider network in order to establish, maintain, or terminate calls with directly peering providers? And in turn, is SIP signaling used within such provider’s networks to establish, maintain, or terminate calls to its directly connected customers? If this scenario exists, what are the incentives to retain this model? Conversely, what incentives could prompt providers from migrating the non-IP technology to a SIP interconnect model with their peering partner?

1. ATIS Standards

20. We seek comment generally on the characteristics of both of the standards published by ATIS’s Non-IP Call Authentication Task Force—the Out-of-Band approach in ATIS-1000096, and the

⁶⁷ *Id.*

⁶⁸ *Id.*

⁶⁹ See ZipDX Reply, CG Docket No. 17-59, WC Docket No. 17-97, at 6 (rec. Sept. 19, 2022) (ZipDX Reply).

⁷⁰ See TransNexus Reply, CG Docket No. 17-59, WC Docket No. 17-97, at 6 (rec. Sept. 16, 2022) (TransNexus Reply).

Non-IP In-Band approach in ATIS-1000095. What are the pros and cons of each approach? How well do they each address the particular barriers that non-IP networks pose to ubiquitous adoption of caller ID authentication? If neither represents a complete solution, what are the specific deficiencies of each standard and in what ways can and should they be improved to remedy those deficiencies? Are additional ATIS standards, or accompanying standards from another standards body such as the Internet Engineering Task Force (IETF), required, and what would they address? What would the respective implementation costs of these two approaches be, separately or in conjunction, and who would bear those costs? Would either model allow providers that have already transitioned to IP networks and implemented STIR/SHAKEN to avoid further upgrades specifically to accommodate non-IP providers?⁷¹ Do these standards adequately address non-IP technology throughout the entire call path; in other words, do they resolve issues around non-IP voice service providers, non-IP intermediate providers, and non-IP interconnection? In a report, ATIS states that the solutions offered in the two standards are not mutually exclusive and that a combination of both solutions could be used by a single provider within its network or by several providers across a given call path.⁷² We seek comment on this view. Do the standards complement one another, and are both standards equally feasible and effective? To the extent that there are multiple non-IP network technologies, can both standards accommodate all types of non-IP network technologies?

21. We seek comment on issues unique to the Out-of-Band standard in ATIS-1000096. In a report, ATIS found that this standard would complement the existing STIR/SHAKEN framework and not require any changes to the networks of providers currently using STIR/SHAKEN in their IP networks.⁷³ We seek comment on these findings. Are there any compatibility concerns between the Out-of-Band standard and the STIR/SHAKEN framework that we should consider? Are there any security concerns associated with the deployment of the Out-of-Band standard?⁷⁴ We ask that commenters that raise security concerns describe if and how the standards-making process fell short in considering these concerns, be specific about the way the ATIS-1000096 standard fails to address those concerns, and propose actionable steps that could be taken to address them promptly. We seek comment on the specific costs a provider would incur to implement the Out-of-Band standard on its network, and how long it could take to achieve full implementation of the standard across the network. Alongside our current STIR/SHAKEN rules for IP networks, would full implementation of this standard on non-IP networks—including the networks of both voice service and intermediate providers—mean that every call in the United States could now be authenticated and verified under the STIR/SHAKEN framework?

22. In October 2021, the North American Numbering Council (NANC) released a report identifying aspects of a governance structure that would be needed to fully implement the Out-of-Band standard.⁷⁵ The NANC identified that the Out-of-Band standard allows for multiple STI-CPSs to store the caller ID authentication information on the Internet, which permits the voice service provider originating

⁷¹ Compare TransNexus Comments at 6 (arguing that the “burden of implementing either ATIS-1000095 or ATIS-1000096 (or both) would only fall on those providers that rely on non-IP technology and interconnections”) with NCTA Comments at 2 (arguing that a non-IP solution would burden IP-based providers by requiring that they “accommodate alternative authentication methods”); see also Cloud Communications Alliance Reply, CG Docket No. 17-59, WC Docket No. 17-97, at 4 (rec. Sept. 16, 2022) (Cloud Communications Alliance Reply) (noting that “these solutions would not require actions by IP-based providers that have implemented STIR/SHAKEN . . . [t]he burden of implementing the ATIS solutions would fall only on providers relying on non-IP technology and interconnection”).

⁷² See ATIS-1000097.v002 § 6.

⁷³ See ATIS-1000097.v002 § A.1.

⁷⁴ See USTelecom Comments at 17 (“STIR/SHAKEN over TDM solutions raise substantial security concerns . . . ”); ATIS-1000097.v002 § A.1.

⁷⁵ NANC Oct. 2021 Report § 2.4.

the call to use a different STI-CPS than the voice service provider terminating it.⁷⁶ In order for this system to function, the NANC found, each STI-CPS in the ecosystem would need to share the caller ID authentication information it receives with every other STI-CPS, requiring a governance system such as an administrator or another entity to manage a central list of every STI-CPS in the ecosystem.⁷⁷ What progress has been made on addressing this governance issue since that time? Is it possible that terminating voice service providers may not receive authentication information in a timely manner because of the time required to disseminate caller ID authentication information to all STI-CPSs (i.e., is there a “race condition”)? Are there any additional governance-related issues we would need to address? Could the existing STIR/SHAKEN governance system be adapted to address governance issues unique to the Out-of-Band standard?⁷⁸ If so, how? Alternatively, we seek comment on the characteristics of a standalone governance structure for just the Out-of-Band standard and the steps the Commission can or should take to establish such a structure.

