October 31, 2024

FCC FACT SHEET*

Call Authentication Trust Anchor

Report and Order—WC Docket No. 17-97

Background: The STIR/SHAKEN caller ID authentication framework combats unlawfully spoofed robocalls by allowing authenticated caller ID information to securely travel with the call itself throughout the entire call path. While the Commission has worked to steadily expand the scope of providers required to implement STIR/SHAKEN, service providers must do their part to reduce unlawful robocalls on the network. Some providers rely on third parties to fulfill their STIR/SHAKEN implementation obligations. While some stakeholders contend that these third-party practices can yield benefits, others caution they undermine confidence in the STIR/SHAKEN framework through improper attestations of caller ID information and diminished accountability. This *Report and Order*, if adopted, would strengthen the Commission's caller ID authentication requirements by establishing clear rules of the road for the use of third parties in the authentication process and placing limits on third-party authentication to ensure that the party with the implementation obligation under our rules remains responsible and accountable for complying with the requirements of the STIR/SHAKEN standards.

What the *Report and Order* Would Do:

- Define "third-party authentication" to provide a clear scope of the third-party authentication practices authorized and prohibited by the new rules.
- Authorize providers with a STIR/SHAKEN implementation obligation to engage third parties to perform the technological act of digitally "signing" calls consistent with the requirements of the STIR/SHAKEN technical standards, subject to two conditions:
    - (1) The provider with the implementation obligation itself makes the critical "attestation-level" decisions for authenticating caller ID information associated with its calls; and
    - (2) All calls are signed using the certificate of the provider with the implementation obligation—not the certificate of a third party.
- Explicitly require all providers with an implementation obligation to obtain a Service Provider Code (SPC) token from the Policy Administrator and present that token to a STIR/SHAKEN Certificate Authority to obtain a digital certificate.
- Require any provider certifying to partial or complete STIR/SHAKEN implementation in the Robocall Mitigation Database to have obtained an SPC token and digital certificate and sign all its calls with that certificate, either themselves or when working with a third party to perform the technological act of signing calls.
- Adopt recordkeeping requirements for third-party authentication arrangements to monitor compliance with and enforce the Commission's rules.

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

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

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

EIGHTH REPORT AND ORDER*

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

By the Commission:

TABLE OF CONTENTS

I. INTRODUCTION

1. Unwanted and illegal calls continue to plague American consumers.[1] Of these calls,

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

[1] The Commission received approximately 157,000 of such complaints in 2020, 164,000 in 2021, 119,000 in 2022, and 96,000 in 2023. FCC, Consumer Complaint Data Center, https://www.fcc.gov/consumer-help-center-data (last visited Aug. 30, 2023).

illegally spoofed robocalls—wherein scammers falsify caller ID information in an attempt to deceive call recipients into believing they are trustworthy—are particularly harmful.[2] Although efforts by service providers, call blocking and analytics companies, and government agencies at the state and federal level are having a positive impact, much more remains to be done.[3] The Commission has long worked to reduce the harm these unwanted calls pose to the public, and we are committed to continuing this fight, and to marshalling every tool at the Commission's disposal to protect American consumers from the threat posed by illegal robocalls.[4]

2. One of the most significant tools in this effort is the STIR/SHAKEN caller ID authentication framework, which allows service providers to verify that the caller ID information transmitted with a particular call matches the caller's number.[5] As the Commission has found, STIR/SHAKEN provides critical information to service providers and call blocking and labeling applications, and supports law enforcement efforts to stop illegal robocallers.[6] Therefore, over the past four years, the Commission has steadily expanded its STIR/SHAKEN implementation requirements in order to pursue ubiquitous deployment of the framework.[7] To realize the benefits of STIR/SHAKEN, however, providers must do their part. They must properly apply the technical standards that constitute the framework and establish a system of trust and accountability among all providers participating in the STIR/SHAKEN ecosystem.[8]

3. While efforts to expand STIR/SHAKEN implementation have steadily improved in recent years, some providers rely on third parties to fulfill their STIR/SHAKEN implementation obligations under the Commission's rules. These practices range from those in which a provider utilizes a third party to perform certain technological acts under the STIR/SHAKEN standards to those in which a provider relies on a downstream intermediate provider to perform all authentication-related obligations on its behalf.[9] While some stakeholders have argued that third-party arrangements can be beneficial,

---

[2] *See Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, 36 FCC Rcd 1859, 1860, para. 1 (2020) (*Second Caller ID Authentication Report and Order*).

[3] Recent data from YouMail show a nearly 10 percent decline in the number of robocalls received during the first half of 2024 compared to the previous year. However, U.S. consumers continue to receive billions of robocalls a month. *See* Press Release, YouMail, Inc., U.S. Consumers Received Just Over 4.1 Billion Robocalls in June, According to YouMail Robocall Index (July 9, 2024), https://www.prnewswire.com/news-releases/us-consumers-received-just-over-4-1-billion-robocalls-in-june-according-to-youmail-robocall-index-302191518.html.

[4] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1861, para. 3.

[5] *Call Authentication Trust Anchor*, WC Docket No. 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd 2573, 2576, para. 5 (2023) (*Sixth Caller ID Authentication Report and Order* or *Sixth Caller ID Authentication Further Notice*).

[6] *See Advanced Methods to Target and Eliminate Unlawful Robocalls*, *Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Sixth Report and Order in CG Docket No. 17-59, Fifth Report and Order in WC Docket No. 17-97, Order on Reconsideration in WC Docket No. 17-97, Order, Seventh Further Notice of Proposed Rulemaking in CG Docket No. 17-59, Fifth Further Notice of Proposed Rulemaking in WC Docket No. 17-97, 37 FCC Rcd 6865, 6886, para. 51 (2022) (*Gateway Provider Order* or *Fifth Caller ID Authentication Further Notice*).

[7] *See Sixth Caller ID Authentication Report and Order*, 38 FCC Rcd at 2580, paras. 15-16.

[8] *See* FCC, Triennial Report on the Efficacy of the Technologies Used in the STIR/SHAKEN Caller ID Authentication Framework at 3 (2022), https://docs.fcc.gov/public/attachments/DOC-390474A1.pdf (finding that the STIR/SHAKEN framework is effective as designed, but that its benefits depend on providers properly applying the STIR/SHAKEN technical standards); *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1863, para. 8.

[9] *See* North American Numbering Council, Call Authentication Trust Anchor Working Group, Deployment of STIR/SHAKEN by Small Voice Service Providers at 6-8 (2021) (NANC Small Providers Report), https://docs.fcc.gov/public/attachments/DOC-377426A1.pdf; USTelecom Comments, CG Docket No. 17-59, WC

(continued….)

particularly for small providers,[10] others have raised concerns that the involvement of third parties is resulting in improperly authenticated calls and diminished accountability, and thus is undermining confidence in the STIR/SHAKEN framework.[11]

4. In this *Eighth Report and Order*, we continue to strengthen our caller ID authentication requirements by establishing clear rules of the road for the use of third parties in the caller ID authentication process and placing limits to ensure that the party with the implementation obligation under our rules remains responsible and accountable for meeting the requirements of the STIR/SHAKEN standards.[12] By so doing, we allow providers to realize the economic benefits and efficiencies of working with third parties on the technical aspects of STIR/SHAKEN authentication while maintaining the integrity of the framework for the protection of consumers.

II. BACKGROUND

A. The STIR/SHAKEN Caller ID Authentication Framework

5. The STIR/SHAKEN caller ID authentication framework is a set of industry-developed standards and protocols designed to combat unlawfully spoofed robocalls by allowing authenticated caller ID information to securely travel with the call itself throughout the entire call path.[13] Consistent with Congressional direction in the 2019 Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act,[14] the Commission required voice service providers[15] to implement STIR/SHAKEN in the

(Continued from previous page)
Docket No. 17-97, at 10 (rec. Aug. 17, 2022) (USTelecom Aug. 17, 2022 Comments) (raising concern about providers relying on downstream providers to sign the traffic they originate using the downstream provider's token); Comcast Corporation Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 12 (rec. Aug. 17, 2022) (Comcast Aug. 17, 2022 Comments) ("Third party authentication tools are already relatively common in the voice services marketplace."); ZipDX Reply, CG Docket No. 17-59, WC Docket No. 17-97, at 2 (rec. Sept. 19, 2022) (ZipDX Sept. 19, 2022 Reply) (explaining that providers can "can outsource the signing [of calls] to a third party"); TransNexus Comments at 4 (discussing "situation[s] where a downstream transit provider authenticates calls using its own STI certificate and . . . determine[s] the attestation level").

[10] *See* NANC Small Providers Report.

[11] *See, e.g.*, TransNexus Comments, WC Docket No. 17-97, at 2-4 (filed Nov. 12, 2021) (TransNexus Small Provider Extension Comments) (arguing that an intermediate provider's use of an originating service provider's SHAKEN certificate represents "a legitimate outsourcing arrangement" while, conversely, use of an "intermediate provider's SHAKEN certificate" to sign for calls of an upstream provider undermines the STIR/SHAKEN framework).

[12] *See infra* Sections III.A, III.B.

[13] More specifically, the Secure Telephony Identity Revisited (STIR) working group of the Internet Engineering Task Force (IETF) developed several protocols for authenticating caller ID information. *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1862-63, paras. 6-7. The Alliance for Telecommunications Industry Solutions (ATIS), in conjunction with the SIP Forum, produced the Signature-based Handling of Asserted information using toKENs (SHAKEN) specification, which standardizes how the protocols produced by STIR are implemented across the industry. *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1859, 1862-63, para. 7.

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

[15] Because the TRACED Act defines "voice service" in a manner that excludes intermediate providers, our authentication and Robocall Mitigation Database rules use "voice service provider" in this manner. *See* 47 U.S.C. § 227b(a)(2)(A); 47 CFR § 64.6300(o) (defining "voice service" as "any service that is interconnected with the public switched telephone network and that furnishes voice communications to an end-user using resources from the North American Numbering Plan or any successor"). For purposes of this item, we use the term "voice service provider" consistent with the TRACED Act definition. In all other instances, we use "provider" and specify the type
(continued….)

IP portions of their voice networks by June 30, 2021,[16] subject to certain exceptions.[17]

6. The STIR/SHAKEN framework consists of two components: (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.[18] The first component relies on public key cryptography to securely transmit the information that an authenticating 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.[19] This encrypted information is contained in a unique part of the network-level message used to initiate a Session Initiation Protocol (SIP) call, the SIP INVITE.[20] After a provider authenticates the caller ID information for a particular call, it adds this information to the "Identity" header field of the SIP INVITE, which travels along with the call from the authenticating provider, through any intermediate providers, and then to the terminating voice service provider.[21] When the terminating voice service provider receives the call with the Identity header attached, it can decrypt it, and then use that information, along with other information, to protect its subscribers from unwanted and illegal calls.[22]

7. The second component relies on digital certificates issued to a provider through a neutral governance system to maintain trust and accountability among providers.[23] The provider first obtains a Service Provider Code (SPC) token from the STIR/SHAKEN Policy Administrator and then presents that token to a STIR/SHAKEN Certificate Authority to obtain a certificate, 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.[24] Under the STIR/SHAKEN standards, this certificate is used to populate the Identity header with encrypted information which can be decrypted by a downstream provider to verify the identity of the authenticating provider—a process sometimes referred to as "signing" a call.[25] This system is overseen

(Continued from previous page)
of provider as appropriate. Unless otherwise specified, we mean any provider, regardless of its position in the call path.

[16] 47 CFR § 64.6301; *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, 3252, para. 24 (2020) (*First Caller ID Authentication Report and Order* or *First Caller ID Authentication Further Notice*).

[17] 47 CFR §§ 64.6304, 64.6306; *see also Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1876-83, paras. 36-51.

[18] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1862-63, para. 7; *Sixth Caller ID Authentication Report and Order*, 38 FCC Rcd at 2576, para. 5.

[19] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1863, para. 8; *Sixth Caller ID Authentication Report and Order*, 38 FCC Rcd at 2576, para. 5.

[20] *First Caller ID Authentication Report and Order*, 35 FCC Rcd at 3244, para. 6.

[21] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1863, para. 8; *Sixth Caller ID Authentication Report and Order*, 38 FCC Rcd at 2576, para. 5.

[22] *See First Caller ID Authentication Report and Order*, 35 FCC Rcd at 3244-45, para. 6. For example, caller ID authentication information may be incorporated with other analytics to determine whether a call should be blocked under our existing safe harbors for call blocking. *See* 47 CFR § 64.1200(k)(3), (11).

[23] *First Caller ID Authentication Report and Order*, 35 FCC Rcd at 3246, para. 9; *Sixth Caller ID Authentication Report and Order*, 38 FCC Rcd at 2576, para. 6.

[24] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1864, para. 11; *Sixth Caller ID Authentication Report and Order*, 38 FCC Rcd at 2576, para. 6.

[25] *See* ATIS-1000074 at 11-12; *id*. at 3 (defining the "Secure Telephone Identity (STI) Certificate" as a "public key certificate, based on a service provider public and private key pair, used to sign and verify" a Personal Assertion Token (PASSporT)). Under this system, the "authorized owner of the certificate used to generate the signature can
(continued….)

by a Governance Authority—a role filled by an entity called the Secure Telephone Identity Governance Authority[26]—which establishes the policies and procedures regarding how providers may acquire and maintain certificates.[27] The Policy Administrator applies the rules set by the Governance Authority,[28] and third-party Certification Authorities (themselves subject to Policy Administrator approval)[29] issue the digital certificates to providers.[30] 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.

8. Currently, all voice service providers, all gateway providers,[31] and certain non-gateway intermediate providers[32] are required to implement STIR/SHAKEN in the IP portions of their networks

(Continued from previous page)
be validated and traced back to the known trust anchor" and "the associated public certificate is used to verify the digital signature and the claims included in the PASSporT." *Id*. at 6. For the purposes of this item, we use the phrase "the technological act of signing a call" to refer to the process of populating the Identity header with attestation-level information and the certificate of the originating service provider. *Id.* at 10-13; *see also* IETF, Authenticated Identity Management in the Session Initiation Protocol (SIP), RFC 8224 at 13-14, 16 (Dec. 19, 2018), https://www.rfc-editor.org/rfc/pdfrfc/rfc8224.txt.pdf. We make clear that this act does not involve making discretionary choices (e.g., choosing an attestation level).

[26] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1864, para. 11; *see also* Secure Telephone Identity Governance Authority (STI-GA), *STI Governance Authority*, https://sti-ga.atis.org (last visited Aug. 27, 2024).

[27] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1864, para. 11; *Sixth Caller ID Authentication Report and Order*, 38 FCC Rcd at 2576, para. 6.

[28] *First Caller ID Authentication Report and Order*, 35 FCC Rcd at 3246, para. 10. The role of Policy Administrator is currently held by iconectiv. *See* iconectiv, *Industry Players*, https://authenticate.iconectiv.com/industry-players (last visited Aug. 27, 2024).

[29] *See First Caller ID Authentication Report and Order*, 35 FCC Rcd at 3246, para. 10; *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1864, para. 11; *Sixth Caller ID Authentication Report and Order*, 38 FCC Rcd at 2576, para. 6. The Policy Administrator has approved 11 certification authorities. *See* iconectiv, *Approved Certification Authorities*, https://authenticate.iconectiv.com/approved-certification-authorities (last visited Aug. 27, 2024).

[30] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1864, para. 11. Under the current Governance Authority rules, a provider must meet certain requirements to receive a certificate. *See* STI-GA, Policy Decision Binder, Version 6.0 at 6 (May 22, 2024), Policy Decision 001: SPC Token Access Policy Version 1.2 (May 18, 2021), https://cdn.atis.org/sti-ga.atis.org/2024/05/22175841/240522-STIGA-Board-Policy-Decision-Binder-FINAL.pdf. To obtain a token, the Governance Authority policy requires that a provider must "(1) [h]ave a current form 499A on file with the FCC . . . ; (2) [h]ave been assigned an Operating Company Number (OCN) . . . ; [and] (3) [h]ave certified with the FCC that [it] ha[s] implemented STIR/SHAKEN or compl[ies] with the [Commission's] Robocall Mitigation Program requirements and [is] listed in the FCC [Robocall Mitigation Database], or . . . has direct access to telephone numbers from the Toll-Free Number Administrator (TFNA)." *Id*.

[31] In 2022, among other requirements, the Commission required gateway providers to authenticate unauthenticated SIP traffic carrying a U.S. North American Numbering Plan number in the caller ID field by June 30, 2023. *See Gateway Provider Order*, 37 FCC Rcd at 6886-87, para. 51; 47 CFR §§ 6302(c) (requiring gateway providers to "authenticate caller identification information for all calls it receives that use North American Numbering Plan resources that pertain to the United States in the caller ID field and for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call"), 64.6300(d) (defining "gateway provider" as "a U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider" and further defining for the purpose of the rule "U.S.-based" and "receives a call directly").

[32] In 2023, the Commission required a non-gateway intermediate provider to authenticate caller identification information for all SIP calls it receives directly from an originating provider and for which the caller identification information has not been authenticated by December 31, 2023. *See Sixth Caller ID Authentication Report and*
(continued….)

unless subject to an implementation extension.[33] Providers that lack control over the network infrastructure necessary to implement STIR/SHAKEN, such as switches for voice service in the IP portion of their network,[34] are exempt from STIR/SHAKEN implementation requirements.[35] All providers, regardless of whether they are required to implement STIR/SHAKEN and the status of that implementation, are required to file certifications in the Robocall Mitigation Database (Database) stating, among other points, whether they have fully, partially, or not implemented STIR/SHAKEN in their

(Continued from previous page)
Order, 38 FCC Rcd at 2587-88, para. 27; 47 CFR §§ 64.6302(d) (detailing caller ID authentication requirements for non-gateway intermediate providers), 64.6300(i) (defining "non-gateway intermediate provider" as "any entity that is an intermediate provider as that term is defined by paragraph (g) of this section that is not a gateway provider as that term is defined by paragraph (d) of this section"), 64.6300(g) (defining "intermediate provider" as "any entity that carries or processes traffic that traverses or will traverse the public switched telephone network at any point insofar as that entity neither originates nor terminates that traffic"); *see also id.* § 64.6302(a) (requiring intermediate providers to "pass unaltered to the subsequent intermediate provider or voice service provider in the call path any authenticated caller identification information it receives with a SIP call").

