6712-01

This document is scheduled to be published in the Federal Register on 06/16/2025 and available online at **https://federalregister.gov/d/2025-10998**, and on **https://govinfo.gov**

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 64

[WC Docket No. 17-97; FCC 25-25; FR ID 298605]

Call Authentication Trust Anchor

AGENCY: Federal Communications Commission.

ACTION: Proposed rule.

SUMMARY: In this document, the Federal Communications Commission (Commission) proposes to require that providers that continue to rely on non-IP networks implement non-IP caller ID authentication frameworks, including proposing to develop criteria for evaluating whether non-IP caller ID authentication frameworks are developed and reasonably available, as required by the TRACED Act, and proposing to conclude that certain existing frameworks satisfy those requirements.

DATES: Comments are due on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, and reply comments are due on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: Pursuant to §§ 1.415 and 1.419 of the Commission's rules, 47 CFR 1.415, 1.419, interested parties may file comments and reply comments, identified by WC Docket No. 17-97, by any of the following methods:

- *Electronic Filers:* Comments may be filed electronically using the Internet by accessing the Commission's Electronic Comment Filing System (ECFS): https://www.fcc.gov/ecfs/. *See Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998).
- *Paper Filers*: Parties who choose to file by paper must file an original and one copy of each filing.

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

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).

FOR FURTHER INFORMATION CONTACT: For further information about the Notice of Proposed Rulemaking (*NPRM*), contact Chris Laughlin, Deputy Division Chief, Competition Policy Division, Wireline Competition Bureau, at Chris.Laughlin@fcc.gov. For additional information concerning the Paperwork Reduction Act proposed information collection requirements contained in this document, send an email to PRA@fcc.gov or contact Nicole Ongele at (202) 418-2991.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's *NPRM*, FCC 25-25, in WC Docket No. 17-97, adopted on April 28, 2025, and released on April 29, 2025. The complete text of this document is available for download at https://docs.fcc.gov/public/attachments/FCC-25-25A1.pdf.

Paperwork Reduction Act: The *NPRM* may contain proposed new and revised information

collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and the Office of Management and Budget (OMB) to comment on the information collection requirements described in this document, as required by the Paperwork Reduction Act of 1995, Public Law 104-13. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, see 44 U.S.C. 3506(c)(4), we seek specific comment on how we might further reduce the information collection burden for small business concerns with fewer than 25 employees.

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

Ex Parte Rules: The proceeding the *NPRM* initiates shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules. Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with Section 1.1206(b) of the Commission's rules. In proceedings governed by Section 1.49(f) of the Commission's rules or for which the Commission has made

available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must, when feasible, be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (*e.g.*, .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

Synopsis

I. DISCUSSION

We propose to conclude that effective non-IP caller ID authentication frameworks are developed and reasonably available, and therefore propose to mandate that voice service providers, gateway providers, and non-gateway intermediate providers that have not upgraded their networks to IP implement one or more non-IP caller ID authentication frameworks in their non-IP networks by a date certain. Although § 4(b)(1)(B) of the TRACED Act applies to "provider[s] of voice service" and defines "voice service" to include any service that is "interconnected with the public switched telephone network and that furnishes voice communications to an end user," 47 U.S.C. 227b(a)(2), the Commission has adopted rules that also apply caller ID authentication obligations to gateway providers and non-gateway intermediate providers, relying on its authority under sections 251(e) and 227(e) of the Communications Act. In this item, we propose amending certain rules that are currently applicable to these three categories of providers. For purposes of this item, we will use the general term "providers" to encompass the three categories of providers covered by our caller ID authentication rules, unless otherwise specified. Under the TRACED Act, the Commission must mandate that providers that continue to rely on non-IP technology "take reasonable measures to implement an effective call authentication framework in [their] non-[IP] networks." We propose to conclude that a "call authentication framework" under section 227b(b)(1)(B) consists of any standards or other structures that define how to authenticate calls. This is supported by the TRACED Act's requirement that the Commission mandate implementation of the

STIR/SHAKEN framework, which consists of the STIR and SHAKEN standards. To fulfill this "reasonable measures" requirement, the Commission requires that voice service providers either upgrade their entire network to IP or participate in efforts to develop a non-IP caller ID authentication solution, and said that it "will continue to evaluate whether an effective non-IP caller ID authentication framework emerges." We propose to clarify that the Commission's rules requiring providers with non-IP networks to either upgrade their networks to IP or participate in efforts "to develop a non-IP solution," refer to the development of a "call authentication framework" for non-IP networks under section 227b(b)(1)(B) of the TRACED Act. This is consistent with the Commission's description when it established these rules in the *First Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking* (85 FR 22029, Apr. 21, 2020). There, the Commission made clear that it was implementing the "reasonable measures" requirement in section 227b(b)(1)(B) and it referred to the STIR/SHAKEN framework as a "SIP-based solution." The TRACED Act requires the Commission to "grant a delay of required compliance" with the implementation deadline for non-IP caller ID authentication for voice service providers materially reliant on non-IP networks "until a call authentication protocol has been developed for calls delivered over non-[IP] networks and is reasonably available." The Commission issued this continuing extension in the *Second Caller ID Authentication Report and Order* (85 FR 73360, Nov. 17, 2020). We propose to conclude, under the best reading of the statute, that the phrase "call authentication protocol" in section 227b(b)(5)(B) refers to the technical procedures underlying the standards or other procedures developed for authenticating calls.