23. We also seek comment on issues unique to the Non-IP In-Band standard in ATIS-1000095. In its report, ATIS found that the Non-IP In-Band standard does not allow for providers to share with each other the full complement of information or in the same manner as the current STIR/SHAKEN framework because a provider is limited in the amount of information it can share over a non-IP network.⁷⁹ However, ATIS identified different measures that could be used to facilitate the sharing of some of this information between providers in certain circumstances, including information beyond simply the attestation level of a call.⁸⁰ Are there any compatibility issues between the standard and the STIR/SHAKEN framework? From the perspective of a terminating voice service provider, we seek comment on the difference between the information it would receive from a SIP call authenticated with STIR/SHAKEN and a call routed over both IP and non-IP networks where the non-IP portions are authenticated with the Non-IP In-Band standard. Is the information provided by the Non-IP In-Band standard as useful as that provided by STIR/SHAKEN? Should we understand the Non-IP In-Band standard as ultimately providing less information to the terminating voice service provider than under the current STIR/SHAKEN framework or under the Out-of-Band standard? If so, which information would the terminating voice service provider not receive as compared to STIR/SHAKEN? To what extent would this lack of information undermine the effectiveness of caller ID authentication across the voice network and the goal of preventing illegally spoofed robocalls?

24. In what situations would deploying the Non-IP In-Band standard be more effective than the Out-of-Band standard? We note that the Non-IP In-Band standard requires an extensive network of provider agreements to be effective. How cumbersome would ensuring these agreements are in place be for the industry in general and providers more specifically? How many bilateral agreements would need to be in place for the average call? Is it feasible to require bilateral agreements at each interconnection point in an average call path? Does using this structure of bilateral agreements to ensure trust between providers under the Non-IP In-Band standard pose any risks to consumers? Is there a maximum number of bilateral agreements beyond which the trust in the system would erode? ATIS found that, under this standard, there would be no additional equipment or network changes needed for providers already operating IP networks.⁸¹ We seek comment on this finding. What are the specific costs that providers

⁷⁶ *Id.*

⁷⁷ *Id.*; ATIS-1000096 § 4 (noting that the method by which each STI-CPS would discover each other is outside the scope of this standard).

⁷⁸ See TransNexus Reply at 10-11.

⁷⁹ See ATIS-1000097.v002 § A.2.

⁸⁰ See *id.*; ATIS-1000095.v002 §§ 4.2, 4.11 (describing how providers can, for example, encode the information typically required by the STIR/SHAKEN framework into different parameters of a non-IP call or designate certain trunk groups as conveying the attestation level of exchanged traffic).

⁸¹ See ATIS-1000097.v002 § A.2.

operating non-IP networks would bear to implement the Non-IP In-Band standard, and how long could it take to achieve full implementation of the standard across the network? How do the costs of implementing the Non-IP In-Band standard compare to implementing the Out-of-Band standard? Alongside our current STIR/SHAKEN rules for IP networks, would full implementation of this standard on non-IP networks—including the networks of both voice service and intermediate providers—mean that every call in the United States could now be authenticated and verified under the STIR/SHAKEN framework?

25. *Effective Framework.* We seek comment on whether the two ATIS standards meet the Commission’s established threshold—fully developed and finalized by industry standards and reasonably available on the commercial market—such that an implementation mandate of one or both standards is appropriate. We asked in our *May 2022 Robocalls Order and Further Notice* whether to mandate implementation of a non-IP caller ID authentication solution.⁸² In response, some commenters argue that we should.⁸³ These commenters identify progress made on standards documents as a reason to require implementation,⁸⁴ and state that solutions are commercially available.⁸⁵ One commenter argues that the ATIS standards satisfy the TRACED Act standard from section (4)(b)(5)(B),⁸⁶ and another argues that the ATIS standards satisfy the threshold the Commission set in the *Second Caller ID Authentication Report and Order*.⁸⁷ By contrast, some commenters oppose an implementation mandate. They argue that industry lacks consensus on either standard as a path forward to achieve ubiquitous deployment of caller ID authentication.⁸⁸ In light of this record we seek further, targeted comment on how the two ATIS standards do—or do not—meet the Commission’s established threshold.

26. We seek comment on whether one or both of these standards is, as established by the Commission in the *Second Caller ID Authentication Report and Order*, “fully developed and finalized by industry standards” and “reasonably available . . . on the commercial market.”⁸⁹ Regarding the first prong, does the publication of standards by ATIS represent full development and finalization? When the

⁸² *May 2022 Robocalls Order and Further Notice* at 67-68, para. 173.

⁸³ See Cloud Communications Alliance Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 4-5 (rec. Aug. 17, 2022) (Cloud Communications Alliance Comments); Credit Union National Association et al. Comments at 3-5; TransNexus Comments at 5-6; ZipDX Comments at 7-8.

⁸⁴ See ZipDX Comments at 7 (“Now that non-IP authentication solutions have been codified, it is time to mandate adoption.”); see also Cloud Communications Alliance Comments at 4 (acknowledging the ATIS Out-of-Band standard as an option for providers to implement); TransNexus Comments at 5 (citing both ATIS standards as options for providers to implement); Letter from Dave Frigen, Chief Operating Officer, Wabash Communications, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 17-97, at 2 (filed Aug. 17, 2021) (“The approved standards are now available.”) (Wabash Aug. 2021 *Ex Parte*).

⁸⁵ See Cloud Communications Alliance Comments at 4-5 (“The key point is that commercially available solutions exist. There is no reasonable basis to continue to exempt non-IP networks from participating in the call validation process.”); Credit Union National Association et al. Comments at 4-5 (referring to “the commercially available alternative technologies that enable caller ID verification on . . . legacy networks”); see Wabash Aug. 2021 *Ex Parte* at 2 (“Out-of-Band SHAKEN software is . . . commercially available today.”).

⁸⁶ See TransNexus Reply at 5.

⁸⁷ See NTCA Reply, CG Docket No. 17-59, WC Docket No. 17-97, at 4 (rec. Sept. 16, 2022) (NTCA Reply).