[33] Pursuant to the TRACED Act, the Commission has adopted limited extensions to its STIR/SHAKEN implementation requirements. Because STIR/SHAKEN only works on IP-based voice networks, the TRACED Act granted providers that "materially rel[y]" on non-IP infrastructure an ongoing implementation extension. 47 U.S.C. § 227b(b)(5)(B). The Commission has also granted certain limited implementation extensions on the basis of "undue hardship." *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1882-83, paras. 49-50. These extensions are reviewed annually, and the Commission has generally declined to extend them. *Wireline Competition Bureau Performs Required Evaluation Pursuant to Section 64.6304(f) of the Commission's Rules*, WC Docket No. 17-97, Public Notice, 36 FCC Rcd 17748, 17749 (WCB 2021) (*First Reevaluation of STIR/SHAKEN Extensions Public Notice*) (declining to extend the small voice service provider STIR/SHAKEN implementation extension). As of June 30, 2023, the only remaining "undue hardship" extensions are for the few providers that cannot obtain the SPC token required to implement STIR/SHAKEN, and for small voice service providers that originate calls via satellite using U.S. North American Numbering Plan telephone numbers. *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1882-83, paras. 49-50; *Sixth Caller ID Authentication Report and Order*, 38 FCC Rcd at 2612-13, paras. 76-77; *Wireline Competition Bureau Performs Required Evaluation Pursuant to Section 64.6304(f) of the Commission's Rules*, WC Docket No. 17-97, Public Notice, 37 FCC Rcd 14876, 14876 (WCB 2022) (*Second Reevaluation of STIR/SHAKEN Extensions Public Notice*) (noting that the June 30, 2023 expiration of the implementation extension for small voice service providers would constitute "a significant step toward the Commission's goal of achieving ubiquitous STIR/SHAKEN implementation").

[34] *See* ACA Connects Comments at 3-4 (describing the relationship between a wholesaler and "facilities-based small broadband providers," including those "that originated as cable operators and later added voice service to their offerings" wherein the reseller "sells voice service to residences and businesses in the community and supplies the last-mile connection" and the wholesaler controls the infrastructure necessary to implement STIR/SHAKEN because it "manages the voice service and handles core functionalities, including switching and interconnection").

[35] *See First Caller ID Authentication Report and Order*, 35 FCC Rcd at 3260, para. 40 ("Finally, we clarify that the rules we adopt today do not apply to providers that lack the network infrastructure necessary to implement STIR/SHAKEN."). This exemption is distinct from the Commission's continuous extension for non-IP portions of a provider's network. *See Sixth Caller ID Authentication Report and Order*, 38 FCC Rcd at 2584-85, para. 19 ("We therefore decline to impose an authentication obligation on all intermediate providers to address circumstances where a call traverses a non-IP network, but may revisit the subject after the Commission concludes its inquiry into whether non-IP authentication or IP interconnection solutions are feasible and can be timely implemented."). The Commission has launched an inquiry into solutions to enable caller ID authentication over non-IP networks, amongst other issues concerning the IP transition. *See generally Call Authentication Trust Anchor*, WC Docket No. 17-97, Notice of Inquiry, 37 FCC Rcd 13451 (2022) (*Non-IP Caller ID Authentication Notice of Inquiry*). The Commission also recently sought comment on how issues regarding IP interconnection impact other tools that may be used to combat scam calls, including artificial intelligence (AI) technologies used to conduct real-time call monitoring. *See Implications of Artificial Intelligence Technologies on Protecting Consumers from Unwanted Robocalls and Robotexts*, CG Docket No. 23-362, Notice of Proposed Rulemaking and Notice of Inquiry, FCC 24-84, at 15, para. 37 (Aug. 8, 2024).

networks,[36] and if they have not, whether that is because they are exempt from having to do so or subject to an implementation extension under the Commission's rules.[37]

B. The STIR/SHAKEN Technical Standards

9. The technical standards and protocols that comprise STIR/SHAKEN are published on the websites of the independent standards-setting bodies that developed the framework.[38] Of those standards and protocols, the Commission's rules require providers with a STIR/SHAKEN implementation obligation to comply with, *at a minimum*, ATIS-1000074, ATIS-1000080, and ATIS-1000084, and all of the documents referenced therein.[39] These documents, which are periodically amended by the Alliance

[36] *See 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, Notice of Proposed Rulemaking, FCC 24-85, at 5-8, paras. 6-9 (Aug. 7, 2024) (*Robocall Mitigation Database NPRM*). The consequences for failing to file in the Database, or for filing certifications and robocall mitigation plans that do not comply with the Commission's rules are significant, and may include the imposition of a Commission forfeiture and/or the removal of a deficient filing from the Database. *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1903, para. 83; *Gateway Provider Order*, 37 FCC Rcd at 6882, para. 40; *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2603, para. 57. The latter remedy "effectively precludes the provider from operating as a provider of voice services in the United States, as the Commission's rules prohibit intermediate and terminating providers from accepting traffic directly from any provider that does not appear in the Database**.**" *Robocall Mitigation Database NPRM* at 4-5, para. 5; *see also Global UC Inc*, Removal Order, 37 FCC Rcd 13376 (EB 2022) (removing a provider's certification because it included a facially deficient robocall mitigation plan); *TELECLUB fka 2054235 Alberta Ltd.*, Removal Order, DA 24-153 (EB Feb. 22, 2024) (same); *Viettel Business Solutions Company et al.*, Removal Order, DA 24-152 (EB Feb. 22, 2024) (removing 12 providers from the Robocall Mitigation Database because their certifications included facially deficient robocall mitigation plans); *BPO Innovate*, Order, DA 24-283 (EB Mar. 27, 2024) (removing a provider's certification because of two deficiencies, including a facially deficient robocall mitigation plan).

[37] *Sixth Caller ID Authentication Report and Order*, 38 FCC Rcd at 2596-97, para. 45 (stating that a filer asserting it does not have an obligation to implement STIR/SHAKEN because of an ongoing extension, or because it lacks control over the network infrastructure necessary to implement STIR/SHAKEN, must both explicitly state the rule that exempts it from compliance and explain in detail why that exemption applies to the filer). All providers are also required to adopt robocall mitigation programs that comply with the Commission's rules and submit written descriptions of those programs in the Robocall Mitigation Database. *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1902, para. 82 (requiring voice service providers to file, and those that did not fully implement STIR/SHAKEN to submit a robocall mitigation plan by June 20, 2021); *Gateway Provider Order*, 37 FCC Rcd at 6880, para. 34 (requiring gateway providers to file and submit a robocall mitigation plan); *Sixth Caller ID Authentication Report and Order*, 38 FCC Rcd at 2588, para. 28 (requiring all voice service providers and intermediate providers to file and submit a robocall mitigation plan); *Wireline Competition Bureau Announces Robocall Mitigation Database Filing Deadlines and Instructions and Additional Compliance Dates*, WC Docket No. 17-97, Public Notice, DA 24-73 at 1 (WCB Jan. 25, 2024) (*Robocall Mitigation Database Filing Deadline Public Notice*); 47 CFR §§ 64.6304, 64.6305.

[38] *See* SIP Forum, *IP-NNI Task Force Introduction*, https://www.sipforum.org/activities/nni-task-force-introduction/#about-nni-tf (last visited Aug. 27, 2024); IETF Datatracker, *Secure Telephone Identity Revisited (stir)*, https://datatracker.ietf.org/group/stir/about (last visited Aug. 27, 2024); ATIS, *Public Documents*, https://access.atis.org/higherlogic/ws/public/documents?view= (last visited Aug. 27, 2024).

[39] *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3258-59, para. 36; *see also Sixth Caller ID Authentication Report and Order*, 38 FCC Rcd at 2586, para 22; *Gateway Provider Order*, 37 FCC Rcd at 6887-88, para. 53. Prior and current versions of the standards are available on the ATIS website. *See, e.g.*, ATIS & SIP Forum, Signature-based Handling of Asserted information using toKENs (SHAKEN), ATIS-1000074.v003 (2022), https://access.atis.org/higherlogic/ws/public/download/67436/ATIS-1000074.v003.pdf/latestATIS-1000074 (ATIS-1000074); ATIS, Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management, ATIS-1000080.v005 (2022), https://access.atis.org/apps/group_public/download.php/69428/ATIS-1000080.v005.pdf (ATIS-1000080); ATIS & SIP Forum, Technical Report on Operational and Management Considerations for SHAKEN STI Certification

(continued….)

for Telecommunications Industry Solutions (ATIS),[40] establish both the technical requirements for authenticating calls and the governance system underlying the STIR/SHAKEN framework.[41]

10. Consistent with these standards, providers can authenticate caller ID information with one of three attestation levels: A-level, B-level, or C-level attestation.[42] Pursuant to ATIS-1000074, an A-level, or "full," attestation signifies the highest level of trust, and requires the authenticating provider to demonstrate that it: (1) is responsible for the origination of the call onto the network; (2) "[h]as a direct authenticated relationship with the customer and can identify the customer"; and (3) "[h]as established a verified association with the telephone number used for the call."[43] A B-level, or "partial," attestation requires the authenticating provider to meet only the first two requirements of A-level attestation. Therefore, a provider can apply a B-level attestation where it has originated the call and has a direct authenticated relationship with the customer but has not established a verified association with the telephone number appearing in the caller ID field.[44] Finally, C-level, or "gateway," attestation requires only that the authenticating provider both be "the entry point of the call into its VoIP network" and have "no relationship with the initiator of the call," as is typically the case for gateway providers processing traffic originated abroad.[45]

(Continued from previous page)
Authorities and Policy Administrators, ATIS-1000084.v002 (2020), https://access.atis.org/apps/group_public/download.php/55473/ATIS-1000084.v002.pdf (ATIS-1000084).

[40] Providers are required to comply with the versions of those standards that were in effect at the time of their respective compliance deadlines, including any errata as of those dates or earlier. *First Caller ID Authentication Report and Order*, 35 FCC Rcd at 3258-59, para. 36; *Gateway Provider Order*, 37 FCC Rcd at 6887-88, para. 53; *Sixth Caller ID Authentication Report and Order*, 38 FCC Rcd at 2585-56, para. 21. Requirements in the standards and protocols referenced in this *Eighth Report and Order* have not materially changed since the first STIR/SHAKEN implementation obligation went into effect in June 2021. *Compare* ATIS, Signature-based Handling of Asserted information using toKENs (SHAKEN), ATIS-10000074-E19E (2019), ATIS, Errata to Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management, ATIS-1000080-E19 (2019), *and* ATIS, Errata to Technical Report on Operational and Management Considerations for SHAKEN STI Certification Authorities and Policy Administrators, ATIS-1000084-E19 (2019), *with* ATIS-1000074, ATIS-1000080, *and* ATIS-1000084. For ease of reference, we cite herein to the current version of the standards and protocols. *See supra* note 39.

[41] ATIS-1000074 "defines the framework for telephone service providers to create signatures in [SIP] and validate initiators of signatures" as well as "the various classes of signers and how the verification of a signature can be used towards the mitigation and identification of illegitimate use of national telecommunications infrastructure." ATIS-1000074 at 1. ATIS-1000080 and 1000084 focus on various operational and governance concerns related to the issuance and management of certificates. *See* ATIS-1000080 at 1; ATIS-1000084 at 1.

[42] ATIS-1000074 at 12-13.

[43] *Id.* at 12 (noting that establishing a verified association with the telephone number used for the call requires "[t]he service provider . . . [to] assert[] that their customer can 'legitimately' use the [telephone number] that appears as the calling party (i.e., the Caller ID)" and providing examples of how the service provider can do so); Lingo Telecom, LLC, File No. EB-TCD-24-00036425, Notice of Apparent Liability for Forfeiture, FCC 24-60, at 10-11, para. 19 (May 28, 2024) (*Lingo Telecom NAL*) (describing calls signed by Lingo with A-Level attestations and proposing a penalty of $2,000,000 for apparent violations of section 64.6301(a) of the Commission's rules); *see also* Lingo Telecom, LLC, File No. EB-TCD-24-00036425, Order, DA 24-790 (EB Aug. 21, 2024) (*Lingo Consent Decree*).

[44] ATIS-1000074 at 12 (stating that partial attestation requires "the signing service provider [to] attest[] that it can trace the origination of the call to a customer for traceback or policy enforcement purposes").

[45] *Id.* at 13 ("The [signing] service provider should be able to trace a call to an interconnecting service provider and/or peer node for traceback or policy enforcement purposes. Gateway attestation may also be used when the STI-AS does not have sufficient information for determining that an 'A' or 'B' attestation level applies even when the call was received at a customer interface.").

11. In addition to the three "core" standards documents referenced above, ATIS has also published a number of other documents related to the STIR/SHAKEN call authentication framework. For example, ATIS-1000088 is a Technical Report that is listed as an "informative reference" in the current version of ATIS-1000074.[46] ATIS-1000088 defines several terms used in ATIS-1000074 and provides guidance on how providers may authenticate calls, consistent with the standards, in more complex call paths in which an authenticating service provider's customer is not the ultimate end user of a voice service, such as where an originating service provider authenticates calls initiated by a reseller that itself maintains a direct relationship with the calling party.[47]

C. Third-Party Authentication and the Fifth and Sixth Further Notices of Proposed Rulemaking

12. The Commission's rules do not currently address providers with a STIR/SHAKEN implementation obligation using a third-party authentication solution. In 2021, the North American Numbering Council's (NANC) Call Authentication Trust Anchor Working Group submitted the 2021 Small Providers Report, which detailed small voice service provider's deployment of STIR/SHAKEN throughout their networks.[48] In that report, the NANC explained that small providers could reduce their costs of authenticating SIP traffic by leveraging authentication solutions offered by third parties.[49] In so doing, the Small Providers Report described three categories of solutions: (1) Hosted SHAKEN;[50] (2) Carrier SHAKEN;[51] and (3) SHAKEN Software.[52] The report describes "SHAKEN Software" as commercially licensed software solutions deployed by an originating service provider or terminating service provider in its networks to perform caller ID authentication.[53] Providers using a SHAKEN Software solution perform all acts to authenticate caller ID information themselves. Hosted SHAKEN and Carrier SHAKEN, however, each involve a third-party performing the technological act of signing a call. More specifically, as described by the NANC, Hosted SHAKEN is "a turn-key SHAKEN authentication and verification solution offered in a public or private cloud that includes all the required SHAKEN components for offering a comprehensive standards-compliant solution[.]"[54] According to the NANC, Hosted SHAKEN can offer value-added features,[55] and providers also have flexibility in how they integrate the solution into their network infrastructure using either HTTP or SIP protocols.[56] The NANC describes Carrier SHAKEN as "another category of turn-key SHAKEN services offered by a growing number of Direct Inward Dialing (DID) or wholesale providers that also provide SIP termination to the PSTN" that "combines SHAKEN authentication service with SIP termination to the PSTN (transit

[46] *Id.* at 2.

[47] ATIS & SIP Forum, A Framework for SHAKEN Attestation and Origination Identified, ATIS-1000088 (2020), https://access.atis.org/higherlogic/ws/public/download/51435/ATIS-1000088.pdf (ATIS-1000088 or "ATIS-1000088 Technical Report"). ATIS-1000088 has not been revised since the first STIR/SHAKEN implementation obligation went into effect in June 2021.

[48] NANC Small Providers Report.

[49] *Id.* at 6.

[50] *Id.* at 7.

[51] *Id.* at 7-8.

[52] *Id.* at 8.

[53] *Id.* These commercially available SHAKEN Software solutions are deployed in a provider's data centers. *Id.*

[54] *Id.* at 7.

[55] *Id.* (providing "call analytics, call treatment, call blocking or diversion along with other consumer enabling features" as examples for value-added features).

[56] *Id.* (including a diagram that provides an example of how a provider might integrate a Hosted SHAKEN solution into its network using SIP protocol).

service)."[57] While these solutions allow a third party to handle the technological act of signing a call, as described by the NANC Small Providers Report, for both Hosted SHAKEN and Carrier SHAKEN: (1) the originating service provider determines the correct attestation level for a call; and (2) the third party signs the call using the originating provider's SPC token.[58]

13. Following the 2021 Small Providers Report, the Commission adopted the *Fifth Caller ID Authentication Further Notice* in May 2022, which, among other things, sought comment on STIR/SHAKEN authentication by third parties.[59] In particular, the Commission asked whether it should allow third-party authentication to meet the originating service provider's STIR/SHAKEN implementation obligation, whether to require all domestic providers to authenticate caller ID information using their own SPC tokens, under what circumstances third-party authentication is appropriate or improper, and whether third-party authentication undercuts the STIR/SHAKEN framework.[60] The resulting record confirmed that third-party authentication is occurring, but is insufficient to understand the full scope of practices being used, whether such practices comply with the Commission's rules, and their impact on the STIR/SHAKEN ecosystem. In particular, while some commenters suggested that explicitly authorizing third-party authentication would benefit the STIR/SHAKEN ecosystem by expanding access to the framework, lowering implementation costs, and improving trust and accountability amongst parties with a STIR/SHAKEN implementation obligation,[61] others cautioned that some third-party authentication arrangements undermine STIR/SHAKEN.[62] Consequently, the Commission released the *Sixth Caller ID Authentication Further Notice* to seek further, focused comment on the types of third-party authentication solutions providers are using, how third-party authentication impacts attestation level determinations under the ATIS standards, the benefits and pitfalls of third-party authentication, and whether the Commission should explicitly authorize, prohibit, or limit third-party authentication to ensure the

[57] *Id.* at 7-8 (describing a use case of how a provider may use a Hosted Shaken solution).

[58] *Id.*

[59] *Fifth Caller ID Authentication Further Notice*, 37 FCC Rcd at 6927-6951, paras. 157-225.

[60] *Id.* at 6951, para. 224.

