coordination between adjacent operations, but 3.7 GHz Service licensees and TT&C earth station operators would be expected to cooperate in good faith and make reasonable efforts to anticipate and resolve technical problems that may inhibit effective and efficient use of the spectrum; and (3) TT&C operators would be expected to make available pertinent technical information about their systems upon request by the 3.7 GHz Service licensees, and licensees of stations suffering or causing harmful interference would be expected to cooperate and resolve the problem by mutually satisfactory arrangements.

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

164. 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.''

165. In formulating its request for comments, the Commission considered alternatives addressing the economic impact of its proposals on small entities, should they be adopted. In the *NPRM,* the Commission broadly proposes to reconfigure the Upper C-band for more intensive, next-generation wireless use by generally deploying the procedures used in—and the lessons learned from—the successful similar transition of the Lower C-band. Throughout that proceeding, the Commission contemplated how its adopted rules would uniquely affect small entities and calibrated its determinations accordingly. The approach taken towards considering the effect of our rules towards small entities in that proceeding largely informs our process in this one. For example, we consider the potential economic hardship or compliance burdens to small entities with respect to the information collection, such as whether they would require certain accommodations or additional time to comply. We seek comment from small entities as to whether these entities face any special or unique concerns regarding this issue. Similarly, in developing its proposals, the Commission considers the effect of modifications that could be made to our rules regarding administrative processes that would reduce the economic impacts of proposed rule changes on small entities. By seeking comment specifically targeting effects on small entities, the Commission will obtain the data required to consider the approach that will be most cost-effective and minimize the economic impact on small entities while also fulfilling the Commission's statutory mandate.

166. Specifically, the *NPRM* proposes to adopt 15-year license terms for new licenses in the Upper C-band. If adopted, small entities should once again benefit from the opportunity for long-term operational certainty and a longer period to develop innovative services. The *NPRM* also contemplates and seeks comment on potential issues that small entities might face in meeting the proposed performance requirements for new Upper C-band licensees. To that end, the *NPRM* inquires whether our proposed point-to-multipoint coverage and service benchmarks might necessitate that we grant small entities certain accommodations or additional time to comply. Similarly, the *NPRM* considers the impact of, and seeks comment on, whether small entities should be offered additional time to fulfill proposed compliance procedures. Finally, the proposed competitive bidding procedures would implement familiar designated entity preferences in an auction of Upper C-band licenses. The *NPRM* proposes to adopt bidding credits for small and very small businesses, and to adopt a rural service provider credit.

167. The Commission finds an overriding public interest in encouraging investment in wireless networks, facilitating access to scarce spectrum resources, and promoting the rapid development of mobile services to Americans. All licensees, including small entities, play a crucial role in achieving these goals. Therefore, the *NPRM* seeks comment on alternative obligations, timing for implementation, and other measures that could accommodate the needs and resources of small entities. The Commission will carefully consider the effects of its proposals on small entities before adopting final rules in this proceeding.

F. Federal Rules That May Duplicate, Overlap, or Conflict With the Proposed Rules

168. None. This proposed rule is not duplicative, nor does it overlap or conflict, with any other federal rules.

V. Ordering Clauses

169. *It Is Ordered,* pursuant to Sections 1, 2, 4(i), 301, 302(a), 303, 304, 307, 309, 316, and 403 of the Communications Act of 1934, as amended, 47 U.S.C. 151, 152, 154(i), 301, 302(a), 303, 304, 307, 309, 316 and 403, and by Section 40002 of the OBBB Act, that this Notice of Proposed Rulemaking *Is Hereby Adopted.*

170. *It Is Further Ordered* that, pursuant to applicable procedures set forth in §§ 1.415 and 1.419 of the Commission's Rules, 47 CFR 1.415, 1.419, interested parties may file comments on the Notice of Proposed Rulemaking on or before 30 days after publication in the **Federal Register**, and reply comments on or before 60 days after publication in the **Federal Register**.