⁸⁸ See ACA Connects Comments at 9 n.23 (arguing that when compared to the initial caller ID authentication standards, “[n]o non-IP call authentication solution appears so far to have achieved a comparable degree of industry consensus on a path forward for implementation”); see also USTelecom Comments at 17-18 (arguing that there “are still no standardized, secure, practical, and currently implementable non-IP solutions”); but see Cloud Communications Alliance Reply at 3 (“Claims that there are no standardized or implementable solutions ignores the current use of commercially available solutions and that ATIS has promulgated standards for two solutions.”).

⁸⁹ *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1874, para. 32.

Commission adopted this threshold, it explained that this “would exist when the fundamental aspects of the protocol are standardized and implementable by industry.”⁹⁰ Have the published standards met this threshold? If not, in what specific ways do they fall short? We seek comment on what specific aspects of these standards lack consensus, as some commenters argue.⁹¹ What problems still need to be solved? Does any lack of consensus stem from technical infeasibility concerns or other factors? Why is ATIS’s adoption of the Out-of-Band and Non-IP In-Band standards itself not indicative of industry consensus? What more needs to be done beyond ATIS publication, either by ATIS or other industry groups, before one or both of these standards would be considered fully developed and finalized? Is it necessary for the IETF to finish related work on Out-of-Band standards and, if so, why?⁹² What is the status of those parallel efforts and when will that work be completed? How does the alleged lack of industry consensus relate to the Commission’s threshold that a standard be “fully developed and finalized by industry standards” before requiring implementation? What progress is industry making to address any open issues? Do the recent revisions to ATIS-1000095 address them? Would rules requiring the implementation of one or both of these ATIS standards drive the development of consensus on whatever open issues remain?

27. Regarding the second prong, is the technology reasonably available on the commercial market? When the Commission adopted this prong, it detailed that it would consider it met when “the equipment and software necessary for implementation is commercially available.”⁹³ One commenter asserts that “commercially available solutions exist,”⁹⁴ another states that the standards “meet the requirements . . . for a non-IP standard that is ‘reasonably available,’”⁹⁵ and others represent that providers have implemented solutions based on the Out-of-Band standard.⁹⁶ Does this mean that the equipment and software needed to implement either of the standards is available on the commercial market? If so, what is the range of costs of this equipment and software, and how should we incorporate cost into our analysis of whether a technology is reasonable available? And are these solutions interoperable? Given that one small provider represented that it has already implemented the Out-of-Band standard,⁹⁷ should we understand that costs associated with implementation can be reasonably borne by providers of all sizes? If not, what needs to occur to make the required equipment and software available and affordable? In the time since these standards were adopted, how widely have they been implemented?⁹⁸ If one or neither have yet to be widely implemented, we seek comment on why. Are providers waiting for a Commission mandate to begin implementation, so as to avoid investing in a solution different from one we may ultimately require?

28. To the extent industry has not made sufficient progress on non-IP caller ID authentication to meet the Commission’s established threshold for an implementation mandate, we seek comment on whether and how to address this outcome. When it adopted the threshold for determining when to

⁹⁰ *Id.* at 1874, para. 32 n.116.

⁹¹ See ACA Connects Comments at 9 n.23; USTelecom Comments at 17-18.

⁹² See IETF, *Out-of-Band STIR for Service Providers*, Draft (2022), <https://datatracker.ietf.org/doc/draft-ietf-stir-servprovider-oob/02/>.

⁹³ *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1874, para. 32 n.116.

⁹⁴ See Cloud Communications Alliance Comments at 4-5.

⁹⁵ NTCA Reply at 4.

⁹⁶ TransNexus Reply at 8-12 (stating that they have “over 50 providers using Out-of-Band PASSporT Transmission Involving TDM Networks as described in the ATIS-1000096 standard”); see also Wabash Aug. 2021 *Ex Parte* at 2-3 (provider stating it implemented the Out-of-Band solution as early as August 2021).

⁹⁷ Wabash Aug. 2021 *Ex Parte* at 2-3.

⁹⁸ See TransNexus Reply at 9.

mandate a non-IP solution, the Commission stated that “we may revisit our approach . . . if we find that industry has failed to make sufficient progress,” and explained that it would “pursue additional steps to ensure more fulsome caller ID authentication in non-IP networks, including by revisiting our non-prescriptive development-based approach if needed.”⁹⁹ The pair of ATIS standards were first published over a year ago, and in that time non-IP voice service providers have been required to work to develop a non-IP caller ID authentication solution if they have not upgraded their entire networks to IP.¹⁰⁰ To the extent voice service providers have not yet resolved any identified issues with non-IP authentication solutions, why have they not done so? Should we modify the obligation we place on voice service providers with non-IP network technology, or more closely scrutinize their compliance with the existing obligation to work to develop a non-IP authentication solution?

29. In the alternative or in addition, should we reconsider our threshold for determining when a non-IP framework is “effective” under the TRACED Act and thus warrants an implementation mandate?¹⁰¹ Do the two benchmarks that the Commission identified in the *Second Caller ID Authentication Report and Order* remain the best way to judge whether a non-IP caller identification framework is effective?¹⁰² Should we consider different factors and, if so, which should we consider? For example, should we consider revising our framework to include any or all of the factors ATIS used to analyze non-IP call authentication solutions in its technical report on the subject?¹⁰³ How would any revisions square with the TRACED Act, which requires us to grant an extension for non-IP voice service providers “until a call[er ID] authentication protocol has been developed for calls delivered over non-[IP] networks and is reasonably available”?¹⁰⁴

30. *Implementing Rules.* If we were to require the adoption of either of the ATIS standards, how should we structure our rules? As we have explained, ATIS has said these standards can complement each other and are not mutually exclusive.¹⁰⁵ If we found that both standards met the threshold for an implementation mandate, do commenters recommend we mandate the adoption of both solutions, just one solution, or that we give providers a choice?¹⁰⁶ Are there benefits to requiring one solution to be widely adopted as opposed to a patchwork approach of different solutions? If we were to allow for the adoption of either standard, how would we structure our rules? Should our rules encourage the deployment of one solution over another? On what timeline should we require implementation of one or both frameworks? What would be a reasonable implementation deadline?