In light of the record developed in response to the *Notice of Inquiry* and marketplace developments, we propose to conclude that certain non-IP caller ID authentication frameworks meet the TRACED Act's requirements. This proposed conclusion is based upon the application of criteria we propose to establish for evaluating whether a given framework is first, developed and reasonably available, and second, effective. In turn, we propose to repeal the continuing

extension from caller ID authentication requirements granted to providers that rely on non-IP technology and modify our rule interpreting the TRACED Act's "reasonable measures" requirement to mandate that providers either upgrade their networks to IP or implement non-IP caller ID authentication frameworks. Continuing to allow providers to complete their IP transitions rather than implement non-IP caller ID authentication frameworks enables them to avoid the additional obligation associated with the new requirement. We propose to give providers a reasonable transition period to either complete their IP transitions or implement one or more non-IP caller ID authentication frameworks in their non-IP networks. The Cloud Communications Alliance et al. asks that we seek comment on requiring all providers to convert their networks to IP by a date certain. We support providers' completing their transition to IP, which is a key goal of the Commission, but this proposal is outside the scope of this proceeding. We propose to rely on the TRACED Act and other Commission authority to implement this mandate. Below, we seek comment on these proposals and any other considerations not addressed or specifically asked about herein.

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

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

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

We propose to establish criteria for evaluating whether a given non-IP caller ID authentication framework meets the TRACED Act's requirements. Consistent with the TRACED Act, we propose to apply the criteria in two steps. First, the Commission must

determine whether any frameworks are "developed" and "reasonably available" to meet the TRACED Act's requirements for repealing the continuing extension from caller ID authentication requirements for providers materially reliant on non-IP networks. Second, the Commission must determine whether any such frameworks meet the TRACED Act's requirement to be "effective," in connection with the TRACED Act's requirement that providers "take reasonable measures to implement an effective call authentication framework" in their non-IP networks. We discuss each step below.

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

Considering these definitions, we propose to retain the two criteria the Commission established in the *Second Caller ID Authentication Report and Order* (85 FR 73360, Nov. 17, 2020) for evaluating whether a non-IP caller ID authentication framework satisfies the requirements in the TRACED Act for repealing the continuing extension. Specifically, the Commission determined that a framework must be: (1) "fully developed and finalized by industry standards," and (2) reasonably available such that "the underlying equipment and software necessary to implement such protocol is available on the commercial market." We believe that these criteria reflect a logical and straightforward understanding of the plain

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

For the first criterion, we propose to consider a set of factors to determine whether a framework is "fully developed and finalized by industry standards." Consistent with the *Second Caller ID Authentication Report and Order* (85 FR 73360, Nov. 17, 2020), we propose to evaluate whether a framework is standards-based, including whether "all fundamental aspects of the protocol which enable its effectiveness are standardized by industry." Relatedly, we propose to consider whether the technical elements of the framework have been published and are accessible by providers or vendors that make frameworks commercially available. As further consistent with the *Second Caller ID Authentication Report and Order* (85 FR 73360, Nov. 17, 2020), we propose to consider whether a framework is "ready for implementation," including whether "the protocol is implementable" by providers. We also propose to consider whether the framework is undergoing further development or improvement. Given that Commission rules obligate providers using non-IP network technology to participate in industry efforts to develop a non-IP caller ID authentication solution, we further propose to consider the extent to which industry was involved in the development and approval of a framework and the standards upon which the framework is based. We seek comment on these factors and whether the Commission should consider any other factors when evaluating whether a framework is fully developed and finalized by industry standards.

For the second criterion, we propose to consider a set of factors to determine whether a framework is reasonably available such that "the underlying equipment and software necessary

to implement such protocol is available on the commercial market." We propose to consider evidence that a framework is being marketed or otherwise offered to providers. We also propose to consider evidence that a framework has been implemented by providers or whether providers are waiting for the Commission to mandate frameworks before investing in implementing available frameworks. Additionally, we propose to consider a framework's cost and evidence that the cost can be reasonably borne by providers. We also propose to consider the need to set up a governance structure for a framework to operate and whether any changes to Commission process or rules are necessary to implement such a structure. We seek comment on these factors and whether the Commission should consider any other factors when evaluating whether a framework is reasonably available such that the underlying equipment and software necessary to implement such protocol is available on the commercial market. For instance, should we consider the extent to which a framework can scale to serve a greater number of providers, and if so, how important is this factor if we determine that multiple frameworks meet the TRACED Act's requirements? Similarly, how, if at all, should we consider whether products implementing a framework are only offered by one or a few vendors? Should we consider whether a product relies on proprietary elements not outlined in the framework and the extent to which a provider must use such proprietary elements for the product to work?