[61] *See, e.g.*, ACA Connects Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 3-4 (rec. Aug. 17, 2022) (ACA Connects Aug. 17, 2022 Comments) (arguing that arrangements with wholesalers "ha[ve] proven to be a cost-effective way for small, facilities-based broadband providers to add voice service to their lineup" and that resellers, particularly small resellers, partnering with wholesalers has "allow[ed] these companies and their customers to enjoy the benefits of call authentication" two years before the implementation deadline for small voice service providers); Comcast Aug. 17, 2022 Comments at 12 (arguing that having providers obtain their own token and sign calls with their digital certificate when using a Hosted SHAKEN solution "appropriately incentivizes providers that can obtain a token to do so and thereby increases transparency and improves the traceback process"); INCOMPAS Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 17-18 (rec. Aug. 17, 2022) (INCOMPAS Aug. 17, 2022 Comments) ("For those that cannot maintain the framework natively, third party authentication has been a way for these providers to adequately meet the Commission's current requirements to transmit authenticated caller ID information to the next voice service provider."); RingCentral Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 10-11 (rec. Aug. 17, 2022) (RingCentral Aug. 17, 2022 Comments) (asserting that "[t]hird-party authentication is critical to innovation and competition[]" because it "removes barriers to entry and enables integration of communications into a wide variety of services and applications").

[62] *See, e.g.*, TransNexus Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 1-4 (rec. Aug. 17, 2022) (TransNexus Aug. 17, 2022 Comments) (arguing that improper third-party signing practices "undermin[e] the accountability designed into the STIR/SHAKEN framework" and "efforts to protect consumers from illegal calls"); USTelecom Aug. 17, 2022 Comments at 10 (asserting that improper third-party attestation practices "undermine the accountability the STIR/SHAKEN framework is intended to impose" and "water down the reliability of attestation levels, thereby also reducing the potential analytical value of authentication information across the ecosystem."); ZipDX Comments, CG Docket No. 17-59, WC Docket No. 17-97, at 15-16 (rec. Aug. 17, 2022) (ZipDX Aug. 17, 2022 Comments) (arguing that the practice of signing calls without the originating provider's token is harmful because then "providers cannot be identified and held accountable for their calls").

reliability of the STIR/SHAKEN framework.[63]

III. DISCUSSION

14. In this *Report and Order*, we take a number of steps to support the STIR/SHAKEN framework and promote trust in our country's voice networks. We do so by authorizing providers with a STIR/SHAKEN implementation obligation[64] to work with third parties to perform the technological act of signing calls to fulfill their compliance obligations under the Commission's rules, but establishing clear limits to ensure that such third-party arrangements neither undermine adherence to the requirements of the STIR/SHAKEN technical standards nor allow providers to avoid accountability for noncompliance. First, we define "third-party authentication" for the purposes of the rules we adopt today. Next, we limit the third-party authentication arrangements authorized under the Commission's rules to those in which the provider with the STIR/SHAKEN implementation obligation: (1) makes all attestation level decisions, consistent with the STIR/SHAKEN technical standards; and (2) ensures that all calls are signed using its own certificate obtained from a STIR/SHAKEN Certificate Authority—not the certificate of a third party. Utilizing a third party to sign traffic without complying with the requirements we adopt today will constitute a violation of the Commission's caller ID authentication rules. We further require that any provider certifying to partial or complete STIR/SHAKEN implementation in the Robocall Mitigation Database must be registered with the STIR/SHAKEN Policy Administrator, obtain its own SPC token from the Policy Administrator, use that token to generate a certificate with the Certificate Authority, and authenticate all its calls with that certificate, whether directly or through a third party. We also adopt recordkeeping requirements regarding third-party authentication arrangements to ensure compliance with the rules we adopt today and promote accountability in the event that any such arrangement leads to abuse of the voice network. Based on our review of the record, we find that taking these steps will enable providers to obtain the economic and other benefits of utilizing third-party technical solutions for STIR/SHAKEN implementation without compromising the integrity of the STIR/SHAKEN technical standards and governance model. This, in turn, will protect consumers by promoting more ubiquitous and accurate caller ID authentication.

A. Authorizing Third-Party Authentication Subject to Limitations to Prevent Abuse

1. Defining the Scope of Third-Party Authentication

15. We first define "third-party authentication" for the purposes of the rules we adopt today, and also delineate the types of providers that are covered by the rules. In the *Sixth Caller ID Authentication Further Notice*, we sought comment on the types of third-party arrangements being used by providers, including whether providers are entering into agreements with third parties to perform all or part of their authentication responsibilities.[65] We sought specific comment on the solutions detailed in the 2021 Small Providers Report produced by the NANC, which described third-party solutions that providers could engage to perform the technological act of signing calls, including "hosted SHAKEN" services offered in a public or private cloud and "carrier SHAKEN" services in which calls are signed by an intermediate provider.[66] As described in the NANC Report, in both of these scenarios, the provider

[63] *Sixth Caller ID Authentication Further Notice*, 38 FCC Rcd at 2619-23, paras. 97-106.

[64] By "STIR/SHAKEN implementation obligation," we mean the applicable requirement under the Commission's rules that a provider implement STIR/SHAKEN in the IP portions of their networks by a date certain, subject to certain exceptions. *Id.* at 2592, para. 36 n.137 (citing 47 CFR §§ 64.6301, 64.6302). When referencing those providers "without" a STIR/SHAKEN implementation obligation, we mean those providers that are subject to an implementation extension, such as a provider with an entirely non-IP network or one that is unable to obtain the necessary SPC token to authenticate caller ID information, or that are exempted from our caller ID authentication requirements because they lack control over the network infrastructure necessary to implement STIR/SHAKEN. *Id.* (citing 47 CFR § 64.6304; *First Caller ID Authentication Report and Order*, 35 FCC Rcd at 3260, para. 40).

[65] *Id.* at 2619, paras. 98-106.

[66] *Id.* at 2621, para. 101; *see* NANC Small Providers Report at 7-8.

with the STIR/SHAKEN implementation obligation determines the appropriate attestation level for a call and the third-party solution signs the call using the obligated provider's token.[67] We also sought comment on several scenarios addressed in the ATIS-1000088 Technical Report in which a provider with a STIR/SHAKEN implementation obligation lacks a direct relationship with the end user of the voice service.[68] These scenarios involve circumstances where the end user of the voice service is not the same as the "customer," as defined by the ATIS -1000088 Technical Report,[69] such as when a wholesale provider originates a call onto the public network for its reseller customer that initiated the call on behalf of an end user.[70] We additionally sought comment on whether we should limit any rule authorizing third-party authentication to the scenarios discussed by the Small Providers Report or those in the ATIS-1000088 Technical Report, or take a broader approach.[71]

16. Based on our review of the record, and for the purposes of the rules we adopt today, we define "third-party authentication" to refer to scenarios in which a provider with a STIR/SHAKEN implementation obligation under the Commission's rules enters into an agreement with another party—a "third party"—to perform the technological act of signing calls on the provider's behalf. This definition of third-party authentication includes, for example, the "hosted SHAKEN" and "carrier SHAKEN" solutions that are described in the Small Providers Report.[72] It excludes instances in which a provider with a STIR/SHAKEN implementation obligation authenticates its own traffic, and simply has a customer that is not the end user that initiated the call.[73] We find that this definition is consistent with the caller ID authentication roles defined by the Commission's rules and the ATIS standards, and will establish a clear scope for the third-party authentication practices we authorize herein.

17. The Commission's rules establish three categories of providers with STIR/SHAKEN implementation obligations: (1) voice service providers that originate calls;[74] (2) non-gateway

[67] *See id.*

[68] *Sixth Caller ID Authentication Further Notice*, 38 FCC Rcd at 2619-20, para. 98 & n.337.

[69] ATIS-1000088 defines "customer" as "[t]ypically a service provider's subscriber, which may or may not be the ultimate end-user of the telecommunications service." ATIS-1000088 at 10. Under this definition, a customer "may be a person, enterprise, reseller, or value-added service provider." *Id.* at 5.

[70] An "end-user" is defined as "[t]he entity ultimately consuming the VoIP-based telecommunications service," which may be "the direct customer of [an originating] service provider or may indirectly use the VoIP-based telecommunications service through another entity such as a reseller or value-added service provider." *Id.* ATIS-1000088, therefore, makes clear that, in some cases, the "customer" and "end user" are not the same. *Id.* at 10-11 ("[I]n a number of cases the end user is not the same entity as the 'customer,' so the customer identity is not directly tied to the end user. In these cases an end user identity is not needed for . . . authentication procedures . . . . As might be required in certain attestation scenarios, there may be a need for the [service provider] to establish (directly or indirectly through the customer) that the customer . . . is servicing a particular end user entity for [telephone number] authorization purposes."); *id*. at 5 (defining "customer" as "[t]ypically a service provider's subscriber, which may or not be the ultimate end-user of the telecommunications service," and which "may be a person, enterprise, reseller, or value added service provider;" and defining "end user" as "[t]he entity ultimately consuming the VoIP-based telecommunications service"); *see also* ATIS-1000074 at 12 (stating that, for full attestation, the "signing service provider is asserting that their customer can 'legitimately' use the [telephone number] that appears as the calling party (i.e., the Caller ID)" and that determining the "legitimacy of the [telephone numbers] the originator of the call can use is subject to signer-specific policy").

[71] *Sixth Caller ID Authentication Further Notice*, 38 FCC Rcd at 2622, para. 103.

[72] *See supra* para. 12 (describing these solutions in greater detail).

[73] *See supra* note 70.

[74] 47 CFR § 64.6301(a)(1)-(2); *see also id*. § 64.6305(d)(4)(vi) (requiring voice service providers to state whether they directly serve end users, serve as wholesale providers originating calls on behalf of another provider or providers, or lack a STIR/SHAKEN implementation obligation).

intermediate providers that carry or process the calls without originating or terminating them;[75] and (3) gateway providers that receive calls from foreign originating or intermediate providers at their US facilities and transmit them downstream.[76] The Commission's rules further state that the STIR/SHAKEN implementation obligation applies to providers with control over the network infrastructure necessary to implement STIR/SHAKEN.[77] Providers that meet these criteria are obligated to implement STIR/SHAKEN and are thus the entities that would be the "first parties" in any third-party authentication arrangement authorized by our rules, i.e., they are the parties with the ultimate compliance obligation. That compliance obligation does not change simply because the provider has an upstream customer (e.g., a reseller or a value-added service provider) that is not the ultimate end user of the voice service and does not itself have a STIR/SHAKEN implementation obligation, e.g., a reseller that qualifies for the STIR/SHAKEN exemption or a value-added service provider (VASP)[78] that provides communications services that are ancillary to the voice service.[79] For instance, in the context of voice service providers,[80] we agree with CCA that "[w]here, consistent with ATIS standards, an originating service provider provides an attestation for calls from its own reseller or [VASP] customer, it is not engaging in third party authentication[; i]t is instead using its certificate to provide an appropriate attestation to traffic from its own customers."[81] Stated differently, the originating service provider in that example is performing its

[75] *Id.* § 64.6302(d).

[76] *Id.* § 64.6302(c).

[77] *See First Caller ID Authentication Report and Order*, 35 FCC Rcd at 3260, para. 40 ("Finally, we clarify that the rules we adopt today do not apply to providers that lack the network infrastructure necessary to implement STIR/SHAKEN.").

[78] A VASP may provide services such as arranging for telephone number assignments from a service provider to a particular customer of the VASP or for the VASP's use irrespective of customer. ATIS-1000088, Appx. A at 18. As is often true with respect to resellers, an "originating [service provider] typically knows the VASP customer and does not have direct knowledge" of the VASP's end users. *Id.*

[79] In these scenarios, the Technical Report provides guidance on the steps a provider with STIR/SHAKEN implementation obligation must take to verify its customer's identity and right to use a number, as required to provide an A- or B-level attestation. *Id.* at 13 ("Where the originating [service provider] has assigned the calling [telephone number] or the customer has provided evidence that it has authorization to use the calling [telephone number] itself, the originating [service provider] can mark an 'A' attestation without reference to authorizations of any indirect end users (e.g., in a reseller or VASP scenario)."), Appx. A at 18-19 (discussing various ways originating service providers can meet their due diligence obligations to establish their customer's right to use a telephone number); *see also id.*, Appx. A at 18 (providing use cases for resellers and value added service providers and explaining that "[i]n most reseller use cases, an originating [service provider] does not know the identity of the ultimate end users and only identifies and authenticates the reseller customer[,]" and "[a]s with reseller scenarios, the originating [service provider] typically knows the [value added service provider] customer and does not have direct knowledge of users of the [value added service provider] call centers or platforms. Any determination of the identity of end-users and their [telephone number] authorizations would need to be traced through the [value added service provider]").

[80] Our framework authorizes all providers with a STIR/SHAKEN implementation obligation, regardless of their position in the call path, and subject to the limitations we set in place, to engage a third party for the technological act of signing calls. Therefore, where an intermediate provider (either a non-gateway intermediate provider or gateway provider) has a STIR/SHAKEN implementation obligation, it may fulfill that obligation through a third party subject to these same rules.

[81] CCA Comments at 1-2; *see also* ACA Connects Comments at 3-5 (requesting that we exclude from our consideration arrangements in which "voice resellers . . . receive call authentication from a third party" such as a wholesale provider); NCTA Comments at 1; *see also* ATIS-1000088 at 9-11 (explaining that an originating service provider's customer may or may not be the ultimate source of the call, or "the end-user entity," and that where it is not, "an end user identity is not needed for [user-to-network interface (UNI)] authentication procedures (only the originating [service provider's] customer needs to be identified as the principal gaining access to the [service provider's] resources)," though "in certain attestation scenarios, there may be a need for the [service provider] to

(continued….)

own STIR/SHAKEN implementation obligation and is not acting as a third party for its upstream customer.[82]

18. We find that any other interpretation would be inconsistent with the requirements for making attestation-level decisions when authenticating calls in the ATIS standards and reference documents. ATIS-1000074 only permits A- and B-level attestations to be made by providers that originate calls onto the IP-based service provider network.[83] Although not defined in ATIS-1000074, that standard uses the term originating service provider, or OSP, consistent with related standards documents, such as ATIS-1000089, which defines originating service provider as: "[t]he service provider that handles the outgoing calls from a customer *at the point at which they are entering the public network*. The OSP performs the SHAKEN Authentication function."[84] Thus, when an originating service provider authenticates a call based on what it knows about its customer and its customer's right to use a telephone number, it is performing its own STIR/SHAKEN implementation obligation, not that of its upstream customer in a third-party capacity.[85] In these circumstances, it is the responsibility of the originating

(Continued from previous page)
establish (directly or indirectly) that the customer UNI is servicing a particular end user entity for [telephone number] authorization purposes").

[82] Thus, if a wholesale provider originates a call onto the public network on behalf of a reseller customer that lacks control over the network infrastructure necessary to implement STIR/SHAKEN, it is the wholesale provider that has the STIR/SHAKEN implementation obligation, not the reseller. *See* ACA Connects Comments at 2, 4; CCA Comments at 4. In this scenario, the wholesale provider is obligated to use STIR/SHAKEN to authenticate the caller ID pursuant to its own obligation under the Commission's rules, not as a third party for the reseller that is exempt from STIR/SHAKEN implementation requirements. *See* ATIS-1000088, Appx. A at 18 (providing STIR/SHAKEN authentication use cases involving resellers and value added service providers and explaining that "[i]n most reseller use cases, an originating [service provider] does not know the identity of the ultimate end users and only identifies and authenticates the reseller customer").

[83] ATIS-1000074 at 12-13.

[84] ATIS-1000089 at 4 (emphasis added); *id*. (noting that the "OSP may also serve in the role as [Telephone Number Service Provider], Resp Org, [a reseller of telephone numbers to other entities], and other roles").

[85] USTelecom, CTIA, and Numeracle urge us to adopt a definition of the term "customer" that is narrower than the one employed by the ATIS standards and reference documents. Specifically, they ask that we define "customer" to mean solely the end user that initiated the voice service, whether an individual or organizational entity. *See* USTelecom Comments at 3; CTIA Reply at 10; Numeracle Comments at 9. We decline to do so at this time because it is not necessary for the purposes of the third-party authentication rules we adopt today. We make clear above that the "first party" within any third-party arrangement is the entity with a STIR/SHAKEN implementation obligation, which under our existing rules and precedent, will necessarily be a voice service provider, intermediate provider, or gateway provider with control over the network infrastructure necessary to implement STIR/SHAKEN. As explained herein, whether the provider's customer is the ultimate end user of the voice service or another upstream entity is not dispositive of whether the provider has a STIR/SHAKEN implementation obligation and whether it may enter into an agreement with a third-party to perform the technological act of signing calls in fulfillment of that obligation subject to the requirements we adopt today. Further, we agree with NCTA, CCA, INCOMPAS, and ACA Connects that narrowing the definition of "customer" to mean solely the entity that initiates the voice service would be a significant departure from a plain reading of the ATIS standards and reference documents, ATIS-1000088 at 5 (defining "customer"); *id.* at 13, and could be disruptive to the use cases that those standards and reference documents clearly contemplate as functioning within the STIR/SHAKEN ecosystem. NCTA Reply at 2-3 (agreeing that narrowing the definition of "customer" to mean "end user" would "conflict[] with ATIS standards, which acknowledge that an originating service provider's customer may be another provider, such as a reseller or a [VASP]. . . . [The Commission] should not interfere now and permit the parties seeking this change to end-run this well-functioning standards development process"); CCA Comments at 3 (contending that a "service provider may be considered an originating service provider . . . for customers that include other types of service providers such as resellers or [VASPs] that subscribe directly to the OSP's services"); INCOMPAS Comments at 13-14 (noting that a variety of "business models and enterprise calling use cases . . . rely on the current interpretation of the standard, [such as] over-the-top hosted or cloud service providers"); ACA Connects Comments at 2 (arguing (continued….)

service provider to utilize reasonable "Know Your Customer" (KYC) protocols to establish a credible evidentiary basis for a "direct authenticated relationship with [its] customer" and/or verification of its customer's right to use the telephone number appearing in the caller ID field, sufficient to apply an A- or B-level attestation under the ATIS standards.[86]

19. We thus decline ZipDX's suggestion that we incorporate providers that lack control over the network infrastructure necessary to implement STIR/SHAKEN as first parties under this framework when they "hold [themselves] out as the originating service provider (even though [they] do[] not actually 'touch' the call)" and "arrange for somebody (the infamous third party) to sign the calls" for them.[87] For the reasons discussed above, such a fluid conception of "originating service provider" would conflict with the text of the Commission's rules establishing the scope of providers subject to a STIR/SHAKEN implementation obligation and would be inconsistent with how the ATIS standards and technical reports use that term.[88]

2. Authorized Third-Party Authentication Practices

20. We next authorize providers with a STIR/SHAKEN implementation obligation to enlist the help of a third-party subject to certain conditions. In the *Sixth Caller ID Authentication Further Notice*, we sought comment on whether we should amend the Commission's rules to explicitly authorize third-party authentication and what, if any, limitations we should place on that authorization to ensure compliance with authentication requirements and the reliability of the STIR/SHAKEN framework.[89]

(Continued from previous page)
that "disrupt[ing] these arrangements[] . . . would be taking a step backward in [our] efforts to promote ubiquitous access to STIR/SHAKEN").