⁹⁹ *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1874, para. 32.

¹⁰⁰ 47 CFR § 64.6303(b).

¹⁰¹ See TRACED Act § 4(b)(1)(B); *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1874, para. 32.

¹⁰² *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1874, para. 32.

¹⁰³ As part of this 2021 technical report, ATIS used eleven factors for evaluating potential solutions: (i) the scope of the solution; (ii) the non-IP call scenarios covered; (iii) whether changes are required to existing TDM network infrastructure; (iv) whether the solution can co-exist with other non-IP call authentication solutions; (v) the knowledge of network topology needed to implement the solution; (vi) whether the solution can support a variety of different use cases; (vii) any security considerations; (viii) what impact the solution might have on the transition to an all-IP network; (ix) whether the approach complements the STIR/SHAKEN framework, rather than competes or duplicates it; (x) whether the solution could be extended to support international deployment of call authentication; and (xi) whether there are any other dependencies other than those previously identified, such as changes to existing standards or policies. See ATIS-1000097 § 4.3.

¹⁰⁴ TRACED Act § 4(b)(5)(B).

¹⁰⁵ See ATIS-1000097.v002 § 6.

¹⁰⁶ See TransNexus Comments at 5-6 (urging the Commission to require providers convert non-IP technology to IP, implement ATIS-1000095, or implement ATIS-1000096).

31. We also seek comment on whether there are unique considerations for how any potential rules would apply to different types of providers. To be effective, would either or both ATIS standards require us to mandate use of the standard(s) by both voice service providers and intermediate providers? For example, the Out-of-Band standard describes a variety of different call scenarios, some involving an intermediate provider interacting with an STI-CPS.¹⁰⁷ If we were to require both voice service providers and intermediate providers to implement this standard, would we need to specify which provider fulfills which function? What would be the appropriate requirements for each type of provider? Is the standard document sufficiently clear on the roles each provider in a call path must play? Are there any intermediate provider-specific issues for the Commission to consider regarding the implementation of either standard? If so, how would we structure our rules to account for them? Should we apply any obligations to non-IP gateway providers and, if so, are there unique considerations around gateway providers' role we need to take into account? If not, why should we exclude these providers from any rules we adopt? Would any rules we adopt need to uniquely account for non-IP interconnection?

2. Alternatives

32. We seek comment on whether there are alternatives to the ATIS standards we should consider to address caller ID authentication on non-IP networks. Are there other standards bodies, entities, or organizations that are working on ways to enable caller ID authentication on non-IP networks or incorporate non-IP network technology into the STIR/SHAKEN framework?¹⁰⁸ If so, we seek comment on the feasibility and efficacy of those alternative approaches. Beyond mandating the adoption of a non-IP caller authentication standard that we deem effective, are there other mechanisms we could use to address the impact of non-IP network technology on ubiquitous participation in caller ID authentication? For example, should we consider rules requiring that originating providers and intermediate providers only exchange calls downstream with an intermediate provider that can preserve the STIR/SHAKEN information in IP? Would such a rule make implementation of either the Out-of-Band or Non-IP In-Band standards unnecessary? Similarly, in response to the *May 2022 Robocalls Order and Further Notice*, ZipDX suggested a scheme by which all providers would be "required to send onward only signed calls."¹⁰⁹ Would this approach be feasible and effective?

33. We seek comment on whether there are any alternative steps we should take to address the impact of non-IP interconnection points on caller ID authentication. The October 2021 NANC Report recommended that industry stakeholders examine this problem in a working group expected to issue its report before the end of this year.¹¹⁰ We welcome the final report of that working group as part of this record, and we seek comment on whether there are any additional steps we can take to help this effort succeed. We are also aware of efforts underway at ATIS on a technical report describing an interconnect profile for VoIP service providers who choose to interconnect over the public Internet.¹¹¹ We seek comment on these efforts, including whether the proposed approach sufficiently satisfies quality of

¹⁰⁷ See ATIS-1000096 § 8.1.

¹⁰⁸ See, e.g., AB Handshake Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 6-7 (rec. Nov. 26, 2021) (providing a description of its non-IP caller ID authentication solution that involves the originating and terminating voice service providers using a call registry system to confirm that the user of the number in the caller ID field originated the call, removing the involvement of intermediate providers in the caller ID authentication process altogether); Cloud Communications Alliance Comments at 4 (identifying AB Handshake's solution as a potential out-of-band call validation solution).

¹⁰⁹ ZipDX Reply at 5-6 (identifying alternatives available to a provider to comply with such a requirement).

¹¹⁰ NANC Oct. 2021 Report § 2.4.

¹¹¹ See ATIS, IPNNI-2022-00007R004.docx, ATIS-10000xx, https://access.atis.org/apps/group_public/download.php/64564/IPNNI-2022-00007R004.docx (last visited Oct. 27, 2022).

service requirements of providers, and whether it would provide enough incentive for non-IP providers to migrate their infrastructure to support SIP signaling using STIR/SHAKEN protocols.

3. Legal Authority

34. We seek comment on what legal authority we could rely on for any rules regarding non-IP caller ID authentication. The text of section 4(b)(1)(B) of the TRACED Act, 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,” appears to contemplate the Commission adopting rules to mandate the adoption of a non-IP caller ID authentication solution by voice service providers.¹¹² 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 solution by voice service providers? In the *Second Caller ID Authentication Report and Order*, the Commission found that the text of the TRACED Act itself, section 251(e) of the Communications Act of 1934 (the Act), and the Truth in Caller ID Act, each provided independent sources of authority to adopt the existing rules implementing section 4(b)(1)(B) covering originating and terminating providers.¹¹³ Do these provisions continue to provide us independent authority to require voice service providers to adopt one or more non-IP caller ID authentication solutions? Are there other potential sources of authority we should consider?