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

First, we propose to conclude that for a framework to be "effective" under the TRACED Act, it must at least satisfy the two requirements for repealing the continuing extension in section 4(b)(5)(B) of the TRACED Act (i.e., "developed" and "reasonably available"). Incorporating these two baseline requirements ensures that providers cannot rely on the continuing extension to avoid implementing frameworks the Commission has concluded are effective. This

understanding is also consistent with the *Second Caller ID Authentication Report and Order* (85 FR 73360, Nov. 17, 2020), wherein the Commission said it "will consider a non-IP caller ID authentication framework to be effective only if it is: (1) fully developed and finalized by industry standards; and (2) reasonably available such that the underlying equipment and software necessary to implement such protocol is available on the commercial market." The Commission acknowledged, however, that while these criteria may be necessary for determining whether a solution is effective, they may not be sufficient. Were we to read the TRACED Act as not incorporating the two baseline requirements, the Commission could find that a caller ID authentication framework is effective under section 4(b)(1)(B), but a provider would not have an obligation to implement that framework if the Commission did not also find that the framework satisfies the requirements for removing the continuing extension under section 4(b)(5)(B). Similarly, the Commission could find that a solution is developed and reasonably available, satisfying the requirements for repealing the continuing extension under Section 4(b)(5)(B) and thereby triggering the requirement in section 4(b)(1)(B) for providers to take reasonable measures to implement an effective non-IP caller ID authentication solution. However, a provider would not be able to implement an effective non-IP caller ID authentication solution if the Commission had not determined at the same time or earlier that such a solution exists. The best reading of the statute and its structure therefore ties the continuing extension from complying with the non-IP caller ID authentication obligation to the obligation to implement an effective non-IP caller ID authentication framework. We seek comment on this view and any alternative interpretations.

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

authentication framework must operate to produce the intended result of authenticating calls as described in the applicable standards. That is, when the standards are properly applied under the conditions specified in the standards, the provider is able to authenticate calls. This meaning is consistent with the Commission's understanding of its requirement under the TRACED Act to assess the efficacy of the technologies used for call authentication frameworks implemented under the statute every three years. In its Triennial Report, "the [Wireline Competition Bureau] assesses the efficacy of the STIR/SHAKEN framework herein based on the proposed standard of how well it effectuates the authentication of caller ID information," and its finding "is predicated . . . on STIR/SHAKEN technical standards and protocols being executed as required by the three ATIS standards that establish them." Additionally, we believe that interpreting "effective" to mean more than just "developed" and "reasonably available" is consistent with the canon of statutory construction against surplusage, by ensuring that each word is operative. We do not believe that "effectiveness" requires that a solution operate to authenticate calls in all instances. We believe our understanding is supported by the TRACED Act requirement that the Commission assess the efficacy of implemented call authentication frameworks every three years. Because Congress in the TRACED Act required the Commission to mandate that providers use STIR/SHAKEN in their IP networks, we believe it is reasonable to conclude that Congress deemed STIR/SHAKEN to be an effective caller ID authentication solution. By requiring the Commission to evaluate the efficacy of call authentication frameworks, including STIR/SHAKEN, we believe Congress acknowledged that even effective caller ID authentication solutions—e.g., STIR/SHAKEN—may not result in perfect call authentication in all instances. Indeed, in conducting the triennial review of the efficacy of call authentication technologies, perfection is not the standard the Commission itself has applied to STIR/SHAKEN. We seek comment on our proposed understanding of "effective," and on any alternative interpretations.

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

In particular, we invite commenters to address whether we must consider factors concerning the feasibility for providers to implement frameworks. For example, must we evaluate the need for providers to enter into bilateral or multilateral agreements to implement certain frameworks? Are we required to consider the extent to which a framework will only work for providers using certain network equipment or facilities, or whether a provider would need to make changes or upgrades to their existing network before implementing a framework? Must we take into account a framework's implementation costs and burdens or its cost effectiveness in determining whether it is effective? If so, how should the Commission evaluate cost-effectiveness? Can a framework still be considered effective if it is not cost-effective for all providers or the cost is burdensome for some providers to implement? Are there other implementation challenges we must or should consider? We note that the Commission recently required all providers with a STIR/SHAKEN obligation to obtain an STI certificate.

We also invite commenters to explain whether we are required to evaluate factors concerning the inherent features and functions of each framework. To what extent must we consider technical limitations of a framework that otherwise authenticates calls as described by the standard? For example, must we evaluate whether and the extent to which a framework's ability to authenticate calls provides functional parity with STIR/SHAKEN? Is it necessary to consider whether a framework is technically futureproof, including whether it would continue to function and be able to incorporate additional functionality as providers make changes and upgrades to their networks? To what extent must we consider the security of a framework and whether it may enable bad actors to transmit false authentication information or otherwise undermine the effectiveness of STIR/SHAKEN? Must we consider a framework's resilience to Denial of Service attacks aimed at different components of the framework? Are we required to

consider whether there are single-points-of-failure embedded within the design of certain frameworks and their impact? We also seek comment on whether we must consider any impacts that these frameworks' implementation may have on E911 and emergency services, and their bearing on the frameworks' effectiveness. ATIS released two reports concerning the impact of non-IP standards on 911 services. The first, ATIS-0500046, Analysis of Non-IP Call Authentication Mechanisms in Support of Emergency Services, "discusses call authentication [including In-Band Authentication and Out-of-Band Multiple STI-CPS Authentication] in the context of emergency services" using "legacy" E911, while ATIS-1000097.v003, Appendix B describes a broader set of issues related to all three non-IP standards and their interaction with different types of 911 systems.

We seek comment on whether the best reading of the statute requires us to take into account any other factors when evaluating a framework's effectiveness. For example, in the *Second Caller ID Authentication Report and Order* (85 FR 73360, Nov. 17, 2020), the Commission said that "significant industry consensus is an important predicate to deeming a non-IP framework 'effective,' given that cross-network exchange of authenticated caller ID information is a central component to caller ID authentication." Must we consider whether and the extent to which industry consensus exists on the merits of a framework and the standards upon which the framework is based? Does presence or lack of consensus bear on a framework's effectiveness? If so, how should we evaluate whether there is sufficient consensus? Should we consider whether any industry participants are withholding such consensus for reasons other than the effectiveness of the framework, such as an unwillingness to compromise on which frameworks are best or a desire to avoid having to invest in implementing a framework?