[86] ATIS 1000074 at 12; 47 CFR § 64.1200(n)(4) (requiring voice service providers to "take affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence"); *see also Lingo Telecom NAL* at 12, para. 25 (proposing a penalty of $2,000,000 for apparent violations of section 64.6301(a) of the Commission's rules).

[87] ZipDX Comments at 3. We similarly reject other commenters' understanding of "third-party authentication" that describe scenarios in which a provider without a STIR/SHAKEN implementation obligation, such as a provider that lacks control over the network infrastructure necessary to implement STIR/SHAKEN, would be considered the "first party." *See, e.g.*, INCOMPAS Comments at 7 (labeling a provider that signs calls on behalf of a provider "that [is] unable to obtain a[n] SPC token" a third party); ACA Connects Comments at 2.

[88] *See, e.g.*, ATIS-1000089 at 4 (defining "Originating Service Provider" as "[t]he service provider that handles the outgoing calls from a customer at the point at which they are entering the public network. The OSP performs the SHAKEN Authentication function"). We understand that there are currently voice service resellers that are voluntarily attempting to authenticate caller ID information despite not having control over the network infrastructure necessary to implement STIR/SHAKEN and, thus, lacking a STIR/SHAKEN implementation obligation under the Commission's rules. *See* ACA Connects Comments at 3. We understand that they often do so by relying on their wholesale providers to sign their calls. *See id.* at 3-4. As explained above, such arrangements do not fall within the definition of third-party authentication that we adopt today, except insofar as the wholesale provider with the STIR/SHAKEN implementation obligation opts to use a third party to perform the technological act of signing calls on its behalf. We nevertheless encourage voice service resellers engaged in any form of authentication arrangement with wholesalers to provide such wholesalers with enough information to enable them to determine the appropriate attestation level of the calls initiated by the resellers' end users, pursuant to the wholesaler's obligations under the Commission's rules and the STIR/SHAKEN standards. *See* ATIS-1000088 at 13 ("In those cases [in which a service provider's (SP) customer is a reseller,] the SP's customer should provide assurances that they can trace the identity of an indirect end user and that user's authorization to utilize a calling TN. The customer should be able to certify that only the authorized party (or calls originated on their behalf) will use the particular set of authorized TNs, and any traceback to the ultimate source will rely on the cooperation of the SP's customer."); *see also* ATIS-1000074 at 12 n.1 (describing various mechanisms by which an originating service provider may assert that its customer can legitimately use the telephone number that appears as the calling party).

[89] *Sixth Caller ID Authentication Further Notice*, 38 FCC Rcd at 2622, para. 103.

Based on the evidence in the record, we permit providers with a STIR/SHAKEN implementation obligation under the Commission's rules to engage third parties to perform the technological act of signing calls as required by the STIR/SHAKEN standards,[90] subject to two conditions: (1) the provider with the implementation obligation must make all attestation-level decisions, consistent with the requirements of the technical standards; and (2) all calls must be signed using the certificate of the provider with the implementation obligation. Relying on third parties to sign traffic without complying with these requirements will constitute a violation of the Commission's caller ID authentication rules. As explained below, we find that this approach will ensure the accountability necessary to maintain trust in the STIR/SHAKEN framework and will promote accurate and reliable A- and B-level attestations.

21. Commenters broadly agree that there are benefits to third-party authentication. Numeracle notes that third-party authentication is "necessary and beneficial for the timely and efficient implementation of STIR/SHAKEN."[91] INCOMPAS adds that, "[e]ngaging in third-party caller ID authentication benefits the STIR/SHAKEN ecosystem by increasing the number of calls that are signed with a SHAKEN signature and by expanding the variety of signing options available to voice service providers and their customers."[92] According to USTelecom, "for some providers, including smaller providers with limited resources, relying on third parties is essential to deploy STIR/SHAKEN in a cost-effective way. In addition, for certain equipment, including legacy IP equipment, third-party signing can be an effective and efficient means to deploy signing capabilities that otherwise would be cost-prohibitive."[93] USTelecom's assertion accords with the NANC Small Providers Report, which concludes that third-party authentication may benefit small providers by reducing the costs associated with STIR/SHAKEN implementation.[94]

22. The record also indicates, however, that certain types of third-party authentication practices can undermine confidence in the STIR/SHAKEN framework, and that guardrails are necessary.[95] TransNexus argues that arrangements in which a "downstream transit provider authenticates

[90] The rules we adopt today are not limited to arrangements based on a "Hosted SHAKEN" model or the "Carrier SHAKEN" model, or any other particular technological solution. *See* NANC Small Providers Report at 7-8 (explaining the different arrangements); TransNexus Comments at 3-4 (same). We agree with TransNexus that limiting third-party authentication to currently existing technical solutions is unnecessary and may even inadvertently prevent innovation should new solutions be developed in the future. *See* TransNexus Comments at 11. We will monitor any new solutions that may develop and may revisit this subject should action to address new risks be warranted.

[91] Numeracle Comments at 3; *see also* CTIA Reply at 2 ("[I]nnovative third-party caller ID authentication services[] can help to promote the widespread implementation of the STIR/SHAKEN framework."); NCTA Reply at 1; INCOMPAS Reply at 2.

[92] INCOMPAS Reply at 2; *see also* CTIA Reply at 3 ("The record makes clear that the use of third-party solutions to authenticate caller ID information can . . . facilitate call authentication and robocall mitigation innovation."); VON Reply at 2.

[93] USTelecom Comments at 2; *see also, e.g.*, INCOMPAS Comments at 5, 10-11; CCA Comments at 12; NYPSC Comments at 2 (agreeing that "allowing providers to utilize third-parties to perform caller ID authentication will aid robocall mitigation efforts by enabling providers who are otherwise unable to implement the FCC's STIR/SHAKEN protocols to authenticate call[er ID] . . . ." and also arguing that third-party authentication aids New York providers in complying with New York law regarding STIR/SHAKEN).

[94] NANC Small Providers Report at 6 ("[S]ervice providers can avoid complicated and costly STIR/SHAKEN implementations on their networks by sending their traffic to a vendor that provides access to a STIR/SHAKEN solution on the vendor's network, or through cloud computing services.").

[95] *See, e.g.*, TransNexus Comments at 5 (arguing that improper third-party signing scenarios "enable[] bad actors, including persons that initiate illegal robocalls and OSPs that originate such robocalls, to hide illegal robocalls amidst other calls authenticated by the transit provider. Accountability is thwarted. Call Validation Treatment is undermined. It becomes more difficult to identify and prevent illegal robocalls."); CTIA Reply at 5-6 ("Beyond raising significant transparency concerns, such inappropriate signing also undermines effective robocall mitigation (continued….)

calls using its own STI certificate and its specific means to determine the attestation level" present serious problems by "undermin[ing] STIR/SHAKEN and robocall prevention," and "enabl[ing] bad actors . . . to hide illegal robocalls amidst other calls authenticated by the transit provider."[96] ACA Connects adds that "[t]hird-party call authentication could raise serious concerns in some contexts, including in situations where a provider employs a third-party for call authentication as a ploy to avoid scrutiny and accountability."[97] NTCA similarly argues that, "[w]hile [third-party services] are a valuable option for providers' compliance with the Commission's caller-ID authentication rules, the potential for bad actors to utilize certain variations of these arrangements in a way that could undermine the integrity of the STIR/SHAKEN ecosystem cannot be overlooked."[98] NTCA and USTelecom agree that safeguards "are necessary to maintain trust in the STIR/SHAKEN ecosystem and allow these arrangements to function as intended for legitimate providers."[99]

23. We thus balance the benefits and concerns associated with third-party authentication by adopting a rule[100] that allows the practice subject to the two conditions specified above: (1) the provider with the STIR/SHAKEN implementation obligation must make all attestation-level decisions, consistent with the requirements of the technical standards; and (2) all calls must be signed using the certificate of the provider with the implementation obligation. These key guardrails will allow providers to realize the benefits of third-party authentication without compromising the integrity of the trust and governance structure upon which STIR/SHAKEN relies.[101] They will ensure that responsibility for properly authenticating a call's caller ID information—including complying with the attestation requirements of the ATIS standards—remains with the party assigned the STIR/SHAKEN implementation obligation under the Commission's rules,[102] and will prevent providers from shirking their due-diligence duties by

(Continued from previous page)
efforts, while also impeding equally valuable traceback and enforcement efforts"); NTCA Comments at 2 (raising a similar point as CTIA).

[96] TransNexus Comments at 4-5. While CCA contests some of TransNexus's assumptions in its evidence purporting to show attestation abuse on the part of transit providers, CCA nevertheless does support Commission action where "a third party may bestow an A or B level attestation without complying with the requisite conditions," such as those listed in ATIS-1000088. CCA Comments at 8-11.

[97] ACA Connects Comments at 4.

[98] NTCA Comments at 1.

[99] *Id.* at 1-2; *accord* USTelecom Reply at 3.

[100] We disagree with TransNexus's argument that we should simply issue a declaratory ruling to clarify that the Commission's rules already require voice service providers and intermediate providers to ensure that calls that they initiate onto the voice network are signed with their certificate, and to make all attestation-level decisions, regardless of which entity actually performs the act of signing. *See* TransNexus Comments at 5, 8-9; *see also* USTelecom Comments at 3 n.9. We instead find that codifying the rules through this *Eighth Report and Order* will not only ensure that all parties are on the same page regarding their STIR/SHAKEN implementation obligations moving forward, but will also give us additional enforcement tools in the event a bad actor originating service provider attempts to hide behind a third party to obscure its identity.

[101] *See supra* para. 7 (describing the STIR/SHAKEN governance model).

[102] Under this approach, originating service providers that rely on delegate certificates to establish a customer's right to use a telephone number, as required for an A-level attestation, may continue to do so to the extent permitted by the ATIS standards. ATIS-1000092 at 1; ATIS-1000080 at 1, 30 (referencing ATIS-1000092). These delegate certificates "provid[e] an end user or other VoIP entity with the ability to create and sign a PASSporT on its calls using a set of credentials . . . associated with [the] delegate certificate that is specific to the telephone number resources [which] that end user or other VoIP entity is authorized to use," ATIS-1000092 at 2, though originating service providers may choose to "ignor[e] all PASSporTs signed with delegate certificate credentials." *Id.* at 10. Because the originating service provider is ultimately responsible for making all attestation-level decisions and providing that information to a third-party performing the technological act of signing a call, the originating service provider remains responsible for vetting their customers and the criteria for applying A-level attestations, whether or
(continued….)

shifting STIR/SHAKEN authentication procedures to third parties.[103] By requiring calls to be signed using the certificate of the provider with the implementation obligation,[104] the STIR/SHAKEN governance model will be able to function as intended by making it easier to identify providers responsible for any authentication information transmitted with a call and facilitating enforcement remedies that may be needed for failures to comply with authentication requirements, including, for example, revocation of a provider's SPC token by the Secure Telephone Identity Governance Authority (STI-GA).[105]

24. We find that this approach will also guard against improper A- and B-level attestations by parties that are not originating service providers. Under the ATIS standards, an A- or B-level attestation

(Continued from previous page)
not a delegate certificate is accepted. *See* SOMOS Comments at 2 (noting that, in the toll-free context, Resp Orgs "currently use delegate certificates to authenticate customers' [telephone numbers]"). We decline SOMOS' suggestion that we should mandate acceptance of delegate certificates by providers in this *Eighth Report and Order*, as such a mandate is beyond the scope of the third-party authentication rules that we adopt today and the record in this proceeding is insufficient to weigh the benefits and burdens of imposing such a requirement. SOMOS Comments at 3 (arguing that the Commission should "mandate the universal acceptance of delegate certificates from Resp Orgs across the entire STIR/SHAKEN ecosystem").

[103] *See, e.g.*, TransNexus Comments at 12; USTelecom Comments at 2-3.

[104] We agree with commenters that the sharing of a provider's certificate with a third-party authenticator for the purpose of populating the identity header of a call does not create a security risk or undermine the STIR/SHAKEN trust model. As TransNexus states, STIR/SHAKEN certificates are similar to other secure certificates used extensively on the Internet: "Most certificate holders provision their certificates and private keys to be hosted by third parties. These companies are experts in securing digital assets, and they use technology best practices and systems to minimize risks." TransNexus Comments at 12-13. Further, we conclude that a provider's direction to a third-party authenticator as to which attestation level to apply to a given call does not raise concerns about privacy or confidentiality. As Numeracle confirms, "the service provider should be able to pass its direction for attestation on to systems maintained by vendors used for technical support to apply the appropriate attestation level to the service provider's own calls without having to also supply its [third-party authenticator] with contextual data related to its decision." Numeracle Comments at 7. NCTA states that any information that may need to be shared "is typically no more information than would be shared in connection with other robocall mitigation efforts, such as traceback or other initiatives to combat abusive calling practices . . . ." NCTA Comments at 4. No commenter argues third-party authentication practices, or specifically the sharing of information and certificates with third parties to perform the technological act of signing calls, presents security, privacy, or confidentiality concerns.

[105] *See* STI-GA, Policy Decision Binder, Version 6.0 at 64 (May 24, 2024) Policy Decision 003: SPC Token Revocation Policy Version 2.2 (Apr. 16, 2024), https://cdn.atis.org/sti-ga.atis.org/2024/05/22175841/240522-STIGA-Board-Policy-Decision-Binder-FINAL.pdf (enabling the STI-GA to engage in a managed revocation process if it finds that the provider with the STIR/SHAKEN implementation obligation "failed to adhere to one or more of the policy and/or technical requirements," including "SPC token Access Policy[or] SHAKEN specifications[,]" or "[w]hen directed by a court, the FCC, or another body with relevant legal authority due to a violation of Federal law related to caller ID authentication"). A few commenters note that the STI-GA is working on ways to address "improper attestations," and last year published a document providing guidance regarding what it considers to be "improper attestation," to "support STI GA processes and policies," including its token revocation process. STI-GA, *Improper Attestation*, https://sti-ga.atis.org/wp-content/uploads/2023/05/Improper-Attestation-Final.pdf; *see* TransNexus Reply at 20 (citing the STI-GA guidance document); CTIA Reply at 11 (same). Commenters agree that improper attestation is a prevalent issue. *See, e.g.*, TNS Comments at 3; USTelecom Reply at 2. By adopting guardrails on third-party authentication practices and ensuring that all calls are signed with the token of the provider with the STIR/SHAKEN implementation obligation, rather than a third party that may perform the technological functions of signing a call for that provider, we assist in the STI-GA's effort to address improper attestation by increasing transparency. *See, e.g.*, USTelecom Reply at 3; NCTA Comments at 2; Numeracle Comments at 1; *see also* TNS Comments at 6 (arguing that the Commission "could . . . use its authority to empower the industry to self-police improper attestations. Industry focused mechanisms can help identify and remedy improper attestations earlier in the process and may be preferred when improper attestations are the result of honest mistakes").

can only be applied if the provider authenticating the call originates it onto the public network.[106] That ATIS criterion can be satisfied in the context of a third-party arrangement where the originating service provider either: (1) arranges with a third party to perform the technological act of signing a call before the provider originates the call onto the public network; or (2) originates the call onto the public network with an agreement in place for a downstream intermediate provider to perform the technological act of signing the call. The second requirement of A- and B-level attestation, i.e., confirmation that an originating service provider has a "direct authenticated relationship" with its customer and can identify the customer,[107] is a determination that cannot be made by a third party with no relationship to that customer. The last requirement for an A-level attestation, i.e., confirmation that the originating service provider has established that the customer has a legitimate right to use the telephone number that appears in the caller ID,[108] also necessarily requires due diligence by the originating service provider. We thus agree with commenters in the record that it is inconsistent with the Commission's rules and the ATIS standards to allow third parties to make such determinations.[109] Since, as discussed above, the calls will need to be signed using the originating service provider's certificate, the rules we adopt today will ensure that such originating service providers are held accountable for improper attestation-level decisions for the calls they originate onto the public network, even if the technological act of signing the calls is performed by a third party.

25. Commenters generally support our adoption of these guardrails.[110] CTIA and Numeracle argue that this approach "is consistent with the existing [ATIS] standards and the FCC's regulatory framework for STIR/SHAKEN implementation."[111] CTIA also notes that requiring the use of "an originating [service] provider's [certificate] will better achieve the goals of the STIR/SHAKEN framework to promote a trusted voice ecosystem and increase transparency and integrity of caller ID information."[112] USTelecom contends that, "when calls are signed with the originating [service] provider's token, the Commission, the provider community, and analytics providers will have the information they need to take action should an originating [service] provider prove to routinely originate and authenticate illegal robocalls . . . ."[113] TransNexus argues that such limitations will, *inter alia*, "improve the quality of caller [ID] authentication information available to terminating providers," and thereby improve their call analytics.[114]

---

[106] *See supra* para. 10.