35. We also seek comment on our authority to place obligations on intermediate providers regarding non-IP caller ID authentication. The text of section 4(b)(2)(A) of the TRACED Act limits the scope of the section to providers of “voice service,” defined as a service that is “interconnected with the public switched telephone network and that furnishes voice communications to an end user.”¹¹⁴ In the *First Caller ID Authentication Report and Order and Further Notice*, the Commission interpreted this language as encompassing only originating and terminating voice service providers.¹¹⁵ Does this section only provide us authority to mandate a non-IP caller ID authentication solution for originating and terminating voice service providers? If so, considering that both the Out-of-Band and Non-IP In-Band standards contemplate roles performed by intermediate providers, how could we structure our rules to provide an effective mandate under our TRACED Act authority? In the *Second Caller ID Authentication Order* and the *May 2022 Robocalls Order and Further Notice*, the Commission relied on authority under section 251(e) of the Act and the Truth in Caller ID Act to impose caller ID authentication obligations on intermediate and gateway providers.¹¹⁶ In addition, in the *May 2022 Robocalls Order and Further Notice*, we found that our ancillary authority in section 4(i) of the Act provides an independent basis to impose caller ID authentication obligations on intermediate providers that have not been classified as common carriers.¹¹⁷ We seek comment on whether these provisions offer us sufficient authority to require intermediate providers to adopt a non-IP caller ID authentication solution. If not, and if we found that a non-IP caller ID authentication framework met our threshold, would it be effective if we did not impose obligations on intermediate providers? Are there other sources of authority we should consider to potentially impose non-IP caller ID authentication obligations on intermediate providers, including gateway providers?

¹¹² TRACED Act § 4(b)(1)(B).

¹¹³ *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1875, paras. 33-35; 47 U.S.C. §§ 227(e), 227b, 251(e).

¹¹⁴ TRACED Act § 4(a)(2)(A).

¹¹⁵ *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3259, para. 37.

¹¹⁶ *May 2022 Robocalls Order and Further Notice* at 47-48, paras. 112-13; *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1931-32, paras. 153-55; 47 U.S.C. §§ 227(e), 251(e).

¹¹⁷ *May 2022 Robocalls Order and Further Notice* at 50, paras. 118-19.

B. The IP Transition

36. The Commission, for the last decade, has been taking regulatory action to encourage the transition to an all IP-network and promote new and innovative product offerings to customers.¹¹⁸ Recognizing the interest in continuing to encourage providers to transition their networks, some commenters to the *May 2022 Robocalls Order and Further Notice* oppose requiring a non-IP caller ID authentication solution on the theory that doing so might detract from the transition to an all-IP network.¹¹⁹ According to NCTA, non-IP caller ID authentication would “eliminate incentives for other providers to transition to IP-based solutions,” thus “distract[ing] from the ultimate goal of full STIR/SHAKEN implementation.”¹²⁰ USTelecom similarly argues that requiring implementation of a non-IP authentication solution would be resource-intensive and “detract from other, more fruitful efforts”—namely, ubiquitous IP network technology that in turn would enable end-to-end STIR/SHAKEN implementation.¹²¹ Conversely, the Cloud Communications Alliance argues that a non-IP caller ID authentication solution “need not hamper or delay the IP interconnection.”¹²² While the IP transition implicates issues well beyond our narrow caller ID authentication inquiry, we take this opportunity to seek comment on these arguments, the status of the IP transition, and on avenues to affirmatively promote the IP transition.

1. Caller ID Authentication and the IP Transition

37. We first seek comment on the nexus between non-IP caller ID authentication and the IP transition generally. In lieu of pursuing a non-IP authentication solution, should we instead further encourage or require providers using non-IP technology in their networks to upgrade to IP? We seek comment on whether encouraging or requiring voice service providers and intermediate providers to spend resources on a non-IP authentication solution would delay the IP transition. Would requiring implementation of a non-IP authentication solution discourage providers from upgrading non-IP network technologies? In what ways? For example, ATIS observes that the adoption of the Out-of-Band standard may necessitate upgrades to non-IP systems that would be rendered useless if a provider transitioned to IP-based technology.¹²³ Would implementation of this standard discourage providers from upgrading to

¹¹⁸ See, e.g., *Modernizing Unbundling and Resale Requirements in an Era of Next-Generation Networks and Services*, WC Docket No. 19-308, Report and Order, 35 FCC Rcd 12425 (2020) (relieving incumbent local exchange carriers of various unbundled network and avoided-cost resale requirements); *Accelerating Wireline Broadband Deployment by Removing Barriers to Infrastructure Investment*, WC Docket No. 17-84, Second Report and Order, 33 FCC Rcd 5660 (2018) (streamlining the discontinuance process for technology transitions); *Accelerating Wireline Broadband Deployment by Removing Barriers to Infrastructure Investment*, WC Docket No. 17-84, Report and Order, Declaratory Ruling, and Further Notice of Proposed Rulemaking, 32 FCC Rcd 11128, 11142, para. 33 (2017) (streamlining the copper retirement process); *Technology Transitions et al.*, GN Docket No. 13-5, WC Docket No. 13-3, Declaratory Ruling, Second Report and Order, and Order on Reconsideration, 31 FCC Rcd 8283, 8304-8305, paras. 64-65 (2016) (adopting the adequate replacement test); *Technology Transitions et al.*, GN Docket No. 13-5 et al., Order, Report and Order and Further Notice of Proposed Rulemaking, Report and Order, Order and Further Notice of Proposed Rulemaking, Proposal for Ongoing Data Initiative, 29 FCC Rcd 1433, 1435, para. 1 (2014) (seeking proposals for service-based experiments in connection with technology transitions).

¹¹⁹ See NCTA Comments at 2-3; Telnix Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 4 (rec. Aug. 17, 2022); USTelecom Comments at 18.