2. Evaluation of Non-IP Caller ID Authentication Frameworks

In this section, we propose to conclude that frameworks using two of the three ATIS-adopted non-IP caller ID authentication standards satisfy the TRACED Act's requirement using the Commission's proposed criteria for evaluating non-IP frameworks. Specifically, we propose

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

a) Developed and Reasonably Available Frameworks.

We propose to conclude that frameworks using all three ATIS non-IP standards meet the first criterion for repealing the continuing extension because they are "fully developed and finalized by industry standards." Specifically, we propose to conclude that because ATIS is a well-established standards development organization, frameworks using all three standards are standards-based and their fundamental aspects are standardized. We propose to recognize that the technical elements of all three frameworks have been published and are accessible by providers and vendors that make frameworks commercially available. We further propose to conclude that there is consensus within the industry that all three frameworks are developed, given that final versions of all three standards have been approved by ATIS, an industry standards organization. Additionally, we propose to conclude that because record evidence indicates that both In-Band Authentication and Out-of-Band Multiple STI-CPS Authentication have been implemented by at least some providers, they qualify as fully developed and finalized. We seek comment on these proposed conclusions. We also seek comment on whether Out-of-Band Agreed STI-CPS Authentication is ready for implementation, and whether it has been implemented by any providers. We seek comment on whether there are any ongoing efforts to

further develop or improve any of the standards either inside or outside of ATIS. WTA explained in 2022 that it believes that "there is no open or ongoing ATIS proceeding regarding further refinement or revision of the In-Band standard . . . ." If there are ongoing efforts to further develop or improve any of the standards, what are the substance of such revisions and what problems or shortcomings in the standards are they designed to solve? What progress is industry making to complete any further development? Have all fundamental aspects of each standard which enable their effectiveness been standardized by industry? Are there any other factors we should consider when evaluating whether each of the standards is fully developed and finalized by industry standards?

Next, we propose to conclude that frameworks using In-Band Authentication and Out-of-Band Multiple STI-CPS Authentication are reasonably available such that the underlying equipment and software necessary to implement those frameworks are commercially available, and therefore meet the second criterion for repealing the continuing extension. Record evidence (from December 2022 and January 2023) indicates that frameworks using In-Band Authentication and Out-of-Band Multiple STI-CPS Authentication have been implemented by some providers, which suggests that the necessary equipment and software is commercially available. For instance, we note that TelcoBridges explained it "offers technology solutions for both" standards. Regarding In-Band Authentication, NCTA noted that at least two providers "have successfully demonstrated an in-band solution." With respect to Out-of-Band Multiple STI-CPS Authentication, the Cloud Communications Alliance stated that Neustar "offers an out-of-band solution" and its members "have undertaken the expense of enabling out-of-band solutions for their networks. . . ." TransNexus explained that it knows "of about 50 providers currently using Out-of-Band [Multiple STI-CPS]," and appears to continue to offer an out-of-band solution, as does TransUnion. We seek additional information concerning the commercial availability, marketing, and deployment of frameworks based on these standards. Have there been increases or decreases in deployments of such frameworks since the *Notice of Inquiry*? If

so, are such increases or decreases relevant to their "commercial availability"? We also seek comment on whether some or all current in-band and out-of-band deployments rely on proprietary elements not outlined in the standard and whether the use of or need to use proprietary elements bear on whether we should conclude that frameworks based on either standard are reasonably available. Are any of the frameworks or associated standards subject to patents or other intellectual property restrictions? We propose to conclude that the governance structure required by Out-of-Band Multiple STI-CPS Authentication does not affect our proposed conclusion that frameworks using this standard are reasonably available. We believe that existing governance structures utilized under STIR/SHAKEN can be expanded to fulfill Out-of-Band Multiple STI-CPS Authentication requirements without unreasonable burden on the existing governance structures or the Commission. We seek comment on this proposed conclusion. Additionally, we seek comment on the cost and burdens of implementing these frameworks, including whether they can be reasonably borne by providers and their relevance to a framework's "commercial availability." Does the reasonability depend on the size and type of provider and structure and location of its network? How many voice service providers with 100,000 or fewer voice service subscriber lines have implemented frameworks using each of these standards? If a framework is not cost effective in some cases or for some providers, can it still be considered reasonably available? Should the Commission consider any other factors when evaluating whether a framework is reasonably available?

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

long will it take? Do vendors and providers believe that it will be easier or more difficult than the other non-IP standards to implement frameworks based on Out-of-Band Agreed STI-CPS Authentication in their equipment and networks? If frameworks based on Out-of-Band Agreed STI-CPS Authentication have been developed, are there any proprietary elements to any such frameworks? Is the standard or any associated frameworks subject to patents or other intellectual property restrictions? Are frameworks being offered and marketed to providers? What are the costs of these frameworks and can those costs be reasonably borne by providers?