171. *It Is Further Ordered* that the Commission's Office of the Secretary *Shall Send* a copy of this Notice of Proposed Rulemaking, including the Initial Regulatory Flexibility Analysis, to the Chief Counsel for the Small Business Administration (SBA) Office of Advocacy.

Federal Communications Commission.

Marlene Dortch,

Secretary.

[FR Doc. 2025–22020 Filed 12–4–25; 8:45 am]

BILLING CODE 6712–01–P

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 64

[CG Docket Nos. 17–59, 02–278, 25–307; WC Docket No. 17–97; FCC 25–76; FR ID 319452]

Advanced Methods To Target and Eliminate Robocalls

AGENCY: Federal Communications Commission.

ACTION: Proposed rule.

SUMMARY: In this document, the Federal Communications Commission (Commission) proposes steps to improve the availability and accuracy of caller identification information transmitted to consumers to enable them to better understand who is calling and decide whether to answer calls. Specifically, the Commission proposes to enhance the effectiveness of STIR/SHAKEN by

requiring terminating providers to transmit verified caller name or other caller identity information for presentation on a consumer's handset whenever they transmit an indication that a call has received an A-level attestation. It also seeks comment on requiring providers to use Rich Call Data (RCD) to transmit verified caller name on IP networks, whether to permit or require use of other solutions, and an alternative option to require that providers implement RCD in their IP networks for all calls. The Commission further proposes to require voice service providers to implement measures to ensure that consumers know which calls originate from outside of the United States and to prohibit spoofing of United States telephone numbers for calls that originate from outside of the United States. Finally, the Commission seeks comment on whether some of its calling-related rules can be simplified, streamlined, or eliminated, perhaps because they are outdated or have not been enforced for a substantial amount of time.

DATES: Comments are due on or before January 5, 2026 and reply comments are due on or before February 3, 2026.

ADDRESSES: Pursuant to § 1.49 of the Commission's rules, 47 CFR 1.49, parties to this proceeding must file any documents in this proceeding using the Commission's Electronic Comment Filing System (ECFS): You may submit comments, identified by CG Docket No. 17–59, WC Docket No. 17–97, and CG Docket No. 02–278, by any of the following methods:

- *Electronic Filers:* Comments may be filed electronically using the internet by accessing the 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 8:00 a.m. and 4:00 p.m. by the FCC's mailing contractor at 9050 Junction Drive, Annapolis Junction, MD 20701. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes and boxes must be disposed of before entering the building.
- Commercial courier deliveries (any deliveries not by the U.S. Postal Service) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701.
- Filings sent by U.S. Postal Service First-Class Mail, Priority Mail, and Priority Mail Express must be sent to 45 L Street NE, Washington, DC 20554.
- *People with Disabilities:* To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an email to *fcc504@fcc.gov* or call the Consumer & Governmental Affairs Bureau at 202–418–0530.

FOR FURTHER INFORMATION CONTACT: For further information about the Notice of Proposed Rulemaking (*NPRM*), contact John B. Adams of the Consumer and Governmental Affairs Bureau at (202) 418–2854 or *JohnB.Adams@fcc.gov.*

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Ninth Further Notice of Proposed Rulemaking, Seventh Further Notice of Proposed Rulemaking Further Notice of Proposed Rulemaking and Public Notice (*NPRM*), in CG Docket No. 17–59; WC Docket No. 17–97; CG Docket Nos. 02–278 and 25–307; FCC 25–76, adopted on October 28, 2025 and released on October 29, 2025. The full text of this document is available online at *https://docs.fcc.gov/public/attachments/FCC-25-76A1.pdf.*

Paperwork Reduction Act Analysis: 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 § 1.1206(b) of the Commission's rules. In proceedings governed by § 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

1. We propose steps to improve the availability and accuracy of caller identification information transmitted to consumers to enable them to better understand who is calling and decide whether to answer calls. Specifically, we propose to enhance the effectiveness of STIR/SHAKEN by requiring terminating providers to transmit verified caller name or other caller identity information for presentation on a consumer's handset whenever they transmit an indication that a call has received an A-level attestation. We also seek comment on requiring providers to use RCD to transmit verified caller name on IP networks, and on whether to permit or require use of other solutions. Additionally, we seek comment on an alternative option to require that

providers implement RCD in their IP networks for all calls. Finally, we propose to require voice service providers to implement measures to ensure that consumers know which calls originate from outside of the United States and to prohibit spoofing of United States telephone numbers for calls that originate from outside of the United States.