¹²⁰ NCTA Comments at 2.

¹²¹ See USTelecom Comments at 17-18 (citing NANC Oct. 2021 Report at 15).

¹²² Cloud Communications Alliance Reply at 3 (observing that “the out-of-band solution for non-IP networks described in ATIS-1000096 states as one of its core principles that the solution ‘supports and facilitates the long-term industry goal of migrating to VoIP-based networks’” (quoting ATIS-1000096 at § 1.1)).

¹²³ ATIS-1000097.v002 § A.1 (asserting there would be “stranded functionality”); see also USTelecom Comments at 17.

IP, given that doing so would make their investment in a non-IP authentication solution obsolete? Are providers currently using resources to upgrade their networks to IP technology that would need to be diverted to accommodate a non-IP caller ID authentication framework? What is the relative scope of resources that would need to be diverted to non-IP caller ID authentication as compared to those resources called for by the IP transition?

38. We next seek comment on the importance of preventing harm to the consumers. Even if requiring a non-IP solution now slows the future IP transition,¹²⁴ consumers today face the problem of illegal robocalls, and caller ID authentication represents a key part of the Commission's—and Congress's—plan for combatting illegal robocalls. To that end, we seek comment on the current status of the IP transition and whether the complete IP transition is likely to occur on a compressed enough timetable to ensure that all people can benefit from the protections offered by ubiquitous caller ID authentication deployment. We note that the Commission and major providers have been discussing the transition from non-IP to IP networks for more than a decade. In 2011, one of the recommendations of the Technology Advisory Committee was to establish 2018 as a date certain for the “PSTN sunset,” when the transition from non-IP to IP technology would be complete.¹²⁵ AT&T cited this goal with approval when it filed its petition on November 7, 2012, asking the Commission to consider conducting trial runs of the transition to next-generation services, including the retirement of non-IP facilities and service offerings and their replacement with IP-based alternatives.¹²⁶ More recently, in arguing for changes to the Commission's part 51 rules, including additional flexibility for copper retirements, USTelecom claimed that “[l]egacy networks that rely on copper and TDM [non-IP] technology are fast becoming relics, serving fewer and fewer telecommunications users as newer broadband services and technologies systematically replace them.”¹²⁷ But we have also received comment in this docket contending that there remains significant work to be done before the transition to an all-IP voice network is complete.¹²⁸ We therefore seek comment on the status of the transition from non-IP to an all-IP network. When do commenters believe the transition will be complete? How close is the transition from being completed? Does that timeframe counsel promoting non-IP caller ID authentication in the interim, before the IP transition is complete, given the consumer harms stemming from illegal robocalls? To the extent that a commenter disagrees, we seek detailed and supported arguments to the contrary.

39. Additionally, we seek comment on whether we have discretion to determine that non-IP caller ID authentication can be forgone altogether in order to avoid detracting from the IP transition. Congress in the TRACED Act required the Commission to mandate that voice service providers “take reasonable measures to implement an effective call authentication framework in the non-[IP] networks of the provider of voice service.”¹²⁹ How do commenters in favor of forgoing a non-IP authentication solution reconcile their advocacy with the TRACED Act's language?¹³⁰ And given that the TRACED Act

¹²⁴ See USTelecom Reply at 15.

¹²⁵ FCC Technology Advisory Council, Status of Recommendations, at 15-16 (June 29, 2011), <https://www.fcc.gov/oet/tac/2011>.

¹²⁶ AT&T Petition to Launch a Proceeding Concerning the TDM-to-IP Transition, GN Docket No. 12-353, at 2-3 n.3, 4 n.7 (filed Nov. 7, 2012).

¹²⁷ USTelecom Comments, WC Docket No. 17-84, at 21-22 (rec. June 15, 2017).

¹²⁸ See TransNexus Reply, CG Docket No. 17-59, WC Docket No. 17-97, at 4 (rec. Jan. 10, 2022) (TransNexus Jan. 2022 Reply); see also Cloud Communications Alliance Reply at 3 (claiming that “the timing for implementation of” the technology transition “is unclear”).

¹²⁹ TRACED Act § 4(b)(1)(B).

¹³⁰ See NCTA Reply at 4-5 (observing that “Congress made clear its desire to have all calls authenticated”).

includes a threshold for when we should mandate implementation,¹³¹ how do these commenters suggest we nonetheless decline to mandate an effective framework when that threshold is met?

2. Actions to Encourage the IP Transition

40. If we were to pursue the promotion of the IP transition—whether instead of or in addition to any non-IP caller ID authentication solution—we seek comment on specific steps we should take toward that end. First, we seek comment on what actions we should take to develop and build consensus around an approach to resolve issues standing in the way of the complete IP transition. The IP transition in certain circumstances may require action by voice service providers, including extensive network overhauls in sparsely populated regions, that are not commercially viable. Historically, the Commission has observed that where “the immediate prospect for stand-alone private sector action is limited,”¹³² Commission action may be necessary to achieve a solution; other times, industry comes to the Commission with solutions.¹³³ Should we develop and then work toward a particular solution that would address the remaining IP transition in whole or in part? For example, we could direct Commission staff to develop a proposal on the subject of the IP transition. We seek comment on the specific topic or topics that Commission staff could most effectively address if this approach were adopted. Instead, should we take steps to encourage stakeholders to develop consensus around how to facilitate the IP transition in the areas that remain largely TDM, either in whole or in part, and present that consensus to the Commission? What steps should we take? The Commission has previously used both of these approaches to generate solutions to complex issues: in the intercarrier compensation context, the Commission both adopted a policy that originally arose out of white papers developed by Commission staff,¹³⁴ and drew on consensus developed by a wide-ranging cross-section of stakeholders.¹³⁵ Are one or both of these approaches appropriate in this case? If one approach would be preferable to another, why? Are there other approaches we should consider?