[107] ATIS-1000088 at 8; ATIS-1000074 at 12. ATIS-1000088 suggests that the originating service provider "authenticate the customer's identity through an authentication transaction, protected network path, or other means." ATIS-1000088 at 13. ATIS-1000088 provides further detail regarding three methods of achieving this customer authentication (i.e., via device-, account-, and network-based authentication). *See id.*, Appx. at 18-19.

[108] *See id.* at 8.

[109] *See, e.g.*, Letter from Alec Fenichel, Chief Technology Officer, TransNexus, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 17-97, at 1 (filed May 22, 2023) (TransNexus May 22, 2023 *Ex Parte*) ("Third-party signing, using the third-party's own STI certificate, undermines STIR/SHAKEN and robocall prevention.").

[110] *See, e.g.*, TransNexus May 22, 2023 *Ex Parte* at 4-5; TransNexus Comments at 12; CTIA Reply at 3-7; Neustar Comments at 2; Numeracle Comments at 3; USTelecom Comments at 2; NTCA Comments at 3-4; ZipDX Comments at 3.

[111] CTIA Reply at 4; *see also* Numeracle Comments at 5-7.

[112] CTIA Reply at 5.

[113] USTelecom Comments at 2; *see also* NTCA Comments at 2 (arguing that the use of the originating service provider's token will support traceback efforts).

[114] TransNexus Comments at 13; *see also id.* at 11 ("The purported benefit [of third-party authentication] is that more calls might be signed. However, signing more calls with an improper attestation, without proper identification of the OSP, and with no accountability for bad actors does not benefit subscribers or voice service providers that are trying to use the STIR/SHAKEN ecosystem properly and in good faith.").

26. We are not persuaded, however, by the arguments advanced by the few commenters that oppose the guardrails we adopt today. INCOMPAS argues that we should not adopt any rules governing third-party authentication,[115] and specifically opposes requiring providers to ensure that third-party authenticators sign calls using the provider's certificate.[116] INCOMPAS argues that instead we should "rely on the authority of the Enforcement Bureau to address those instances when an illegal robocaller is attempting to evade accountability through third-party authentication[, and] . . . rely on the [STI-GA] to address any ongoing issues or gaps in the standards that lead to attestation abuse."[117] We are committed to enforcing the Commission's rules against illegal robocallers and agree that the STI-GA should exercise its authority to hold providers accountable for non-compliance with the ATIS standards.[118] That does not mean, however, that we should not proactively adopt common-sense guardrails to prevent abuse of third-party authentication arrangements. By codifying these new rules, we give more certainty to providers seeking to comply with our caller ID authentication framework, establish clear standards that the Enforcement Bureau can apply when investigating misconduct,[119] and enable the STIR/SHAKEN ecosystem to realize additional benefits, such as making authentication information more valuable for call analytics.[120] INCOMPAS and VON also argue that changes to the Commission's rules may risk creating regulatory conflict with foreign jurisdictions, but provide no detail as to why imposing guardrails on third-party authentication would cause such an issue.[121] While we acknowledge that maintaining

[115] INCOMPAS Reply at 6.

[116] *See* INCOMPAS Comments at 12. INCOMPAS implies that third-party authentication arrangements using the third party's certificate, rather than the originating service provider's, do not impede traceback efforts because "domestic originating providers . . . typically are identified to the Industry Traceback Group ('ITG') by the signing company" in such arrangements, and use of an origination identifier or "origID" by third-party signing providers would be sufficient to "ensure that the Commission or ITG can identify the source of any illegal robocalls." INCOMPAS Reply at 4-5. We disagree. The origID field is an "opaque identifier" that "does not convey any [service provider] or customer information in and of itself." ATIS 1000088 at 15. Moreover, use of the origID field is permitted, but not required, by the ATIS standards, which do not establish detailed specifications regarding its use by providers. *See* ATIS 1000074 at 13. The approach described by INCOMPAS requires the ITG to obtain the cooperation of a third-party signing provider before it can identify the originator of an illegal call. In contrast, requiring third-party signers to use the originating service provider's token will allow the ITG to directly identify the originating service provider, thereby improving the efficiency of the traceback process and accountability within the STIR/SHAKEN ecosystem. *See* NTCA Comments at 2 ("One of the virtues of providers' use of STIR/SHAKEN is to identify the OSP—'traceback' efforts that get to the source of the illegally spoofed calls are bolstered by every operator in a call chain passing STIR/SHAKEN identity headers end-to-end.").

[117] *Id.* at 6.

[118] *See supra* note 105 (describing the STI-GA's authority to revoke the SPC token of a provider that does not comply with the requirements for authenticating calls under the ATIS standards).

[119] *See* TNS Comments at 6 (arguing that the Commission should increase enforcement against improper attestations); USTelecom Reply at 3 (same).

[120] *See supra* para. 25 (citing record support for the conclusion that these guardrails will improve the value of call analytics). We thus reject INCOMPAS's inference that it is sufficient to simply rely on providers to voluntarily establish appropriate parameters for the application of STIR/SHAKEN technical standards in commercial arrangements with third parties. INCOMPAS Reply at 4-5. As discussed below, we require all third-party authentication arrangements to be memorialized in written agreements that comport with the rules we adopt today.

[121] *See* INCOMPAS Reply at 7 ("[A]s other countries implement STIR/SHAKEN, it will be important not to implement rules that alter the standard in significant ways resulting in varied implementations that can impair interoperability among SHAKEN systems internationally."); VON Reply at 3 ("If the Commission were to impose third-party authentication restrictions, it would create a variance from the technical standard and from other national implementations of that standard, thereby complicating eventual efforts to enable interoperability of the U.S. STIR/SHAKEN mechanism with those of other countries. This would, in turn, undermine or complicate the effort to enable more internationally originated traffic to be SHAKEN-signed and recognized by U.S. terminating providers.").

"interoperability among SHAKEN systems internationally" is certainly important in protecting domestic consumers from illegal robocalls originating abroad, our action today eliminates the risk of such regulatory conflict by remaining consistent with the ATIS standards.[122]

B. Implementation and Compliance Requirements

27. In this section, we adopt several implementation requirements for providers that utilize third-party authentication and amend certain rules to comport with those requirements.[123] Specifically, and as described below, we require all providers with a STIR/SHAKEN implementation obligation to: (1) obtain an SPC Token and digital certificate; (2) certify to complete or partial implementation in the Robocall Mitigation Database *only* if they have obtained an SPC token and digital certificate and sign calls with their certificate; and (3) memorialize and maintain records of any third-party authentication agreement(s) they have entered into, subject to certain limitations.

28. *Requirement to Obtain a Token and Digital Certificate.* Consistent with the third-party authentication rule we adopt today, all providers with a STIR/SHAKEN implementation obligation under the Commission's rules will now be explicitly required to obtain an SPC token from the Policy Administrator and present that token to a STIR/SHAKEN Certificate Authority to obtain a digital certificate. This requirement is necessary now that all calls, whether technologically signed directly by the provider with the STIR/SHAKEN implementation obligation or by a third party, must be signed with the former's certificate,[124] thereby ensuring that accountability for compliance with our caller ID authentication rules remains with the party required to implement STIR/SHAKEN under the Commission's rules.[125] The record indicates that requiring all providers with a STIR/SHAKEN implementation obligation to obtain their own SPC tokens and digital certificates will also result in other benefits,[126] such as "encourag[ing] continued innovation" within the existing STIR/SHAKEN framework[127] and ensuring that providers with STIR/SHAKEN implementation obligations under the

[122] INCOMPAS Reply at 7.

[123] In the *Sixth Caller ID Authentication Further Notice*, the Commission sought comment on whether any other rules would need to be amended if it explicitly authorized third-party authentication. *Sixth Caller ID Authentication Further Notice*, 38 FCC Rcd at 2623, para. 104.

[124] NTCA Comments at 2 (arguing that the Commission should require "all [Originating Service Providers] using 'third-party signing' arrangements [to] themselves register with the STI-PA and a STI-CA to procure their own tokens and certificates, and that their own certificates are then used to sign each originating call"); *see also* ZipDX Comments at 2-3 (arguing that an "originating voice service provider can apply that signature itself, or it can use another party—but the signature must be that of the originating voice service provider"); TransNexus Comments at 8 (asserting that the Commission's rules already "require voice service providers to implement and use STIR/SHAKEN as described in the ATIS standards, including ATIS-1000080. Therefore, OSPs that do not register for STIR/SHAKEN with the [] Policy Administrator, get a SHAKEN certificate from an STI Certification Authority, and authenticate their calls, either directly itself or using a Hosted or Carrier service with its STI certificate are not compliant with the Commission's rules").

[125] NTCA Comments at 3-4 (explaining that this solution would prevent harm to consumers and practices that undermine industry's investment in the STIR/SHAKEN framework); USTelecom Comments at 2-3 ("When calls are signed with the originating provider's token, the Commission, the provider community, and analytics providers will have the information they need to take action should an originating provider prove to routinely originate and authenticate illegal robocalls, thus providing the accountability the STIR/SHAKEN framework is designed to facilitate. The same applies when a gateway provider relies on a third party to sign calls on its behalf to meet the Commission's emerging gateway provider signing requirement.").

[126] *See infra* Section III.C.

[127] CTIA Reply at 6 & n.14 (pointing to current innovation in the areas of call analytics and robocall mitigation and the development of new tools and capabilities).

Commission's rules "have a fair and proportionate financial stake in the STIR/SHAKEN ecosystem."[128] We believe the positive effects of this requirement will be far-reaching, as the record indicates that many providers claiming to have implemented STIR/SHAKEN have not obtained their own tokens and certificates.[129] Indeed, TransNexus estimates "that about 64% of providers" in the Robocall Mitigation Database that claim STIR/SHAKEN implementation are not registered with the Policy Administrator.[130]

29. We disagree with INCOMPAS that "requiring all providers to obtain a token that could be used by a third-party authenticator would necessitate changes with both the industry's token access policies and the Commission's current administration of voice service providers."[131] In support of its arguments, INCOMPAS merely lists the STI-GA's SPC token access standards, including the requirement to obtain an Operating Company Number (OCN),[132] and states that many providers "do not operate a business model that allows them to get an OCN."[133] INCOMPAS does not, however, explain why this would be the case for any provider with a STIR/SHAKEN implementation obligation, much less "many" providers with STIR/SHAKEN implementation obligations. In fact, in recent years, the Wireline Competition Bureau has repeatedly found that few providers are currently unable to obtain an SPC token due to revisions made to the STI-GA token access policy in May 2021.[134] Consistent with this finding, the record in this proceeding evidences that the barriers to and costs associated with obtaining and maintaining SPC tokens and digital certificates are low,[135] including for small providers.[136] Moreover, the

[128] NCTA Comments at 3 (continuing that requiring providers with STIR/SHAKEN implementation obligations to obtain SPC tokens will "prevent OSPs from dodging token access fees by hiding behind a third party").

[129] *See, e.g.*, ZipDX Reply at 4 (noting that provider certifications in the Robocall Mitigation Database show that many have not obtained a token per the STI-PA list).

[130] TransNexus May 22, 2023 *Ex Parte* at 3.

[131] INCOMPAS Reply at 6.

[132] *See* STI-GA, Policy Decision Binder, Version 6.0 at 6 (May 22, 2024), Policy Decision 001: SPC Token Access Policy Version 2.1 (May 18, 2021), https://cdn.atis.org/sti-ga.atis.org/2024/05/22175841/240522-STIGA-Board-Policy-Decision-Binder-FINAL.pdf (requiring providers to "[h]ave been assigned an Operating Company Number (OCN), or a Resp Org ID").

[133] INCOMPAS Reply at 6 n.11 (listing the current STI-GA token access policy that requires "a provider to have (1) a current FCC Form 499A on file with the Commission, (2) been assigned an Operating Company Number ("OCN"), and (3) certified that they have implemented STIR/SHAKEN or comply with the Robocall Mitigation Program requirements and are listed in the FCC Robocall Mitigation Database"). While INCOMPAS states that some providers are unable to get an OCN "from the Commission," OCNs are assigned by the National Exchange Carrier Association (NECA). *See* NECA, Company Codes (OCNs), https://www.neca.org/business-solutions/company-codes (last visited Aug. 27, 2024).

[134] *First Reevaluation of STIR/SHAKEN Extensions Public Notice*, 36 FCC Rcd at 17751 & n.26 (finding that the extension remains necessary because "an entity that meets the definition of a provider of 'voice service' cannot comply with the STIR/SHAKEN rules if it is unable to receive a token" but explaining how the Governance Authority had revised its policies to account for the main concerns underlying this extension); *Second Reevaluation of STIR/SHAKEN Extensions Public Notice*, 37 FCC Rcd at 14880-81; *Wireline Competition Bureau Performs Required Evaluation Pursuant to Section 64.6304(F) of the Commission's Rules*, WC Docket No. 17-97, Public Notice, DA 23-1157, 4-6 (WCB Dec. 15, 2023) (explaining that we "continue to believe that the Governance Authority's revised policy has resolved the main practical concern that originally created a need for the SPC token extension and that token access does not stand as a significant barrier to full participation in STIR/SHAKEN").

[135] INCOMPAS states that "voice service providers are required to provide the STI Policy Administrator with all-associated IP addresses as part of acquiring a Service Provider Code token," and claims that this is a highly burdensome step. INCOMPAS Reply at 6 n.12. INCOMPAS does not explain why supplying IP addresses to the Policy Administrator is highly burdensome, however, or why any burden of submitting the information would outweigh the benefits of requiring providers with a STIR/SHAKEN implementation obligation to register with the Policy Administrator. We note that the Policy Administrator states that it collects IP addresses from providers for the purpose of whitelisting. *See, e.g.*, STI-PA, Secure Telephone Identity (STI) Service Provider Methods and

(continued….)

compliance deadline we adopt below provides ample time for all sizes of providers to come into compliance with our newly adopted rules, thereby minimizing any compliance burdens.[137]

30. *Robocall Mitigation Database Certifications.* Consistent with the foregoing requirements, we update the Commission's rules to prohibit any provider with a STIR/SHAKEN implementation obligation from certifying to complete or partial implementation in the Robocall Mitigation Database unless they have obtained an SPC token and digital certificate and sign calls with their certificate, either themselves or when working with a third party to perform the technological act of signing calls having met the necessary conditions we impose in this Order.[138] For all of the reasons discussed above, we agree with TransNexus that providers that have a STIR/SHAKEN implementation obligation but rely on third-party authentication arrangements using the third party's certificate are not in compliance with the governance model established by STIR/SHAKEN technical standards, which require providers to obtain an SPC token and digital certificate to authenticate calls.[139] Such providers should not,

(Continued from previous page)
Procedures, STI-PA-US-METHODPROCSP-001 Issue 6, at 4 (Oct. 2021), https://authenticate.iconectiv.com/sites/authenticate/files/2021-10/Service_Provider_Guidelines_Issue_6.pdf. According to the National Institute of Standards and Technology's Computer Security Resource Center (CSRC), a whitelist can be defined as "[a]n approved list or register of entities that are provided a particular privilege, service, mobility, access or recognition." NIST, *CSRC Glossary*, https://csrc.nist.gov/glossary/term/whitelist (last visited Aug. 27, 2024).

[136] *See* STI-GA, Policy Decision Binder, Version 6.0 at 78 (May 22, 2024), Policy Decision 005: Funding Policy Version 5.1 (Dec. 15, 2023), https://cdn.atis.org/sti-ga.atis.org/2024/05/22175841/240522-STIGA-Board-Policy-Decision-Binder-FINAL.pdf (setting a provider's annual fee for token access in 2024 equal to the provider's assessable Form 499-A revenues (the greater of revenue lines 432 or 514) times .00002722, with a minimum annual fee of $500); NCTA Comments at 3 n.3; NTCA Comments at 3-4; NYPSC Comments at 3 (agreeing that "access to a [token] is no longer a significant barrier to the implementation of STIR/SHAKEN . . . because of the allowed use of third-party authentication methods"); TransNexus Comments at 12 (asserting that "[t]he ability to obtain SPC tokens is not likely to present a barrier to providers' compliance with the Commission's rules and STIR/SHAKEN standards" and citing to the NANC Small Providers Report's assertion that "VoIP providers generally, are SIP connected networks. These service providers should have no significant barriers preventing the implementation of SHAKEN, irrespective of size. The market for SHAKEN solutions is robust and competitive and Section 2.2 discusses the general options available for any providers in this category"); USTelecom Comments at 1 n.5; TransNexus Reply at 17-18; ZipDX Reply at 4.

[137] *See infra* paras. 34-35. We note that providers that cannot obtain an SPC token after diligently pursuing one from the Policy Administrator may still claim an implementation extension under the Commission's existing rules. While the Commission sought comment on whether to eliminate the SPC token extension in the *Sixth Caller ID Authentication Further Notice*, 38 FCC Rcd at 2623, paras. 107, 108, we decline to do so at this time. In March 2023, the Commission updated its requirements for submissions to the Robocall Mitigation Database, including a new requirement that providers claiming a STIR/SHAKEN implementation extension or exemption explicitly state the rule that excepts it from compliance and why the provider qualifies for the extension or exemption. *Sixth Caller ID Authentication Report and Order*, 38 FCC Rcd at 2596-97, para. 45. All providers were required to file submissions to the Robocall Mitigation Database that comply with this and additional content requirements by February 26, 2024. *Robocall Mitigation Database Filing Deadline Public Notice* at 2. These filings are currently under review. As part of that assessment, the Wireline Competition Bureau will determine the number of providers still relying on the SPC token extension and the merit of the justifications submitted by those claiming the extension. We will be better able to determine whether to retain or eliminate the SPC token extension at that time.

[138] In the *Sixth Caller ID Authentication Further Notice*, the Commission sought comment on whether it should "prohibit providers from certifying to having implemented STIR/SHAKEN in the Robocall Mitigation Database unless their calls are signed with their own SPC token, whether directly or through a third party." *Sixth Caller ID Authentication Further Notice*, 38 FCC Rcd at 2622, para. 103.