b) Effective Frameworks

We propose to conclude that frameworks using In-Band Authentication and Out-of-Band Multiple STI-CPS Authentication satisfy the proposed criteria for determining whether a non-IP caller ID authentication framework is effective. First, we propose to conclude that these frameworks satisfy the first two criteria of effectiveness—developed and reasonably available—based on our proposed conclusion above that they satisfy these TRACED Act requirements. Second, we propose to conclude that these frameworks are effective under the plain meaning of the TRACED Act because they operate to produce the intended result of authenticating calls as described in the applicable standard. We believe that record evidence of deployments of In-Band Authentication and Out-of-Band Multiple STI-CPS Authentication frameworks in the marketplace are *prima facie* evidence that these frameworks are in fact operating to authenticate calls as described in each standard, as providers would otherwise be unlikely to implement them in the absence of a mandate. We also note record evidence indicating that the two standards are interoperable, i.e., that they will continue to operate to authenticate calls even if other providers in the call path are using frameworks based on the other standard. We seek comment on our proposed conclusion. Do commenters have additional evidence concerning testing or real-world deployments showing whether these frameworks, when implemented as designed, successfully authenticate calls? What is the experience of those who have implemented these two types of frameworks? Are there any other bases for concluding that frameworks using In-Band

Authentication and Out-of-Band Multiple STI-CPS Authentication do or do not authenticate calls as intended under the standards based on the plain meaning of the TRACED Act?

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

Other non-IP caller ID Authentication frameworks. We seek comment on whether there are any other non-IP frameworks that we should evaluate using our criteria. For instance, are there any other standards either ratified or in development by ATIS, IETF, or any other standards organization that we should consider? Are there proprietary frameworks that we should consider or be aware of that might meet the TRACED Act requirements? For example, the Commission noted in the *Notice of Inquiry* that AB Handshake has previously submitted a proprietary solution for consideration. At least two commenters explained that the AB Handshake solution, "meets the Commission's standards for effectiveness." Should we consider AB Handshake or other providers' solutions? We also note that IETF appears to be developing a new out-of-band

standard. We seek comment on its development status and how it may differ from the three ATIS standards discussed above. If there are other frameworks that commenters believe we should consider, we seek comment on the application of the criteria and factors described above to those frameworks, as well as other considerations we should take into account when evaluating the frameworks. Some commenters responding to the *Notice of Inquiry* discussed alternative IP voice traffic delivery methods, such as transmission over the public Internet. We do not believe these alternatives bear on whether non-IP caller ID authentication solutions meet the TRACED Act's requirements and warrant mandating non-IP caller ID authentication, but commenters are invited to provide information otherwise.

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

B. Mandating Implementation of Non-IP Caller ID Authentication

We propose to conclude that the development and availability of effective non-IP caller ID authentication frameworks warrants mandating that providers that continue to maintain non-

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

Repealing the continuing extension. In connection with our proposed determination above that non-IP caller ID authentication frameworks are developed and reasonably available, we propose to repeal the continuing extension from robocall mitigation obligations granted to providers that rely on non-IP technology. Section 4(b)(5)(B) of the TRACED Act requires the Commission to "grant a delay of required compliance" with the implementation deadline for non-IP caller ID authentication for voice service providers materially reliant on non-IP networks "until a call authentication protocol has been developed for calls delivered over non-[IP] networks and is reasonably available." The Commission issued this continuing extension in the *Second Caller ID Authentication Report and Order* (85 FR 73360, Nov. 17, 2020). Providers reliant on non-IP technology therefore "are deemed subject to a continuing extension" under the Commission's rules. As explained above, we believe that frameworks based on certain ATIS standards qualify as developed and reasonably available and therefore justify repeal of the continuing extension. Are there other factors the Commission must or should consider before repealing the continuing extension? If the Commission determines that non-IP caller ID

authentication frameworks have been developed and are reasonably available, does it have any discretion under the TRACED Act to maintain the continuing extension?

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

Modifying the "reasonable measures" rule. In connection with our proposed determination above that available non-IP caller ID authentication frameworks are effective, we propose to modify Section 64.6303 of our rules, which implements the TRACED Act's "reasonable measures" requirement, to mandate that providers either upgrade their networks to IP or implement one or more non-IP caller ID authentication frameworks. Under section 4(b)(1)(B) of the TRACED Act, voice service providers must "take reasonable measures to implement an effective call authentication framework in [their] non-internet protocol networks." In the *Second Caller ID Authentication Report and Order* (85 FR 73360, Nov. 17, 2020), the Commission concluded that "[a] voice service provider satisfies this obligation by either (1) completely upgrading its non-IP networks to IP and implementing the STIR/SHAKEN authentication framework on its entire network, or (2) working to develop a non-IP authentication solution." At the time, the Commission stated that "[i]f and when we identify an

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

We seek comment on these proposals and their implications. What are the costs and benefits of requiring providers to either complete their IP transitions or implement a non-IP

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

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

C. Compliance Deadline

We propose a two-year timeline for providers that continue to maintain non-IP infrastructure to either complete their IP transitions or fully implement one or more of the available non-IP caller ID authentication frameworks in their non-IP networks. Under our

proposal, the two-year timeline would commence from the effective date of any implementing rules we adopt. We seek comment on this proposal. In the *Notice of Inquiry*, the Commission sought comment on a reasonable implementation timeline for deployment of one or both non-IP caller ID authentication frameworks. Several commenters agreed the Commission should set a deadline for providers to implement a non-IP framework if they have not completed their IP transition by that date, and others proposed a specific date, which has since passed.