41. Second, we seek comment on any unintended outcomes caused by Commission rules, such as our interconnection or intercarrier compensation rules, and whether we should revise any rules to encourage the IP transition. For example, are there any rules that create regulatory asymmetries or that encourage providers to delay or forgo upgrading their network technology to IP?¹³⁶ If so, how should these rules be changed? Are there targeted rule changes we could adopt to promote the IP transition?¹³⁷

¹³¹ See TRACED Act § 4(b)(5)(B) (calling for an extension “until a call[er ID] authentication protocol has been developed for calls delivered over non-[IP] networks and is reasonably available”).

¹³² *Connect America Fund et al.*, WC Docket Nos. 10-90 et al., Report and Order and Further Notice of Proposed Rulemaking, 26 FCC Rcd 17663, 17668, para. 5 (2011) (*USF-ICC Transformation Order* or *USF/ICC Transformation Further Notice*), *aff’d*, *In re FCC 11-161*, 753 F.3d 1015 (10th Cir. 2014), *cert. denied*, 135 S. Ct. 2050 and 135 S. Ct. 2072 (2015).

¹³³ See, e.g., *USF-ICC Transformation Order*, 26 FCC Rcd at 17936, para. 803 (establishing a timeline for intercarrier compensation reform with transition periods based in part on a proposal submitted by the ABC Plan Coalition, a stakeholders group).

¹³⁴ See *USF-ICC Transformation Order*, 26 FCC Rcd at 17676, para. 34; see also Jay M. Atkinson & Christopher C. Barnekov, Federal Communications Commission Office of Plans and Policy, *A Competitively Neutral Approach to Network Interconnection*, OPP Working Paper No. 34 (2000), <https://www.fcc.gov/reports-research/working-papers/competitively-neutral-approach-network-interconnection>; Patrick DeGraba, Federal Communications Commission Office of Plans and Policy, *Bill and Keep at the Central Office As the Efficient Interconnection Regime*, OPP Working Paper No. 33 (2000), <https://www.fcc.gov/reports-research/working-papers/bill-and-keep-central-office-efficient-interconnection-regime>.

¹³⁵ See, e.g., *USF-ICC Transformation Order*, 26 FCC Rcd at 17936, para. 803.

¹³⁶ See ZipDX Reply at 5 (noting that “[s]ome carriers have zero motivation” to upgrade to IP and may even have “some regulatory inter-carrier compensation advantages”).

¹³⁷ See NTCA Reply at 7.

Many of our rules address complicated issues with long histories that involve difficult issues of economics. To the extent commenters argue we should modify or adopt new rules to promote the IP transition, we seek comment on how we can avoid creating new unintended consequences. Additionally, we seek comment on any costs and benefits that likely would arise out of any proposed rule modifications. If, for example, a rule change would eliminate a mechanism that generates revenue for a provider, how should the Commission address that loss of revenue?

42. Third, we seek comment on whether we should take a more aggressive approach to promoting the IP transition by requiring providers to take action to upgrade their networks. One commenter in this docket has suggested we go so far as to establish a regulatory sunset for non-IP technology.¹³⁸ Should we pursue such an approach, or in the alternative adopt a new goal date for the sunset? If so, what date would be realistic? Beyond enabling providers to implement STIR/SHAKEN, what specific benefits would this approach offer? Regarding caller ID authentication, could this timeline be short enough to avoid adopting a non-IP authentication requirement entirely, or would we nonetheless need to mandate one in the interim? What costs would providers incur to upgrade their networks to IP, and how do these compare to implementing non-IP authentication solutions? Are there other parties that may be impacted, and what costs would they bear? How would we address recovery of these costs? Should the Commission consider adopting a mechanism allowing providers to recover their costs? If so, what factors should the Commission consider in adopting a cost recovery mechanism? If we adopted a general sunset for non-IP technology, what would the rule require? Rather than a general sunset, should we adopt a more targeted rule or set of rules to phase out non-IP technology? What would a more targeted rule require? What impact would a full IP transition have on other Commission rules, and what revisions would be required to those rules? And what legal authority would we rely on to take this action?

IV. PROCEDURAL MATTERS

43. *Ex Parte Rules.* This proceeding shall be treated as a “permit-but-disclose” proceeding in accordance with the Commission’s *ex parte* rules.¹³⁹ 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 rule 1.1206(b).¹⁴⁰ In proceedings governed by rule 1.49(f) or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda

¹³⁸ Letter from Richard Shockey, Principal, Shockey Consulting, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 17-97, at 1-2 (filed July 29, 2021) (arguing that “[t]here is a critical need for All IP Interconnection and a Sunset of TDM/SS7 technology in the PSTN to . . . tackle the long-term problem of robocalls” and observing that the United Kingdom has set a sunset date of 2025 for TDM/SS7).

¹³⁹ 47 CFR § 1.1200 *et seq.* Although the Commission’s rules do not generally require *ex parte* presentations to be treated as “permit but disclose” in Notice of Inquiry proceedings, *see id.* § 1.1204(b)(1), we exercise our discretion in this instance, and find that the public interest is served by making *ex parte* presentations available to the public, in order to encourage a robust record. *See id.* § 1.1200(a).

¹⁴⁰ 47 CFR § 1.1206(b).

summarizing oral *ex parte* presentations, and all attachments thereto, must 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).¹⁴¹ Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

44. *Comment Filing Procedures.* Pursuant to sections 1.415, 1.419, and 1.430 of the Commission's rules, 47 CFR §§ 1.415, 1.419, 1.430, 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). See *Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998).