[139] *See supra* para. 28 (describing the STIR/SHAKEN governance model and need to obtain an SPC token and digital certificate to authenticate calls); TransNexus May 22, 2023 *Ex Parte* at 3-4 (arguing that STIR/SHAKEN standards are not being followed properly and that "[w]ith third-party signing, OSPs are not STI Participants. They (continued….)

therefore, claim to have implemented STIR/SHAKEN pursuant to the technical standards required by the Commission's rules in the Robocall Mitigation Database.[140] While we recognize that some of these providers may have relied on third-party SPC tokens and certificates out of a good faith belief that such arrangements are permissible under the Commission's rules in the past, such practices will now be expressly prohibited by our rules, and providers that have relied on third-party tokens and digital certificates in the past will now need to obtain their own SPC tokens and certificates and use them to sign calls, consistent with the requirements of the STIR/SHAKEN standards and the compliance deadlines we set below. Providers that do not obtain and use an SPC token and certificate must update their Robocall Mitigation Database certifications to state that they have not fully or partially implemented STIR/SHAKEN[141] to avoid being referred to the Enforcement Bureau for violations of the Commission's rules, including the rules governing certifications submitted to the Robocall Mitigation Database and the obligation to submit information to the Commission that is true, accurate, and up-to-date.[142]

31. We decline to adopt new content requirements for Robocall Mitigation Database certifications at this time. In the *Sixth Caller ID Authentication Further Notice*, the Commission sought comment on requiring providers to submit additional information to the Robocall Mitigation Database, "including the identity of the third party providing [their authentication] solution, any requirements the provider has imposed on the third party to ensure compliance with the requirements of the ATIS technical standards and the Commission's rules, and what the provider itself does to ensure compliance with those requirements under the third-party arrangement[.]"[143] In response to the *Further Notice*, commenters suggest that we should require providers to submit a variety of additional information to the Robocall Mitigation Database, including evidence of registration with the Policy Administrator,[144] the identity of

(Continued from previous page)
operate outside the STIR/SHAKEN governance model. Therefore, they cannot claim a STIR/SHAKEN implementation").

[140] TransNexus May 22, 2023 *Ex Parte* at 3; Numeracle Comments at 9 ("The Commission should require all providers to sign calls with their own SPC token to certify [in the Database] that they have implemented STIR/SHAKEN"); *see also* NTCA Comments at 2 (agreeing with TransNexus that a third party signing on behalf of an OSP "that is neither registered with the [STI-PA] nor registered with a [STI-CA] . . . runs counter to the STIR/SHAKEN standards"); ZipDX Reply at 4 (arguing that Commission rules "already require originating providers to sign their own calls, but many do not" and "are explicitly flouting the [Commission's] regulations"); *see also* 47 CFR § 64.6305(d)(1), (e)(1), (f)(1) (requiring providers to certify in the Robocall Mitigation Database whether they have implemented the STIR/SHAKEN authentication framework); *id.* § 64.6300(m) (defining "STIR/SHAKEN authentication framework" as the STIR/SHAKEN standards).

[141] Providers that qualify for a STIR/SHAKEN implementation extension because they cannot satisfy the requirements to obtain an SPC token can claim the extension in their Robocall Mitigation Database submissions at this time.

[142] 47 CFR § 64.6305(d)(1)-(4), (e)(1)-(4), (f)(1)-(4) (requiring voice service providers, gateway providers, and non-gateway intermediate providers to certify to its STIR/SHAKEN implementation status in the Database), (d)(5), (e)(5), (f)(5) (requiring a provider to update its filings in the Database within 10 business days if there is any change information), (d)(3)(ii), (e)(3)(ii), (f)(3)(ii) (requiring that filings in the Database be signed by an officer in conformity with Commission rules that require filings to include true and correct information, under penalty of perjury).

[143] *Sixth Caller ID Authentication Further Notice*, 38 FCC Rcd at 2622-23, para. 104.

[144] TransNexus Comments at 14 & n.15 ("For example, the [Database] filer might provide the OCN they used to register with the STI-PA. This might require the STI-PA to modify their webpage listing of Authorized Providers, https://authenticate.iconectiv.com/authorized-service-providers-authenticate, to include the primary registration OCN of each authorized provider. This would be beneficial, as there are already duplicate names listed, with no way to identify which provider using that name is authorized.").

any third-party authentication solutions they use,[145] and information that details their Know Your Customer standards.[146]

32. We conclude that any value of requiring providers to submit this information at this time is minimal, and does not warrant the additional operational and administrative burdens of requiring providers to update their Robocall Mitigation Database submissions. For instance, now that we require all providers with a STIR/SHAKEN implementation obligation to obtain their own SPC token from the Policy Administrator and a digital certificate from a Certification Authority, we conclude it unnecessary for providers to make a further showing at this time that they are registered with the Policy Administrator, as TransNexus suggests. Moreover, as Numeracle points out, the Policy Administrator's list of providers authorized to participate in STIR/SHAKEN is publicly available, allowing Commission staff to easily verify a provider's registration status without further expanding the Robocall Mitigation filing requirements.[147] We also believe it is unnecessary to require providers to identify any third-party authentication solutions they use in their Robocall Mitigation Database submissions, as NCTA suggests.[148] Under the rules we adopt today, which require calls to be signed using the digital certificate of the provider with the STIR/SHAKEN implementation obligation, responsibility and accountability for compliance with the STIR/SHAKEN standards will be traced back to that provider, not a third-party entity that technologically signs the call. Further, we agree with INCOMPAS that requiring providers to identify the specific third-party solutions that they may employ to perform the technological act of signing calls could require providers to update their Robocall Mitigation Database submissions more frequently if such solutions change, thereby increasing administrative burdens for providers with minimal benefit.[149] Lastly, providers are already required to describe in their robocall mitigation plans how they comply with their existing obligation to know their customers under the Commission's rules.[150] We, thus, decline to further amend our requirements for Robocall Mitigation Database certifications at this time,[151] but we will closely observe how providers comply with the requirements we adopt today to determine

[145] NCTA Comments at 3 (arguing that disclosure of this information "will further increase transparency and enable the Commission to monitor compliance without requiring public disclosure of more sensitive details that bad actors could seek to exploit").

[146] Numeracle Comments at 8 n.5 (arguing that "[t]he Commission should mandate that a provider must explicitly state its KYC standards in its robocall mitigation plan").

[147] iconectiv Authenticate, *authorized providers*, https://authenticate.iconectiv.com/authorized-service-providers-authenticate (last visited Aug. 27, 2024); *see also* Numeracle Comments at 9.

[148] NCTA Comments at 3.

[149] *See* INCOMPAS Comments at 14 (arguing that we should not require providers to identify any third-party authentication solutions they rely on in the Robocall Mitigation Database because providers would "constantly" have to update their filings and certification, "deter[ing] interest in trying out a variety of different solutions across one's network" and innovation).

[150] 47 CFR § 64.6305(d)(2)(ii) (requiring a voice service provider to describe how it complies with its obligation to know its customers pursuant to section 64.1200(n)(4) in its Robocall Mitigation Database certification), (e)(2) (requiring a gateway provider to describe how it complies with its obligation to know now its upstream providers pursuant to § 64.1200(n)(5) in its Robocall Mitigation Database certification), (f)(2) (requiring a non-gateway intermediate provider to include a description of any procedures in place to know its upstream providers in its certification).

[151] ZipDX proposes that "[n]ew [Robocall Mitigation Database] registrations should not immediately become active. Instead, FCC staff should vet the registration to ensure that the applicant has a token from the STI-PA and if not, that the filed RMP contain a thorough, credible explanation as to why not." ZipDX Reply at 4. In August 2024, we launched a separate proceeding to consider procedural measures for improving the overall quality of information submitted to the Robocall Mitigation Database. *See Robocall Mitigation Database NPRM.* We believe that addressing ZipDX's procedural proposal would be more appropriate in the context of that proceeding, and thus decline to do so here.

whether additional information would assist our compliance reviews and enforcement activities in the future.[152]

33. *Recordkeeping*. To ensure compliance with the requirements we adopt herein for third-party authentication, and to enable the Commission to monitor such compliance and enforce its rules, we require that providers that choose to work with a third party to perform technological act of signing calls do so pursuant to a written agreement.[153] The agreement must specify the specific tasks that the third party will perform on the provider's behalf and confirm that provider will: (1) make all attestation-level decisions for calls signed pursuant to the agreement, and (2) ensure that all calls will be signed using the provider's certificate. Providers may be required to submit a copy of the agreement to the Commission in connection with a review of the provider's compliance with the Commission's rules or an investigation by the Enforcement Bureau.[154] We require that a current agreement be in place for as long as any third-party authentication arrangement exists, and that all copies of third-party agreements be maintained for a period of two years from the end or termination of the agreement.[155]

34. *Compliance Deadline*. The new third-party authentication guardrails we adopt in this *Report and Order* include recordkeeping and Robocall Mitigation Database certification requirements under 47 CFR §§ 64.6301(b)(3)-(b)(5), 64.6302(f)(3)-(f)(5), and 64.6305(d)-(f), which may contain new or modified information collections subject to review by the Office of Management and Budget (OMB) under the Paperwork Reduction Act (PRA).[156] While the remaining amendments to sections 64.6301-64.6305 adopted in this *Report and Order* do not themselves require OMB approval, in practice,

[152] ACA Connects argues that the "Commission could further require reseller providers to disclose to the Commission (on a confidential basis), the identity of any wholesale provider that authenticates some or all of their calls." ACA Connects Comments at 5-6 & n.9 (suggesting this could enhance current accountability mechanisms for "white-label voice providers relying on wholesale providers for call authentication"). As discussed above, however, in the context of a wholesale provider originating a call onto the public network for a reseller which lacks control over the network infrastructure necessary to implement STIR/SHAKEN, it is the wholesale provider that has the STIR/SHAKEN implementation obligation, that must authenticate the calls using its own digital certificate. *See supra* para. 17.

[153] In the *Sixth Caller ID Authentication Further Notice*, the Commission sought comment on the measures it would "need to implement to monitor compliance with its rules if third-party authentication arrangements are employed." *Sixth Caller ID Authentication Further Notice*, 38 FCC Rcd at 2622-23, para. 104. No commenter raises arguments for or against recordkeeping requirements.

[154] To the extent that an agreement between a provider with the STIR/SHAKEN implementation obligation and a third party contains confidential information, providers may seek confidential treatment for that information. 47 CFR § 0.459.

[155] We emphasize that there must be a memorialized agreement between the provider with the STIR/SHAKEN implementation obligation and the third party performing the technological act of signing a call for the arrangement to be considered third-party authentication under the rules we adopt today. For example, the Commission's rules require voice service providers to authenticate the traffic that they originate, and, if they fail to do so, non-gateway intermediate providers must themselves authenticate any unauthenticated calls they receive directly from originating providers. Consequently, an intermediate provider that receives an unauthenticated call from an originating provider does not engage in third-party authentication simply because it is the entity that uses STIR/SHAKEN to authenticate the call. In such an instance, the intermediate provider is discharging its own authentication obligation under the Commission's rules by signing the unsigned traffic. If, however, the originating service provider has executed an agreement for its immediate downstream intermediate provider to perform the technological act of signing a call on the originating provider's behalf, subject to the conditions adopted in this *Eighth Report and Order*, that would qualify as a third-party authentication arrangement. We thus reject INCOMPAS's argument that our definition of third-party authentication should apply when downstream providers are merely "signing calls that were not signed up-stream," even if the downstream provider "may not be offering signing service *per se*." INCOMPAS Comments at 6.

[156] *See infra* para. 54 (delaying the amendments to 47 CFR §§ 64.6301- 64.6305).

compliance with the requirements of these provisions will likely entail compliance with the provisions of 64.6301(b)(3) through (5), 64.6302(f)(3) through (5), and 64.6305(d) through (f), respectively. Therefore, we set a compliance deadline for all our newly adopted requirements of 30 days after publication in the Federal Register, or 120 days after release of this *Report and Order*, whichever is later.

35. We expect that requiring providers to comply with all of the obligations we adopt in the *Report and Order* on the same date will facilitate compliance with our rules, and consequently we elect to delay the effectiveness of the entirety of the modifications to sections 64.6301 through 64.6305 pending OMB approval of sections 64.6301(b)(3) through (5), 64.6302(f)(3) through (5), and 64.6305(d) through (f). Consistent with the Commission's approach in prior rulemakings,[157] we direct the Wireline Competition Bureau to announce effective dates for 47 CFR §§ 64.6301-64.6305 through Public Notice. Any provider with a STIR/SHAKEN implementation obligation that has failed to both: (1) obtain an SPC token from the Policy Administrator and a digital certificate from a Certificate Authority; and (2) ensure that all calls that it is required to authenticate are signed using its own digital certificate, will be required to update their certifications in the Robocall Mitigation Database to state that they have not fully or partially implemented STIR/SHAKEN by the effective date of the rules listed in this paragraph as announced by Public Notice.

36. The record reflects support for our adoption of a single compliance deadline for our third-party authentication obligations based on the schedule above.[158] Commenters explain that providers using third-party authentication solutions may have to make a number of commercial and network changes to comply with the newly adopted authentication and robocall mitigation requirements, such as creating new commercial arrangements with customers or third-party vendors,[159] taking the steps needed to obtain a token and certificate,[160] determining the process for assigning an attestation level,[161] and making changes to their network to sign calls with their own token.[162] We agree with NCTA that adopting a transition period would "promote fairness and avoid exposing providers relying on good faith on non-conforming third-party solutions to the threat of immediate liability."[163] We also agree with INCOMPAS that "[w]hile the evolution toward broad token access should be encouraged, expecting a flash-cut" to such a change would not be practical.[164] Therefore, we grant providers a reasonable amount of time to adjust their third-party call authentication practices to comply with the rules we adopt today, and will not require compliance with these rules sooner than 120 days after release of this *Report and Order*. Although we find that this approach will allow sufficient time for providers to adjust their third-party authentication practices,[165] providers should comply with our new rules as soon as reasonably practicable.

---

[157] *See Sixth Caller ID Authentication Report and Order*, 38 FCC Rcd at 2627, para. 125; *Robocall Mitigation Database Filing Deadline Public Notice* at 2.

[158] NCTA Comments at 3; INCOMPAS Comments at 7; INCOMPAS Reply at 6; TransNexus Reply at 17.

[159] INCOMPAS Reply at 6; NCTA Comments at 3.

[160] INCOMPAS Reply at 6; TransNexus Reply at 17.

[161] TransNexus Reply at 17.

[162] NCTA Comments at 3; TransNexus Reply at 17; *see also* CCA Comments at 13.

[163] NCTA Comments at 3; *see also* TransNexus Reply at 17; INCOMPAS Comments at 7.

[164] INCOMPAS Comments at 7.

[165] *See Rural Call Completion*, WC Docket No. 13-39, Third Report and Order, 33 FCC Rcd 8400, 8416, para. 42 (2018) (*Rural Call Completion Third Report and Order*) (finding, "based upon [Commission] experience, that 45 days will provide covered providers with sufficient time to adjust their call routing practices" and that "a 90-day phase-in period . . . will permit covered providers adequate time to make adjustments to existing contractual arrangements"). While we do not adopt CCA's request to implement a six-month compliance period, we note that in practice, delaying the effectiveness of our rules pending OMB approval is likely to offer a similar compliance period. CCA Comments at 2; *Rural Call Completion Third Report and Order*, 33 FCC Rcd at 8416, para. 43 (continued….)

C. Summary of Cost-Benefit Analysis

37. We find that the benefits of the third-party authentication rules we adopt today will greatly exceed the costs they will impose on providers. In the *Sixth Caller ID Authentication Report and Order*, the Commission confirmed the conclusion that "our STIR/SHAKEN rules are likely to result in, at a minimum, $13.5 billion in annual benefits," and that the benefits associated with the rules will greatly outweigh the costs imposed on providers.[166] We again affirm this conclusion, and find that "[l]imiting the ability of illegal robocallers to evade existing rules will preserve and extend the benefits of STIR/SHAKEN."[167]

38. *Benefit: Preserving the Structural Integrity of the STIR/SHAKEN Regime.* Establishing clear rules of the road for providers using third parties to authenticate voice service calls will increase the STIR/SHAKEN framework's benefits. Our new third-party authentication requirements will increase compliance with the Commission's caller ID authentication rules, promote accountability and trust within the STIR/SHAKEN framework, and improve the accuracy of A- and B- level attestations. As a result, more illegal robocalls will be identified and stopped before they can reach American consumers, helping increase confidence in the U.S. telephone network. In adopting these requirements, we strike a balance that allows providers to realize the benefits of third-party authentication while preventing abuses that could undermine the STIR/SHAKEN standards. The new rules will increase the number of calls signed with a SHAKEN signature, give providers and their customers more signing options, and make it more cost-effective for all providers to implement STIR/SHAKEN. Indeed, the record reflects that third-party authentication may "confer[] substantial benefits,"[168] particularly for small providers, as deploying STIR/SHAKEN in the IP portion of their voice service network may otherwise be cost-prohibitive.[169] The cost savings that make third-party authentication a worthwhile, cost-effective investment for small providers is an added benefit.

39. *Benefit: Ensuring Reliable Access to Emergency and Healthcare Communications.* In the *First Caller ID Authentication Report and Order*, the Commission noted that "hospitals and 911 dispatch centers have reported that robocall surges have disabled or disrupted their communications network, and such disruptions have the potential to impede communications in life-or-death emergency situations. In one instance, Tufts Medical Center in Boston received more than 4,500 robocalls in a two-hour period. In another, the phone lines of several 911 dispatch centers in Tarrant County, Texas, were disabled because of an hourlong surge in robocalls."[170] Although the Commission declined then to estimate the considerable public safety benefits of reduced robocalling, in the wake of subsequent Commission orders estimating the public safety benefits of reduced emergency response delays, we elect to do so now. In the *Location-Based Routing Report and Order*, we estimated that a one-minute reduction in average emergency response times would save 13,837 lives, a mortality risk reduction worth $173 billion annually.[171] Based on that figure, any reduction in emergency response delays caused by robocalls could confer large benefits. For example, if unwanted and illegally spoofed robocalls caused

(Continued from previous page)
(noting that the OMB approval process was likely to give providers "approximately six-months, if not more, to come into compliance" with any associated rules).