A. Need for Improved Caller Identity Information

2. We believe that our proposals will empower consumers by giving them the information they need when deciding whether to answer a call. STIR/SHAKEN has served the Commission's goals of making spoofing more difficult, improving providers' call blocking and spam labeling decisions, and increasing the overall level of trust consumers have that a particular call originated from the telephone number being presented. However, consumers often cannot be sure who is calling unless a number is stored in their contact list or otherwise recognized. STIR/SHAKEN information does not provide consumers with robust information about who is calling, and an A-level attestation indicator alone does not give consumers enough information to decide whether a call is worth answering. In the absence of accurate caller name, and possibly other caller identity information, consumers might mistakenly believe that a checkmark or other indication that a call received an A-level attestation is an assurance that a call is not a scam or otherwise unlawful.

3. We believe that providing consumers with a verified caller name or other caller identity information would empower a more informed decision about whether to answer the call. We further believe that when a consumer's handset presents this additional information, it will reduce their confusion about the meaning of a green checkmark or other indicator that a call has received an A-level attestation, which will further increase trust and better enable consumers to avoid spoofed, scam, and other unlawful calls. Finally, we believe that transmitting verified caller identity information to the terminating provider will give providers additional information to use in their analytics, potentially making the analytics more accurate and thus addressing concerns about calls being labeled inaccurately.

4. Consumer surveys strongly support the goal of our proposals and suggest that legitimate callers, especially business callers, can benefit as well. One consumer survey indicated that 90% of consumers are uncomfortable answering unidentified calls and that 78% of consumers have missed an important call in the last month because they did not answer an unidentified call. Another survey revealed that 92% of consumers assume unidentified calls are fraudulent and that 56% of consumers sometimes risk answering an unidentified call because they fear it is a call they cannot afford to miss. It also asserted that employees who make calls on behalf of businesses believe that ensuring that consumers know who is calling is the most effective way to improve answer rates. As many as 88% of enterprise calls are not answered, which can reduce efficiency, increase costs of doing business, and reduce customer service. Notably, a different survey indicates that consumers are more likely to answer calls as more trusted caller identity information is presented to them. According to that survey, 73% will answer a call if the name of the caller is presented, 76% will answer if the caller's name and logo are presented, and 78% will answer if the reason for the call also is presented.

B. Defining Caller Identity Information

5. We propose to define ''caller identity information'' as having the same meaning given the term ''caller identification information'' in our rules, but excluding the originating telephone number or portion thereof and billing number information.

6. Terms like ''Caller ID'' and ''Caller ID with Name'' historically have been used to refer to functionalities that enabled a terminating provider to present to consumers, respectively, the originating telephone number or the originating telephone number and the associated caller name from a CNAM database. The Truth in Caller ID Act and our implementing rules define ''caller identification information'' to include both the originating telephone number and ''other information regarding the origination of the call,'' which our rules define to include certain enumerated items and ''[o]ther information regarding the source or apparent source of a telephone call'' and refer to any service or device used to provide caller identification information to a consumer as a ''caller identification service.''

7. In the context of the TRACED Act and the STIR/SHAKEN framework, however, ''caller ID authentication'' often is used to refer more narrowly to the originating telephone number alone. To be clear and to avoid duplication of rules that already require authentication of originating phone numbers using the STIR/SHAKEN framework, we use the term ''caller identity information'' throughout this document to refer to the caller's name, location, and ''other information regarding the source or apparent source of a telephone call,'' which generally means information other than the originating telephone number and billing information, and have proposed to define that term similarly in our rules. We seek comment on this analysis.