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

Specifically, we ask that commenters address how any remaining technical, financial, or other obstacles may affect the time needed to implement any of the discussed non-IP caller ID authentication frameworks. We note that the Commission previously adopted compliance timelines of roughly 15 months for voice service providers, 13 months for gateway providers, and 10 months for certain non-gateway intermediate providers to implement STIR/SHAKEN in

their IP networks, and providers were generally able to meet those deadlines. Our rules adopted pursuant to the TRACED Act granted certain providers extensions from this deadline and permitted providers to request exemptions. Given those compliance timelines, would the significantly longer two-year compliance timeline we propose here be necessary to reasonably account for any additional burdens providers may face in implementing one of the non-IP frameworks? Both TransNexus and TelcoBridges say that deployment time depends on the existing network capabilities, but can be as short as a few days. Is a shorter timeline warranted given that some providers have already begun to implement one or both of the commercially available non-IP frameworks? Is two years adequate time for providers to make adjustments to any existing contractual arrangements that may be impacted by implementing one or more of the non-IP frameworks? Are there any technical or operational hurdles unique to the non-IP caller ID authentication frameworks that require additional time for providers to comply? If commenters believe that more or less time is needed to implement one or more of the commercially available non-IP caller ID authentication frameworks, they should discuss specific reasons why our proposed two-year timeline is insufficient or too long, propose an alternative timeline, and provide detail on why their proposed alternative is appropriate.

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

small providers? Do certain classes of small providers, such as rural or intermediate providers, face unique challenges to implementing non-IP caller ID authentication? For purposes of the STIR/SHAKEN implementation extension for small voice service providers, the Commission considers a "small voice service provider" to be "a provider that has 100,000 or fewer voice service subscriber lines (counting the total of all business and residential fixed subscriber lines and mobile phones and aggregated over all of the provider's affiliates)." Would a similar approach be appropriate in the non-IP caller ID authentication context, or should we adopt a different threshold? If so, why? Are there certain gateway and non-gateway intermediate providers that warrant an extension, such that the extension should not be tied to the number of subscriber lines? If so, how should we determine the class or classes of such providers subject to an extension? If we grant an extension to some providers, how much additional time would be appropriate in light of the public interest in promptly closing the non-IP caller ID authentication gap? How would any extension account for the importance of ubiquitous caller ID authentication? Instead of a categorical approach, should we instead rely on individualized waiver requests pursuant to the Commission's longstanding waiver standard? The Commission may exercise its discretion to waive a rule where the particular facts at issue make strict compliance inconsistent with the public interest. In considering whether to grant a waiver, the Commission may take into account considerations of hardship, equity, or more effective implementation of overall policy on an individual basis.

We invite commenters to address how our proposed compliance timeline relates to providers' efforts to transition their networks to IP technology. In the *Notice of Inquiry*, we sought comment on the status of providers' efforts to fully transition their networks to all-IP technology and the effect that a non-IP caller ID authentication requirement would have on the IP transition's progress. We seek additional comment on this issue in light of our proposed mandate of non-IP caller ID authentication and the Commission's recent efforts to ease regulatory barriers to IP transitions. For example, should any compliance timeline take into

account providers' assertions about the time it would take to transition their networks to all IP? Do providers opting to fully upgrade their networks to IP face unique challenges that counsel for a longer compliance timeline? Would two years give providers adequate time to adjust existing contractual arrangements, or to negotiate new ones, as a result of upgrading their networks to all IP? What, if any, technical or financial circumstances affect providers' ability to transition to all-IP technology that our proposed timeline does not account for? To the extent that providers believe that transitioning their networks to IP warrants a longer compliance timeline, they should propose a specific alternative compliance timeline, and discuss in detail the reasons that such providers need additional time to comply.

D. Cost-Benefit Considerations

We seek comment on the costs and benefits associated with requiring providers to implement a non-IP caller ID authentication framework. As explained above, the TRACED Act requires that the Commission provide a continuing extension from implementing a non-IP caller ID authentication framework to providers materially reliant on non-IP networks "until a call authentication protocol has been developed for calls delivered over non-[IP] networks and is reasonably available." Thereafter, providers must take reasonable measures to implement an effective caller ID authentication framework in their non-IP networks, which we propose to mean implementing a non-IP caller ID authentication framework for providers that continue to rely on non-IP networks by the end of the proposed two-year transition period. Because implementation of a non-IP framework and its accompanying costs must be incurred at some point, we propose to focus our cost-effectiveness analysis on timing, rather than the implementation requirement. Under that proposed focus, we believe the Commission must weigh the costs and benefits of imminent action versus further delay.

We believe that the potential cost of mandating one or more non-IP caller ID authentication frameworks at a particular point in time is that a more effective or efficient framework meeting the TRACED Act's requirements could become available after providers

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

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

E. Legal Authority

We seek comment on the Commission's legal authority to adopt the proposals outlined above. In particular, we propose that the TRACED Act, the Truth in Caller ID Act, and section

251(e) of the Communications Act provide the Commission with ample authority to adopt the rules implementing the proposals discussed herein. We note that the Commission has long invoked these same statutory provisions to adopt caller ID authentication obligations. For example, in the *Second Caller ID Authentication Report and Order* (85 FR 73360, Nov. 17, 2020), the Commission found that the text of the TRACED Act provided authority to adopt rules implementing Section 4(b)(1)(B) for originating and terminating providers, while section 251(e) and the Truth in Caller ID Act provided further, independent sources of authority for rules applying to intermediate providers, as well as originating and terminating providers. We seek comment on this proposal, and on any alternative sources of legal authority upon which we could rely.