[166] *Sixth Caller ID Authentication Report and Order*, 38 FCC Rcd at 2616, para. 86 (citing to the reasoning provided in the *First Caller ID Authentication Report and Order and Further Notice* and explaining that the Commission sought comment on this conclusion in the *Fifth Caller ID Authentication Further Notice*).

[167] *Id.* at 2616, para. 87.

[168] CCA Comments at 13.

[169] *See, e.g.*, USTelecom Comments at 2 n.5.

[170] *See First Caller ID Authentication Report and Order*, 35 FCC Rcd at 3264, para. 50.

[171] *See Location-Based Routing for Wireless 911 Calls*, PS Docket No. 18-64, Report and Order, FCC 24-4, at 52, para. 118 (Jan. 26, 2024).

only a one-second delay in average emergency response times, the potential mortality risk-reduction benefit would be worth $2.88 billion annually (i.e., 173/60=2.88). Assuming a linear relationship between prevalence of robocalling and possible emergency response delays, a one-tenth reduction in robocalling and the accompanying tenth-of-a-second reduction in emergency response time, which could be achieved by better third-party authentication, would be worth $288 million annually. A more modest one-twentieth reduction in robocalling and one-twentieth-of-a-second reduction emergency response times would be worth $144 million annually.[172]

40. *Benefit*: *Reducing Network Congestion and Consumer Complaints.* The Commission has noted previously that unwanted and illegal robocalls increase network congestion and the labor costs of handling numerous customer complaints.[173] Third-party-authenticated traffic that does not currently meet STIR/SHAKEN technical standards and results in illegal or unwanted robocalls terminates on the networks of unwitting carriers, forcing them to bear the costs of unwanted call traffic in the form of increased customer complaints and network congestion. Tightening third-party authentication requirements will generate savings for voice service providers, which may pass them on to consumers in the form of lower rates.

41. *Costs.* While some argue that limitations on third-party authentication may be costly without concomitant benefits,[174] the record more broadly reflects that the costs of requiring providers that use third-party solutions to authenticate calls with their own token and applying their attestation level to their calls will be minimal for all providers, including small providers.[175] As explained above, by adopting a minimum compliance period for our third-party authentication requirements of 120 days following release of this *Report and Order*, we take a balanced approach that maximizes the benefits to providers using third-party authentication solutions while minimizing its costs. And, though we acknowledge that our adopted third-party authentication requirements will have implementation and recordkeeping costs, we conclude that explicitly authorizing third-party authentication with our adopted limitations will produce significant benefits, including increased trust in the STIR/SHAKEN framework and the accuracy of A- and B-level attestations.

D. Legal Authority

42. Consistent with our proposals, we adopt the foregoing obligations pursuant to the legal authority that the Commission relied on in prior caller ID authentication and call blocking orders. We note that no commenter questioned our proposed legal authority.

---

[172] To achieve $100 million in annual public safety benefits, our third-party authentication rules would only have to reduce unwanted and illegal robocalls such that average emergency response times were improved by a mere 0.035 seconds, or about one-thirtieth of a second. Given the prevalence of robocalls and their ability to disrupt communications and cause network congestion, it is highly likely that implementing third-party authentication rules to strengthen the STIR/SHAKEN ecosystem will reduce robocalls by at least this much, resulting in life-saving benefits.

[173] *First Caller ID Authentication Report and Order*, 35 FCC Rcd at 3264-45, para. 52.

[174] *See, e.g.*, CCA Comments at 12, 13 (arguing that "the alleged harms from third party authentication have not been substantiated" if flexible third party signing is not permitted, "[r]esellers, VASPs or other entities will incur the costs of developing or outsourcing the platform required to sign calls. . . . Although CCA is unable at this time to assign cost estimates to such changes, they surely are not trivial. Apart from costs, the changes will take time to implement and operationalize").

[175] *See, e.g.*, NCTA Comments at 3 n.3 (explaining that since token access fees are based on 499 revenues, they will not be unreasonably burdensome for small providers and for those providers "that do not file Form 499s, some small, flat fee may still be appropriate to avoid free riding"); ZipDX Reply at 4 (arguing that that the cost to obtain and maintain a token is revenue-based and will be small for a small reseller); *supra* note 136 (describing calculation of token access fees).

43. *Third-Party Authentication.* We conclude that section 251(e) of the Act and the Truth in Caller ID Act provide us with the authority to authorize providers to engage in third-party authentication practices subject to certain limits.[176] Specifically, we find that our section 251(e) numbering authority and the Truth in Caller ID Act each provide the Commission with independent authority to require providers that use third parties to authenticate calls to adhere to two limitations: (1) the provider with the STIR/SHAKEN implementation obligation under the Commission's rules must be the entity that determines whether A-, B-, or C- level attestation should be applied to the call; and (2) all calls must be signed using the SPC token of the provider with the implementation obligation.

44. As the Commission explained in the *First Caller ID Authentication Report and Order*, section 251 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] Further, the Truth in Caller ID Act provides us with authority to adopt rules that are "necessary to . . . protect voice service subscribers from scammers and bad actors."[178] As the Commission has found in several caller ID authentication and call blocking orders, we again find that section 251(e) and the Truth in Caller ID Act provide the Commission with the authority "to prescribe rules to prevent the unlawful spoofing of caller ID and abuse of NANP resources by all voice service providers[.]" [179] The record reflects that the limitations on third-party authentication we adopt today are necessary to ensure the integrity of and trust in the STIR/SHAKEN ecosystem and will help shield customers from the scourge of illegal robocalls. Adopting rules for third-party authentication practices will also help prevent the fraudulent exploitation of the NANP by ensuring that the parties responsible for implementing STIR/SHAKEN under the Commission's rules remain accountable for meeting the STIR/SHAKEN standards. We thus find that section 251(e) of the Act and the Truth in Caller ID Act provide us with the authority to adopt the foregoing third-party authentication rules.

45. *Implementation and Compliance Measures.* We conclude that the TRACED Act provides additional, independent authority to require providers to obtain an SPC token and sign their calls with their own certificate in order to satisfy a STIR/SHAKEN implementation obligation under the Commission's rules.[180] Congress expressly required the Commission to require voice service providers to implement the STIR/SHAKEN caller ID authentication framework in the TRACED Act.[181] Requiring providers to acquire their own SPC token from and register with the Policy Administrator, obtain a digital certificate from a STIR/SHAKEN Certificate Authority, and sign calls with their digital certificate will better ensure that providers are meeting their responsibilities to properly authenticate calls and comply with the requirements of the ATIS standards. Our third-party authentication rules will therefore help maintain the integrity of the trust and governance structure upon which STIR/SHAKEN relies, as these

[176] 47 U.S.C. §§ 227(e), 251(e); *Sixth Caller ID Authentication Further Notice*, 38 FCC Rcd at 2623-24, para. 109.

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

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

[179] *Sixth Caller ID Authentication Further Notice*, 38 FCC Rcd at 2617-18, para. 93 (citing the *Gateway Provider Order* at 48, para. 117 (quoting *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Fourth Report and Order, 35 FCC Rcd 15221, 15234, para. 37 (2020))); *see Seventh Caller ID Authentication Report and Order*, 38 FCC Rcd at 52426-47, paras. 66-67; *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1909-10, paras. 97-100; *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3260-61, paras. 42, 44.

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

[181] 47 U.S.C. § 227b(b)(1)(A). Consistent with the Commission's prior call blocking and caller ID authentication orders, we find that sections 201(b) and 201(a) of the Act, and the Commission's ancillary authority in section 4(i) of the Act, provide us with additional sources of authority to adopt these robocall mitigation requirements. *See, e.g.*, *Sixth Caller ID Authentication Further Notice*, 38 FCC Rcd at 2617-19, paras. 92-95.

rules will better ensure that providers are held accountable for properly implementing STIR/SHAKEN. Adopting these requirements will thus increase the efficacy and trust of the call authentication framework that the TRACED Act required.

46. We also find that section 251(e) of the Act and the Truth in Caller ID Act also provide us with the authority to adopt the implementation and compliance measures for the third-party authentication rules that we adopt in this *Report and Order*.[182] Specifically, we conclude that section 251(e) of the Act and the Truth in Caller ID Act authorize us to: (1) prohibit any provider from certifying to full or partial implementation in the Robocall Mitigation Database unless they have obtained their own SPC token and sign calls with their own digital certificate; (2) require that any third-party authentication arrangement be memorialized in an agreement between the party with the STIR/SHAKEN implementation obligation under the Commission's rules and the third-party signer; and (3) require the memorialized agreement be in place for as long as any third-party authentication arrangement exists, and that all copies of third-party agreements be maintained for a period of two years from the end or termination of the agreement. As explained above with respect to our third-party authentication rules, these measures will help providers realize the benefits of third-party authentication while providing greater mechanisms for accountability that will ensure that providers are complying with their STIR/SHAKEN implementation obligations. Consequently, we find that these requirements will also prevent the fraudulent abuse of North American Numbering Plan (NANP) resources as directed in section 251(e) of the Act, as well as protect voice service subscribers as directed in the Truth in Caller ID Act by increasing trust in the STIR/SHAKEN standards.

IV. PROCEDURAL MATTERS

47. *Regulatory Flexibility Analysis.* The Regulatory Flexibility Act of 1980, as amended (RFA),[183] requires that an agency prepare a regulatory flexibility analysis for notice and comment rulemakings, unless the agency certifies that "the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities."[184] Accordingly, we have prepared a Final Regulatory Flexibility Analysis (FRFA) concerning the possible impact of the rule changes contained in this *Report and Order* on small entities. The FRFA is set forth in Appendix B.

48. *Paperwork Reduction Act.* This document may contain new or modified information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104-13. All such new or modified information collection requirements will be submitted to the Office of Management and Budget (OMB) for review under the PRA. OMB, the general public, and other Federal agencies will be invited to comment on new or substantively modified information collection requirements contained in this proceeding. Any non-substantive modification to a previously approved information collection will be submitted to OMB for review pursuant to OMB's process for non-substantive changes. In addition, we note that pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, *see* 44 U.S.C. 3506(c)(4), we previously sought specific comment on how the Commission might further reduce the information collection burden for small business concerns with fewer than 25 employees. In this present document, we have assessed the effects of: (1) requiring that any third-party authentication arrangement be memorialized in an agreement between the party with the STIR/SHAKEN implementation obligation under the Commission's rules and the third-party signer; and (2) allowing providers to certify to complete or partial implementation in the Robocall Mitigation Database *only* if they have obtained an SPC token and digital certificate and sign calls with their certificate. We find that small providers have had ample time to develop processes to allow them to respond within the appropriate time and that providers for which this presents a significant burden, either due to their size or for some

[182] 47 U.S.C. §§ 227(e), 251(e); *Sixth Caller ID Authentication Further Notice*, 38 FCC Rcd at 2623-24, para. 109.

[183] 5 U.S.C. §§ 601–612. The RFA has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

[184] 5 U.S.C. §§ 605(b).

other reason, may request a waiver. With respect to any non-substantive modification to a previously approved information collection, such changes are non-substantive and are not give rise to new or substantively modified information collection burdens for small business concerns with fewer than 25 employees pursuant to the Small Business Paperwork Relief Act of 2002.

49. *Congressional Review Act.* The Commission will submit this draft *Eighth Report and Order* to the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, for concurrence as to whether this rule is "major" or "non-major" under the Congressional Review Act, 5 U.S.C. § 804(2). The Commission will send a copy of this *Eighth Report and Order* to Congress and the Government Accountability Office pursuant to 5 U.S.C. § 801(a)(1)(A).

50. *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).

51. *Additional Information*. For further information about the *Eighth Report and Order,* contact Emily Caditz, Attorney Advisor, Competition Policy Division, Wireline Competition Bureau, at Emily.Caditz@fcc.gov, or (202) 418-2268.

V. ORDERING CLAUSES

52. Accordingly, pursuant to sections 4(i), 4(j), 201, 202, 217, 227, 227b, 251(e), 303(r), 403, 501, 502, and 503 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 154(i), 154(j), 201, 202, 214, 217, 227, 227b, 251(e), 303(r), 403, 501, 502, and 503, IT IS ORDERED that this *Eighth Report and Order* IS ADOPTED.

53. IT IS FURTHER ORDERED that part 64 of the Commission's rules IS AMENDED as set forth in Appendix A.

54. IT IS FURTHER ORDERED that, pursuant to sections 1.4(b)(1) and 1.103(a) of the Commission's rules, 47 CFR §§ 1.4(b)(1), 1.103(a), this *Eighth Report and Order*, including the rule revisions and redesignations described in Appendix A, SHALL BE EFFECTIVE 30 days after publication in the Federal Register. The Commission directs the Wireline Competition Bureau to announce the completion of any review by the Office of Management and Budget that the Wireline Competition Bureau determines is required under the Paperwork Reduction Act and the relevant effective date by subsequent public notice.

55. IT IS FURTHER ORDERED that the Office of the Managing Director, Performance & Program Management, SHALL SEND a copy of this *Eighth Report and Order* in a report to Congress and the Government Accountability Office pursuant to the Congressional Review Act, *see* 5 U.S.C. § 801(a)(1)(A).

56. IT IS FURTHER ORDERED that the Commission's Office of the Secretary, SHALL SEND a copy of this *Eighth Report and Order*, including the Final Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

APPENDIX A

Final Rules

The Federal Communications Commission amends Part 64 of Title 47 of the Code of Federal Regulations as follows:

PART 64—MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

Subpart HH—Caller ID Authentication

1. Amend section 64.6301 by revising paragraphs (a) and (b) to read as follows:

§ 64.6301 Caller ID Authentication.

(a) * * *

(1) Obtain an SPC token from the Secure Telephone Identity Policy Administrator and use that token to obtain a Secure Telephone Identity certificate from a Secure Telephone Identity Certificate Authority;

(2) Using the certificate obtained pursuant to paragraph (a)(1) of this section:

(i) Authenticate and verify caller identification information for all SIP calls that exclusively transit its own network;

(ii) Authenticate caller identification information for all SIP calls it originates and that it will exchange with another voice service provider or intermediate provider and, to the extent technically feasible, transmit that call with authenticated caller identification information to the next voice service provider or intermediate provider in the call path; and

(3) * * *

(b) A voice service provider may fulfill its obligations to authenticate caller identification information under paragraph (a)(2) of this section by entering into an agreement with a third-party authentication service, provided that the voice service provider:

(1) Requires the third party to sign all calls using the certificate obtained by the voice service provider in accordance with paragraph (a)(1);

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

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

(i) Specifies the specific tasks that the third-party authenticator will perform on the voice service provider's behalf, and

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

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

(5) Retains a copy of any agreement entered into pursuant to paragraph (b) of this section for a period of two (2) years.

2. Amend section 64.6302 by redesignating paragraphs (a) as (b), (b) as (c), (c) as (d), and (d) as (e), inserting new paragraphs (a) and (f), and revising paragraphs (c), (d), and (e) to read as follows:

§ 64.6302 Caller ID authentication by intermediate providers.

* * * * *

(a) Obtain an SPC token from the Secure Telephone Identity Policy Administrator and use that token to obtain a Secure Telephone Identity certificate from a Secure Telephone Identity Certificate Authority;

* * * * *

(c) Authenticate caller identification information for all calls it receives for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call using the Secure Telephone Identity certificate it received from the Secure Telephone Identity Certificate Authority pursuant to paragraph (a) of this section, except that the intermediate provider is excused from such duty to authenticate if it:

* * * * *

(d) Notwithstanding paragraph (c) of this section, a gateway provider must authenticate caller identification information using the Secure Telephone Identity certificate it received pursuant to paragraph (a) of this section for all calls it receives that use North American Numbering Plan resources that pertain to the United States in the caller ID field and for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call, unless that gateway provider is subject to an applicable extension in § 64.6304.

(e) Notwithstanding paragraph (c) of this section, a non-gateway intermediate provider must authenticate caller identification information using the Secure Telephone Identity certificate it received pursuant to paragraph (a) of this section for all calls it receives directly from an originating provider and for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call, unless that non-gateway intermediate provider is subject to an applicable extension in § 64.6304.

(f) An intermediate provider may fulfill its obligations to authenticate caller ID information under paragraphs (d) and (e) of this section by entering into an agreement with a third-party authentication service, provided that the intermediate provider:

(1) Requires the third party to sign all calls using the certificate obtained by the intermediate provider in accordance with paragraph (a) of this section;

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

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

(i) Specifies the specific tasks that the third-party authenticator will perform on the intermediate provider's behalf, and

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

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

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

3. Amend section 64.6303 by revising paragraphs (b)(1) and (c)(1) to read as follows:

§ 64.6303 Caller ID authentication in non-IP networks.

* * * * *

(b) * * *

(1) Upgrade its entire network to allow for the processing and carrying of SIP calls and fully implement the STIR/SHAKEN framework as required in § 64.6302(d) throughout its network; or

* * * * *

(c) * * *

(1) Upgrade its entire network to allow for the processing and carrying of SIP calls and fully implement the STIR/SHAKEN framework as required in § 64.6302(e) throughout its network; or

* * * * *

4. Amend section 64.6304 by revising paragraph (b) to read as follows:

§ 64.6304 Extension of implementation deadline.

* * * * *

(b) ***Voice service providers, gateway providers, and non-gateway intermediate providers that cannot obtain an SPC token.*** Voice service providers that are incapable of obtaining an SPC token due to Governance Authority policy are exempt from the requirements of § 64.6301 until they are capable of obtaining an SPC token. Gateway providers that are incapable of obtaining an SPC token due to Governance Authority policy are exempt from the requirements of § 64.6302(d) regarding call authentication. Non-gateway intermediate providers that are incapable of obtaining an SPC token due to Governance Authority policy are exempt from the requirements of § 64.6302(e) regarding call authentication.

* * * * *

5. Amend section 64.6305 by revising paragraphs (d)(1)(i), (d)(1)(ii), (e)(1)(i), (e)(1)(ii), (f)(1)(i), and (f)(1)(ii) to read as follows:

§ 64.6305 Robocall Mitigation and Certification.