C. Transmitting Caller Identity Information to Consumers

1. Requiring Transmission of Caller Identity Information to Consumers When A-Level Attestations Are Indicated

8. We propose to require terminating providers to transmit to consumer handsets verified caller identity information whenever they transmit to the handset an indication that a call received an A-level attestation. To be clear, we do not propose to require terminating providers to transmit to consumer's handsets whether a call has received an A-level attestation or to transmit any new caller identification information. Instead, we propose a requirement that would apply only when a terminating provider chooses to transmit to the handset an indication that a call received an A-level attestation and seek comment on this proposal.

9. We believe that presenting an A-level attestation indicator on a handset with only the originating number provides little benefit to consumers because they might not understand the meaning of the indicator, mistakenly taking it to indicate that the call is not a scam or otherwise is lawful. Are marketplace solutions, on their own, sufficient to drive widespread presentation of verified caller identification information?

10. We believe that verified caller identity information helps legitimate callers, especially business callers, as well as consumers. If consumers have trustworthy caller identity information, they can make better informed decisions about whether to answer a call, which is likely to lead to higher answer rates and engagement. Information from the industry appears to support this belief. TransUnion states that customers are up to 105% more likely to answer a branded call. Similarly, a TNS survey found that 76% of Americans would prefer to engage with businesses that use branded calling and that 81% of consumers would answer a branded call if they recently had engaged with that brand. Is our belief correct?

11. While we believe that an indication that a call received an A-level attestation provides little benefit to

consumers taken alone, we also believe that combining it with verified caller identity information would benefit consumers significantly. We seek comment on this belief. Does verified caller identity information, such as caller name or logos, provide significant benefit to consumers? Does providing an indication that a call received an A-level attestation at the same time increase this benefit?

12. Does indicating that a call received an A-level attestation without additional caller identity information create opportunities for fraud? Are there situations where it would significantly benefit consumers to receive an A-level attestation indicator without any other verified caller identity information? Would adopting our proposal cause providers to stop transmitting A-level attestation indicators to consumer handsets? If so, would that enhance or undermine the goals of STIR/SHAKEN? What actions, if any, should we take to address any such outcomes?

13. *Minimum Caller Identity Information.* Current call branding solutions generally include caller name and the option for branding, such as logos. We propose to adopt a minimum requirement for what caller identity information must be provided; specifically, a verified name, whether personal or business. We believe that this is the most reasonable minimum requirement because some callers, such as individual callers, will not have a brand logo or other information to provide for a call. We seek comment on this proposal. Is there other information that would be appropriate to require? If we do not set a minimum requirement, is there information that we should specify does not meet the required standard?

14. Are there situations in which we should not require terminating voice service providers to transmit caller name or other caller identity information to consumer handsets? For example, what requirements should apply to callers who have a legitimate need for privacy, such as domestic violence shelters? What about callers who simply wish to maintain privacy? For example, what about callers who place calls using *67 or a handset that has a privacy setting to hide caller identify information? Does the Truth in Caller ID Act or any other provision of law require us to ensure that callers may prevent transmission of identifying information to the called party? We also seek comment on existing industry practices regarding privacy. For example, the ATIS RCD standard states that the terminating voice service provider is not to transmit RCD to the called party's handset if the caller requested privacy.

15. *Handset Capabilities.* Consumers can use a variety of handsets to receive calls, including traditional wireline phones, wireline phones for IP networks, and mobile phones. Consumers also might use assistive devices, services, mobile applications, or technologies when receiving calls. We seek comment on the capabilities of the various types of handsets to present caller identity information to consumers.