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

In addition to its authority under the TRACED Act, the Commission has consistently found independent authority for caller ID authentication requirements, including those applicable to intermediate providers, in section 251(e) of the Act and the Truth in Caller ID Act. As the Commission explained in the *First Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking* (85 FR 22029, Apr. 21, 2020), section 251(e) provides the Commission with exclusive, independent jurisdiction over numbering issues in the United States

and "enables us to act flexibly and expeditiously with regard to important numbering matters[,]" including "[w]hen bad actors unlawfully spoof the caller ID that appears on a subscriber's phone[.]" The Truth in Caller ID Act provides us with further authority to adopt rules that are "necessary to . . . protect voice service subscribers from scammers and bad actors." Beginning with the *Second Caller ID Authentication Report and Order* (85 FR 73360, Nov. 17, 2020), the Commission has repeatedly found both provisions to provide authority to impose caller ID authentication obligations on voice service providers and intermediate providers alike. We seek comment on whether these provisions grant us sufficient authority to require intermediate providers to adopt a non-IP caller ID authentication framework.

II. INITIAL REGULATORY FLEXIBILITY ANALYSIS

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

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

To protect the American public from illegally spoofed robocalls, the *NPRM* seeks comment on proposals that would address gaps in the STIR/SHAKEN caller ID authentication framework, which works to provide trust that a calling party is who they claim to be. Although the STIR/SHAKEN framework mandated by Congress is effective, it relies on IP technology, resulting in critical information being stripped out when a call path includes non-IP networks. To address this problem, the Commission proposes to: conclude that effective non-IP caller ID

authentication frameworks have been developed and are reasonably available; repeal the continuing extension from caller ID authentication requirements granted to providers that rely on non-IP technology; modify our rules concerning providers' obligation to take reasonable measures to implement effective caller ID authentication in their non-IP networks to require that providers implement one or more non-IP caller ID authentication frameworks; and require that providers certify in the Robocall Mitigation Database that they have implemented a non-IP caller ID authentication framework. The Commission proposes to give providers a two-year transition period to implement one or more non-IP caller ID authentication frameworks in their non-IP networks, with a possible extension of this transition period for providers with 100,000 or fewer voice service subscriber lines. The Commission proposes to rely on the TRACED Act and other Commission authority to implement these mandates.

B. Legal Basis

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

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

The RFA directs agencies to provide a description of and, where feasible, an estimate of the number of small entities that may be affected by the proposed rules, if adopted. The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction." In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act." 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.

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. First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, according to data from the SBA's Office of Advocacy, in general a small business is an independent business having fewer than 500 employees. These types of small businesses represent 99.9% of all businesses in the United States, which translates to 34.75 million businesses.

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." 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. 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.

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." U.S. Census Bureau data from the 2022 Census of Governments indicate there were 90,837 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States. Of this number, there were 36,845 general purpose governments (county, municipal, and town or township) with populations of less than 50,000 and 11,879 special purpose governments (independent school districts) with enrollment populations of less than 50,000. 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."

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." For purposes of the Telecom Act Standard, the Commission determined that a cable system operator that serves fewer than 498,000 subscribers, either directly or through affiliates, will meet the definition of a small cable operator. Based on industry data, only six cable system operators have more than 498,000 subscribers. Accordingly, the Commission estimates that the majority of cable system operators are small under this size standard. We note however, that the Commission neither requests nor collects information on whether cable system operators are affiliated with entities whose gross annual revenues exceed $250 million. 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.

Competitive Local Exchange Carriers (CLECs). Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. Providers of these services include several types of competitive local exchange service providers. Wired Telecommunications Carriers is the closest industry with an 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. U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 3,378 providers that reported they were competitive local service providers. Of these providers, the Commission estimates that 3,230 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

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 is the closest industry with an 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. U.S. Census Bureau data for 2017 show that there were 3,054 firms in this industry that operated for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 1,212 providers that reported they were incumbent local exchange service providers. Of these providers, the Commission estimates that 916 providers have 1,500 or fewer employees. 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.

Interexchange Carriers (IXCs). Neither the Commission nor the SBA have developed a small business size standard specifically for Interexchange Carriers. Wired Telecommunications Carriers is the closest industry with an 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. U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 127 providers that reported they were engaged in the provision of interexchange services. Of these providers, the Commission estimates that 109 providers have 1,500 or fewer employees. 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.

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

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 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. Mobile virtual network operators (MVNOs) are included in this industry. The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year. Of that number, 1,375 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 207 providers that reported they were engaged in the provision of local resale services. Of these providers, the Commission estimates that 202 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size

standard, most of these providers can be considered small entities.

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 is the closest industry with an 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. U.S. Census Bureau data for 2017 show that there were 3,054 firms in this industry that operated for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 90 providers that reported they were engaged in the provision of other toll services. Of these providers, the Commission estimates that 87 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

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 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. MVNOs are included in this industry. The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year. Of that number, 1,375 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring

Report, as of December 31, 2021, there were 62 providers that reported they were engaged in the provision of prepaid card services. Of these providers, the Commission estimates that 61 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

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

Toll Resellers. Neither the Commission nor the SBA have developed a small business size standard specifically for Toll Resellers. Telecommunications Resellers 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. MVNOs are included in this industry. The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year. Of that number, 1,375 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 457 providers that reported they were engaged in the provision of toll services. Of these providers, the Commission estimates that 438 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

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. 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 Voice over Internet Protocol (VoIP) services, wired (cable) audio and video programming distribution, and wired broadband Internet services. By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry. Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.