* * * * *

(d) * * *

(1) * * *

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

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

* * * * *

(e) * * *

(1) * * *

(i) It has fully implemented the STIR/SHAKEN authentication framework across its entire

network and all calls it carries or processes are compliant with § 64.6302;

(ii) It has implemented the STIR/SHAKEN authentication framework on a portion of its network and calls it carries or processes on that portion of its network are compliant with § 64.6302; or

* * * * *

(f) * * *

(1) * * *

(i) It has fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it carries or processes are compliant with § 64.6302;

(ii) It has implemented the STIR/SHAKEN authentication framework on a portion of its network and calls it carries or processes on that portion of its network are compliant with § 64.6302; or

* * * * *

APPENDIX B

Final Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980 (RFA),[1] as amended, an Initial Regulatory Flexibility Analysis (IRFA) was incorporated into the *Call Authentication Trust Anchor Further Notice of Proposed Rulemaking* released in March 2023 (*Sixth Caller ID Authentication Further Notice*).[2] The Federal Communications Commission (Commission) sought written public comment on the proposals in the *Sixth Caller ID Authentication Further Notice*, including comment on the IRFA. The comments received are discussed below. This Final Regulatory Flexibility Analysis (FRFA) conforms to the RFA.[3]

A. Need for, and Objectives of, the Order

2. The *Eighth Report and Order* takes important steps in the fight against illegal robocalls by explicitly authorizing providers to use third-party authentication solutions to comply with their existing STIR/SHAKEN implementation obligations and adopting associated implementation and compliance measures.[4] The decisions we make here protect consumers from unwanted and illegal calls while balancing the legitimate interests of callers placing lawful calls. First, the *Eighth Report and Order* requires a provider that uses a third-party solution for signing calls to satisfy its STIR/SHAKEN implementation obligation under the Commission's rules to make the attestation-level decisions itself, and ensure that its calls are signed with its own certificate, rather than that of a downstream provider or other third party.[5] Second, it requires all providers with a STIR/SHAKEN implementation obligation to: (1) obtain an SPC Token and digital certificate; (2) certify to complete or partial implementation in the Robocall Mitigation Database only if they have obtained an SPC token and digital certificate and ensure their calls are signed with their own certificate; and (3) memorialize any third-party authentication arrangement in an agreement and maintain a record of such agreement(s) for two years from the end or termination of the agreement, alongside certain additional requirements.[6] These guardrails for third-party authentication arrangements will help to ensure providers remain accountable for complying with their STIR/SHAKEN implementation requirements and are transparent regarding their caller ID authentication practices.

B. Summary of Significant Issues Raised by Public Comments in Response to the IRFA

3. Though there were no comments raised that specifically addressed the proposed rules and policies presented in the *Sixth Caller ID Authentication Further Notice* IRFA, the Commission did receive comments addressing the burdens on small providers. There is general agreement that the barriers to and costs associated with obtaining and maintaining SPC tokens and digital certificates are low for small providers.[7] However, one commenter argued that small entities should be allowed six months to

[1] 5 U.S.C. § 603. The RFA, 5 U.S.C. §§ 601-612, was amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Public Law No. 104-121, 110 Stat. 847 (1996).

[2] *Call Authentication Trust Anchor*, WC Docket No. 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd 2573, Appx. C (2023) (*Sixth Caller ID Authentication Report and Order* or *Sixth Caller ID Authentication Further Notice*).

[3] *See* 5 U.S.C. § 604.

[4] *See Eighth Report and Order* Section III.

[5] *See Eighth Report and Order* Section III.A.

[6] *See Eighth Report and Order* Section III.B.

[7] *Eighth Report and Order* at Section III.B.

comply any rules limiting third party authentication,[8] instead of 30 days following publication of the rules in the Federal Register, or 120 days after release of this Report and Order, whichever is later.[9] The Commission notes in the *Eighth Report and Order* that, in practice, the compliance period adopted for the new third party authentication rules is likely to offer a similar compliance period requested by the commenter. The Commission also considered the potential impact of the compliance period and believes this timeline will produce significant benefits, including increased trust in the STIR/SHAKEN framework and the accuracy and trust of A- and B- level attestations.

C. Response to Comments by the Chief Counsel for Advocacy of the Small Business Administration

4. Pursuant to the Small Business Jobs Act of 2010, which amended the RFA, the Commission is required to respond to any comments filed by the Chief Counsel for Advocacy of the Small Business Administration (SBA), and to provide a detailed statement of any change made to the proposed rules as a result of those comments.[10] The Chief Counsel did not file any comments in response to the proposed rules in this proceeding.

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

5. 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 rules adopted herein.[11] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "mall 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]

6. *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

[8] CCA Comments at 13; *see also* TransNexus Reply Comments at 17, n. 63 (arguing in favor of a transition period and citing CCA); NTCA Comments at 3(same).

[9] *Eighth Report and Order* at Section III.B.

[10] 5 U.S.C. § 604(a)(3).

[11] *See* 5 U.S.C. § 603(b)(3).

[12] *See* 5 U.S.C. § 601(6).

[13] *See* 5 U.S.C. § 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] *See* 15 U.S.C. § 632.

[15] 5 U.S.C. § 601(3)-(6).

[16] *See* SBA, Office of Advocacy, "What's New With Small Business?," https://advocacy.sba.gov/wp-content/uploads/2023/03/Whats-New-Infographic-March-2023-508c.pdf (Mar. 2023).

businesses represent 99.9% of all businesses in the United States, which translates to 33.2 million businesses.[17]

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

8. 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

[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. S*ee* 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.

[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.

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]

9. *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.[29] 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.[30] By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry.[31] Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.[32]

10. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[33] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[34] Of this number, 2,964 firms operated with fewer than 250 employees.[35] 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

[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.

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

[30] *Id.*

[31] *Id.*

[32] 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.

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

[34] *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.

[35] *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.

in the provision of fixed local services.[36] Of these providers, the Commission estimates that 4,146 providers have 1,500 or fewer employees.[37] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

11. *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[38] is the closest industry with an SBA small business size standard.[39] Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.[40] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[41] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[42] Of this number, 2,964 firms operated with fewer than 250 employees.[43] 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.[44] Of these providers, the Commission estimates that 4,146 providers have 1,500 or fewer employees.[45] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

12. *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[46] is the closest industry with an SBA small business size standard.[47] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[48] U.S. Census Bureau data for 2017 show that there were 3,054 firms

---

[36] 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.https://docs.fcc.gov/public/attachments/DOC-379181A1.pdf.

[37] *Id.*

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

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

[40] 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.

[41] *Id.*

[42] *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.

[43] *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.

[44] 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.

[45] *Id.*

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

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

[48] *Id.*

in this industry that operated for the entire year.[49] Of this number, 2,964 firms operated with fewer than 250 employees.[50] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 1,227 providers that reported they were incumbent local exchange service providers.[51] Of these providers, the Commission estimates that 929 providers have 1,500 or fewer employees.[52] 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.

13. *Competitive 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 several types of competitive local exchange service providers.[53] Wired Telecommunications Carriers[54] 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.[55] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[56] Of this number, 2,964 firms operated with fewer than 250 employees.[57] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 3,956 providers that reported they were competitive local exchange service providers.[58] Of these providers, the Commission estimates that 3,808 providers have 1,500 or fewer employees.[59] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

14. *Interexchange Carriers (IXCs).* Neither the Commission nor the SBA have developed a small business size standard specifically for Interexchange Carriers. Wired Telecommunications

---

[49] *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.

[50] *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.

[51] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/public/attachments/DOC-379181A1.pdf.

[52] *Id.*

[53] 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.

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

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

[56] *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.

[57] *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.

[58] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[59] *Id.*

Carriers[60] is the closest industry with a SBA small business size standard.[61] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[62] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[63] Of this number, 2,964 firms operated with fewer than 250 employees.[64] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 151 providers that reported they were engaged in the provision of interexchange services. Of these providers, the Commission estimates that 131 providers have 1,500 or fewer employees.[65] 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.

15. *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.[66] For purposes of the Telecom Act Standard, the Commission determined that a cable system operator that serves fewer than 677,000 subscribers, either directly or through affiliates, will meet the definition of a small cable operator based on the cable subscriber count established in a 2001 Public Notice.[67] Based on industry data, only six cable system operators have more than 677, 000 subscribers.[68] 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

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

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

[62] *Id.*

[63] *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.

[64] *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.

[65] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/public/attachments/DOC-379181A1.pdf.

[66] 47 U.S.C. § 543(m)(2).

[67] *FCC Announces New Subscriber Count for the Definition of Small Cable Operator*, Public Notice, 16 FCC Rcd 2225 (CSB 2001) (*2001 Subscriber Count PN*). In this Public Notice, the Commission determined that there were approximately 67.7 million cable subscribers in the United States at that time using the most reliable source publicly available. *Id*. We recognize that the number of cable subscribers changed since then and that the Commission has recently estimated the number of cable subscribers to traditional and telco cable operators to be approximately 58.1 million. *See Communications Marketplace Report*, GN Docket No. 20-60, 2020 Communications Marketplace Report, 36 FCC Rcd 2945, 3049, para. 156 (2020) (*2020 Communications Marketplace Report*). However, because the Commission has not issued a public notice subsequent to the *2001 Subscriber Count PN,* the Commission still relies on the subscriber count threshold established by the *2001 Subscriber Count PN* for purposes of this rule. *See* 47 CFR § 76.901(e)(1).

[68] S&P Global Market Intelligence, S&P Capital IQ Pro, *Top Cable MSOs 12/21Q* (last visited Mar. 14, 2023); S&P Global Market Intelligence, Multichannel Video Subscriptions, Top 10 (April 2022).

million.[69] 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.

16. *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] Of this number, 2,964 firms operated with fewer than 250 employees.[74] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 115 providers that reported they were engaged in the provision of other toll services.[75] Of these providers, the Commission estimates that 113 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.

17. *Wireless Telecommunications Carriers (except Satellite).* This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves.[77] 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.[78] The SBA size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[79] U.S. Census Bureau data for 2017 show that there were 2,893 firms in this industry that operated for the entire year.[80] Of that number, 2,837 firms employed fewer than 250

---

[69] 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).

[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.

[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 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[76] *Id.*

[77] *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.

[78] *Id.*

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

[80] *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.

employees.[81] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 797 providers that reported they were engaged in the provision of wireless services.[82] Of these providers, the Commission estimates that 715 providers have 1,500 or fewer employees.[83] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

18. *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 reselling satellite telecommunications."[84] Satellite telecommunications service providers include satellite and earth station operators. The SBA small business size standard for this industry classifies a business with $35 million or less in annual receipts as small.[85] U.S. Census Bureau data for 2017 show that 275 firms in this industry operated for the entire year.[86] Of this number, 242 firms had revenue of less than $25 million.[87] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 71 providers that reported they were engaged in the provision of satellite telecommunications services.[88] Of these providers, the Commission estimates that approximately 48 providers have 1,500 or fewer employees.[89] Consequently using the SBA's small business size standard, a little more than of these providers can be considered small entities.

19. *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 a SBA small business size standard.[90] 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.[91] Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure.[92] Mobile virtual network operators (MVNOs) are

[81] *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.

[82] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[83] *Id.*

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

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

[86] *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.

[87] *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.

[88] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[89] *Id.*

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

[91] *Id.*

[92] *Id*.

included in this industry.[93] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[94] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[95] Of that number, 1,375 firms operated with fewer than 250 employees.[96] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 293 providers that reported they were engaged in the provision of local resale services.[97] Of these providers, the Commission estimates that 289 providers have 1,500 or fewer employees.[98] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

20. *Toll Resellers*. Neither the Commission nor the SBA have developed a small business size standard specifically for Toll Resellers. Telecommunications Resellers[99] is the closest industry with an 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.[100] Mobile virtual network operators (MVNOs) are included in this industry.[101] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[102] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[103] Of that number, 1,375 firms operated with fewer than 250 employees.[104] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 518 providers that reported they were engaged in the provision of toll services.[105] Of these providers, the Commission

[93] *Id*.

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

[95] *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.

[96] *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.

[97] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[98] *Id.*

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

[100] *Id.*

[101] *Id*.

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

[103] *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.

[104] *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.

[105] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

estimates that 495 providers have 1,500 or fewer employees.[106] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

21. *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[107] 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.[108] Mobile virtual network operators (MVNOs) are included in this industry.[109] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[110] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[111] Of that number, 1,375 firms operated with fewer than 250 employees.[112] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 58 providers that reported they were engaged in the provision of payphone services.[113] Of these providers, the Commission estimates that 57 providers have 1,500 or fewer employees.[114] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

22. *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.[115] 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.[116] 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.[117] The SBA small business size standard for this industry classifies firms with annual receipts of $35 million

---

[106] *Id.*

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

[108] *Id.*

[109] *Id*.

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

[111] *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.

[112] *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.

[113] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[114] *Id.*

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

[116] *Id.*

[117] *Id*.

or less as small.[118] U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year.[119] Of those firms, 1,039 had revenue of less than $25 million.[120] Based on this data, the Commission estimates that the majority of "All Other Telecommunications" firms can be considered small.

E. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements for Small Entities

23. The *Eighth Report and Order* requires providers that choose to engage in third-party authentication to do so subject to certain limitations. These changes affect small and large companies and apply to all the classes of regulated entities identified above. Specifically, the *Eighth Report and Order* authorizes providers to engage third parties to perform the technological act of signing calls, as required by the STIR/SHAKEN standards, provided that providers with a STIR/SHAKEN implementation obligation make all attestation-level decisions for calls authenticated by third-parties,[121] and ensure that all calls authenticated using third-party solutions are signed using the certificate of the provider with the STIR/SHAKEN implementation obligation under the Commission's rules.[122]

24. The *Eighth Report and Order* also adopts implementation and compliance requirements, consistent with the above requirements for third-party authentication. First, providers with a STIR/SHAKEN implementation obligation must acquire their own SPC token and digital certificate. Second, these providers may only certify to complete or partial implementation in the Robocall Mitigation Database if they have obtained an SPC token and digital certificate and sign calls with their certificate, whether by themselves or through a third party.

25. Finally, the *Eighth Report and Order* also adopts a recordkeeping requirement for providers with a STIR/SHAKEN implementation obligation that enter into an arrangement with a third party to authenticate the provider's calls. It requires that any third-party authentication arrangement be memorialized in an agreement between the party with the STIR/SHAKEN implementation obligation under the Commission's rules and the third-party signer, and include information that will help the Commission monitor compliance with our third-party authentication rules.[123] The agreement must specify the specific tasks that the third party will perform on the behalf of the provider with the STIR/SHAKEN implementation obligation, and confirm that the provider with the STIR/SHAKEN implementation obligation will: (1) make all attestation-level decisions for calls signed pursuant to the agreement, and (2) ensure that all calls will be signed using this provider's certificate. Providers may be required to submit a copy of the agreement to the Commission in connection with a review of the provider's compliance with these requirements or an investigation by the Enforcement Bureau. Under this rule, a current agreement must be in place for as long as any third-party authentication arrangement exists, and all copies of third-party agreements must be maintained for a period of two years from the end or termination of the agreement. The record reflects that third-party authentication may particularly benefit small providers that may be burdened by the costs of deploying STIR/SHAKEN in the IP portion of their voice service

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

[119] *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.

[120] *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.

[121] *Eighth Report and Order* at Section III.A.2.

[122] *Eighth Report and Order* at Section III.A.2.

[123] *Eighth Report and Order* at Section III.B.

network. The benefits of the third-party authentication rules adopted in the *Eighth Report and Order* will greatly exceed the minimal costs imposed on small providers.

F. Steps Taken to Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered

26. The RFA requires an agency to provide, "a description of the steps the agency has taken to minimize the significant economic impact on small entities . . . including a statement of the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each one of the other significant alternatives to the rule considered by the agency which affect the impact on small entities was rejected."[124]

27. The *Eighth Report and Order* considered alternatives that may minimize the economic impact on small providers. We authorize providers with a STIR/SHAKEN implementation obligation under the Commission's rules to engage in third-party authentication to comply with that obligation, subject to certain limitations. Our third-party authentication rules thus impose guardrails solely on those providers choosing to make use of a third party to comply with their obligation. Given evidence in the record that third-party authentication may help to reduce costs for small providers, we find that our explicit authorization of the practice, subject to certain guardrails, will enable those providers to accrue those benefits while remaining compliant with the Commission's STIR/SHAKEN implementation obligations.[125] We also find that our action explicitly requiring all providers, regardless of whether they choose to engage in third-party authentication, to obtain an SPC token, use that token to obtain a certificate, and ensure that all calls are signed using that certificate, will be minimally burdensome for small providers, as evidenced by the record.

28. We also adopt an approach to authorizing third-party authentication that will ensure that our requirements do not unduly burden all providers, including small providers. Recognizing arguments in the record that providers could be required to make a number of commercial and network changes to comply with the newly adopted authentication requirements, we grant providers a minimum of 120 days following release of this *Report and Order* to comply with our rules.[126] We considered, but decline to adopt, a six month compliance deadline, as discussed above in section B, based on Commission precedent demonstrating that this timeframe would allow providers sufficient time to make any necessary changes to contracts with downstream providers and that, in practice, delaying the effectiveness of our rules pending OMB approval is likely to offer a similar compliance period. Finally, we also considered and decline to require providers to submit additional information to the Robocall Mitigation Database, which should thus reduce burdens on all providers.[127]

G. Report to Congress

29. The Commission will send a copy of the *Eighth Report and Order*, including this FRFA, in a report to be sent to Congress pursuant to the Congressional Review Act.[128] In addition, the Commission will send a copy of the *Eighth Report and Order*, including this FRFA, to the Chief Counsel for Advocacy of the SBA. A copy of the *Eighth Report and Order* (or summaries thereof) will also be published in the Federal Register.[129]

---

[124] 5 U.S.C. § 604(a)(6).

[125] *Eighth Report and Order* at Section III.A.1.

[126] *Eighth Report and Order* at Section III.B.

[127] *Eighth Report and Order* at Section III.B.

[128] 5 U.S.C. § 801(a)(1)(A).

[129] *Id*. § 604(b).