- Electronic Filers: Comments may be filed electronically using the Internet by accessing ECFS: 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 commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.
 - Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701.
 - U.S. Postal Service first-class, Express, and Priority mail must be addressed to 45 L Street, NE, Washington, DC 20554.
 - Effective March 19, 2020, and until further notice, the Commission no longer accepts any hand or messenger delivered filings. This is a temporary measure taken to help protect the health and safety of individuals, and to mitigate the transmission of COVID-19.¹⁴²

45. *Availability of Documents.* Comments, reply comments, and *ex parte* submissions will be publicly available online via ECFS. These documents will also be available for public inspection during regular business hours in the FCC Reference Information Center, when FCC Headquarters reopens to the public.

46. *People with Disabilities.* To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer and Governmental Affairs Bureau at (202) 418-0530 (voice), (202) 418-0432 (TTY).

47. *Contact Person.* For additional information on this proceeding, contact Connor Ferraro, Wireline Competition Bureau, Competition Policy Division, at Connor.Ferraro@fcc.gov or (202) 418-1322.

¹⁴¹ 47 CFR § 1.49(f).

¹⁴² See *FCC Announces Closure of FCC Headquarters Open Window and Change in Hand-Delivery Policy*, Public Notice, 35 FCC Rcd 2788 (2020), <https://www.fcc.gov/document/fcc-closes-headquarters-open-window-and-changes-hand-delivery-policy>.

V. ORDERING CLAUSE

48. Accordingly, IT IS ORDERED, pursuant to Sections 1, 2(a), 4(i), 227(e), 227b, 251(e) and 403 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 152(a), 154(i), 227(e), 227b, 251(e), and 403, that this Notice of Inquiry IS ADOPTED.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

**STATEMENT OF
CHAIRWOMAN JESSICA ROSENWORCEL**

Re: *Call Authentication Trust Anchor*, WC Docket No. 17-97, Notice of Inquiry (October 27, 2022).

Scam artists are always looking for an angle. Those behind illegal robocalls are no exception. When we shut down one way for them to make these annoying calls, they look for another. So we have to be just as relentless. We need to be just as inventive using the tools we have to bring these junk calls to an end.

Last year, the Federal Communications Commission required that carriers nationwide authenticate all calls using a technology called STIR/SHAKEN. When this network technology is present, consumers can trust that when the phone rings the caller is who they say they are—and not some scam artist with a false number trying to sell you something you did not ask for and do not need. It helps reduce the number of spoofed calls.

But while STIR/SHAKEN has proven effective on networks that rely on Internet Protocol, it does not work in the same way on older parts of our networks with traditional copper lines. That is why we are kicking off this inquiry today. We are not just going to wait for this infrastructure to be updated and eligible for STIR/SHAKEN, we are going to look for ways to combat these calls on the oldest portions of our networks.

In other words, we are going to get creative because this is what we need to do to take on these junk calls. We constantly need to look for new ways to address this problem—and new partners to join us in the fight. To that end, we now have a Memorandum of Understanding with 43 states, plus the District of Columbia and Guam, to share resources and information to crack down on robocalls. These partnerships have already yielded real results. A few months back, we worked with our colleagues in Ohio to target auto warranty robocall scams. Working together, we were able to reduce these calls by 80 percent. We also need to punish the bad actors responsible for these calls, as we did this month when for the first time ever we ordered seven voice providers to shape up or face removal from our Robocall Mitigation Database, which leads to expulsion from America's phone networks.

Like I said at the start, we can't stop because scam artists are always looking for the next opportunity. But I think being relentless also means identifying the loopholes in existing laws that fraudsters can exploit and may need further attention from Congress. That means addressing the definition of autodialer that was narrowed by the Supreme Court last year in a decision involving the Telephone Consumer Protection Act. It means expanding the Commission's ability to track the businesses that entities like these scammers set up to obscure ownership by providing the agency with streamlined authority to access Bank Secrecy Act information. It means making sure that when we issue fines we have a fair shot at collecting them by providing the Commission with the opportunity to pursue these cases in court and not just rely on our colleagues at the Department of Justice to do so.

This continued fight against illegal robocalls wouldn't be possible without the dedicated work of the agency's Robocall Response Team and the individuals behind today's inquiry, including Jerusha Burnett, Aaron Garza, Karen Schroeder, Mark Stone, and Kristi Thornton from the Consumer and Governmental Affairs Bureau; Lisa Gelb, Daniel Stepanicich, Kristi Thompson, and Lisa Zaina from the Enforcement Bureau; Kimberly Cook and Jim Schlichting from the International Bureau; Chuck Needy and Emily Talaga from the Office of Economics and Analytics; Richard Mallen, Linda Oliver, William Richardson, and Derek Yeo from the Office of General Counsel; Ken Carlberg from the Public Safety and Homeland Security Bureau; and Pam Arluk, Allison Baker, Matt Collins, Elizabeth Drogula, Lynne Engledow, CJ Ferraro, Victoria Goldberg, Jesse Goodwin, Trent Harkrader, Zach Ross, Hayley Steffen, Gil Strobel, and David Zesiger from the Wireline Competition Bureau.

**STATEMENT OF
COMMISSIONER GEOFFREY STARKS**

Re: *Call Authentication Trust Anchor*, WC Docket No. 17-97, Notice of Inquiry (October 27, 2022).

I'm glad that today we consider this *Notice of Inquiry* as the next step toward closing critical loopholes in our STIR/SHAKEN call authentication regime. While we are making progress, unwanted and illegal calls continue to be a troublesome burden on the American public. As such, combatting these robocalls remains one of my highest priorities as a Commissioner. To truly make a dent, we must continue to push providers to implement STIR/SHAKEN. The record that develops from this *Notice of Inquiry* will help us chart a path forward on mitigating robocalls on legacy, no-Internet Protocol networks.

The other benefit of this *Notice* is that it can help to facilitate the transition to all-IP networks. The Commission has been working on incentivizing providers to transition their networks to IP for over a decade. I'm hopeful that this *Notice* moves us closer by adding another reason for providers to consider upgrading their networks. I thank the Wireline Competition Bureau staff for their fine work. I approve.