The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 4,590 providers

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

Wireless Telecommunications Carriers (except Satellite). This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves. 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. The SBA size standard for this industry classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that there were 2,893 firms in this industry that operated for the entire year. Of that number, 2,837 firms employed fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 594 providers that reported they were engaged in the provision of wireless services. Of these providers, the Commission estimates that 511 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

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. 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. Providers of Internet services (e.g., dial-up ISPs) or VoIP services, via client-supplied telecommunications connections are also included in this industry. The SBA small business size standard for this industry classifies firms with annual receipts of $40 million or less as small. U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year. Of those firms, 1,039

had revenue of less than $25 million. Based on this data, the Commission estimates that the majority of "All Other Telecommunications" firms can be considered small.

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

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

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

The *NPRM* seeks comment on the costs and benefits of its proposals and inquiries, which we anticipate will help the Commission identify and evaluate relevant compliance matters for

small entities, including compliance costs and other burdens that may result from the proposals and inquiries. Specifically, the Commission proposes an analysis of the costs and benefits with respect to the timing of any mandate in the *NPRM* and seeks comment thereon. Further, the *NPRM* specifically seeks comment on the costs of requiring providers to either implement a non-IP caller ID authentication framework or upgrade their networks to all IP, the costs for providers to actually implement a non-IP caller ID authentication framework in their networks, and the costs for the providers to certify that they have implemented a non-IP caller ID authentication framework in the Robocall Mitigation Database. The *NPRM* also seeks comment on how many small voice service providers have implemented each of these frameworks. We seek comment from small and other entities about these costs.

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

The RFA directs agencies to provide a description of any significant alternatives to the proposed rules that would accomplish the stated objectives of applicable statutes, and minimize any significant economic impact on small entities. The discussion is required to include alternatives such as: (1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the rule for such small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof, for such small entities.

The *NPRM* seeks comment on proposals and alternatives that may have a significant impact on small entities. In particular, it seeks comment on the benefits and burdens of requiring all providers, including small and other entities, to implement a non-IP caller ID authentication framework. The *NPRM* specifically asks about frameworks based on standards promulgated by ATIS, as well as whether alternative non-IP caller ID authentication frameworks exist that satisfy the TRACED Act's requirements to first, be "developed" and "reasonably available," and

second, be "effective." This includes whether the Commission should use proposed criteria to evaluate whether non-IP caller ID authentication frameworks meet the TRACED Act's requirements, or if any alternative criteria for how to evaluate any such frameworks should be considered. Additionally, the *NPRM* seeks comment on whether providers, including small and other entities, possess the resources necessary to implement these changes in the proposed two-year timeframe. The *NPRM* also solicits comment on whether additional time may be needed to implement these frameworks, or whether extensions should be granted for certain providers including providers that have 100,000 or fewer voice service subscriber lines. Finally, the Commission seeks comment on the proposed analysis of the costs and benefits with respect to the timing of any mandate and any alternatives that may avoid or minimize those costs.

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

None.

III. ORDERING CLAUSES

Accordingly, pursuant to sections 4(i), 4(j), 201, 202, 217, 227, 227b, 251(e), 303(r), and 403 of the Communications Act of 1934, as amended, 47 U.S.C. 154(i), 154(j), 201, 202, 217, 227, 227b, 251(e), 303(r), and 403, the *NPRM* IS ADOPTED.

IT IS FURTHER ORDERED that the Commission's Office of the Secretary, SHALL SEND a copy of the *NPRM*, including the Initial Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

List of Subjects in 47 CFR Part 64

Carrier equipment, Communications common carriers, Reporting and recordkeeping requirements, Telecommunications, Telephone.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch,
Secretary.

Proposed Rules

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

PART 64 – MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

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

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

Subpart HH – Caller ID Authentication

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

§ 64.6300 Definitions.

* * * * *

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

* * * * *

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

§ 64.6302 Caller ID authentication by intermediate providers.

* * * * *

(f) * * *

* * * * *

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

* * * * *

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

§ 64.6303 Caller ID authentication in non-IP networks.

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

* * * * *

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

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

* * * * *

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

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

* * * * *

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

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

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

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

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

§ 64.6304 Extension of implementation deadline.

(a) *Small voice service providers.*

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

* * * * *

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

§ 64.6305 Robocall mitigation and certification.

* * * * *

(d) * * *

* * * * *

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

* * * * *

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

* * * * *

(5) * * *

* * * * *

(vi) * * *

* * * * *

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

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

(viii) * * *

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

* * * * *

(e) * * *

* * * * *

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

* * * * *

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

* * * * *

(5) * * *

* * * * *

(vi) * * *

* * * * *

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

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

(viii) * * *

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

* * * * *

(f) * * *

* * * * *

(2) A non-gateway intermediate provider relying on non-Internet Protocol networks shall certify that it has implemented one or more effective non-IP caller ID authentication

frameworks in its non-Internet Protocol networks and all calls it carries or processes its non-Internet Protocol networks are compliant with § 64.6303(c).

* * * * *

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

* * * * *

(5) * * *

* * * * *

(vi) * * *

* * * * *

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

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

(viii) * * *

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

* * * * *

7. Remove and reserve § 64.6306.

§ 64.6306 [Removed and Reserved]

[FR Doc. 2025-10998 Filed: 6/13/2025 8:45 am; Publication Date: 6/16/2025]