16. Modern mobile phones can present images, such as logos, as well as text on the screen. In addition, we believe that most modern mobile phone operating systems currently support the presentation of verified caller identity information, including verified logos, on their screens. We seek comment on this belief. Does the ability to present verified caller identity information on the screen vary depending upon the manufacturer of the mobile phone or the operating system? If so, how can we address this issue and ensure that consumers receive this valuable information? Are there steps we can take to ensure consumers consistently understand the information presented regardless of the device and/or operating system they are using? Are there similar options for IP or traditional wireline service that would allow the full range of verified caller identity information to be presented? If not, are most IP or traditional wireline phones capable of, at a minimum, presenting verified caller name? Would the transition of traditional wireline service to IP-based networks enhance consumer access to verified caller identity information?

17. We seek comment on the impact of our proposal on people with disabilities who use assistive devices and technologies, such as braille readers, TTYs, and assistive technologies integrated into handsets. For example, do mobile phones vary depending upon the manufacturer or operating system in how they present caller identification information when the consumer uses assistive technologies built into the phone? How would our proposal affect users of third-party assistive devices, generally? When text or other graphic communication is transmitted via assistive devices (*e.g.,* TTY text-based communications) and is converted into digital audio packets for transmission over IP networks, will that affect the transmission of caller identification information associated with the call? If so, how and what steps should we take to mitigate any loss of caller information?

18. *Telecommunications Relay Services (TRS).* We seek comment on how our proposals affect the use of TRS. When a provider of TRS (of any type) connects a call from a TRS user to the called party, is the caller identification information, including the level of attestation, for the caller transmitted to the called party or is caller identification information, including the level of attestation, for the TRS center transmitted to the called party? Why? Does the result depend upon the capabilities of the TRS provider, the voice service providers in the call path, or something else? In the context of caller identification information and caller ID authentication, is connecting to the TRS provider treated as part of initiating the call or as a separate segment of the call path following call initiation? Do voice service providers who perform attestation assign different attestation levels depending upon whether the originating number or other caller identification information is for the caller or for the TRS center? If so, why? How does the likelihood that a called party will answer a call differ when the caller identification information, including the level of attestation, is for the TRS center versus for the caller? If caller identification information for the TRS center, rather than for the caller, is transmitted to the called party, what steps should we take to ensure that caller identification information for the caller is transmitted to the called party? Does connecting to a TRS center affect the terminating provider's ability to perform authentication functions? If so, how?

19. We also seek comment on the implications of these proposals for different types of relay services. For example, when a user of TTY-based TRS or Speech-to-Speech Relay Service (STS) calls 711 to connect to the relay service, is the caller identification information, including attestation level, for the relay center or for the caller? Why? Does the result depend on the capabilities of the relay center, the voice service providers in the call path, or something else? Does the attestation level assigned by a voice service provider differ depending on whether the caller identification information is for the relay center or for the caller? Why and how? Providers of Video Relay Service (VRS) and IP Relay assign their users telephone numbers. Before connecting a call placed by a VRS or IP Relay user, the TRS provider must first query the TRS Numbering database to determine whether the call is point-to-point or requires a communications assistant. Calls requiring a

communications assistant are first routed to the TRS center and then to the terminating provider, perhaps via intermediate providers. How does the involvement of the TRS center affect transmission of caller identification information, including attestation level, over the entire call path? For these different types of relay services, how does the likelihood that a called party will answer a call differ when the caller identification information, including level of attestation, is for the TRS center versus for the caller? Do the differences between caller identify information and attestation level, if any, when the caller identification information is for the caller or for the TRS center affect the likelihood that a called party will answer? How and how much? Some providers of IP Captioned Telephone Services (IP CTS) utilize call forwarding capabilities to provide captions and allow IP CTS users to share their mobile phone number, rather than the telephone number assigned for purposes of connecting to IP CTS. How do the characteristics and transmission paths of these calls affect the end-to-end transmission of caller identification information, including assignment and transmission of an attestation level? What steps should we take to ensure the end-to-end transmission of caller identity information for calls that involve these types of relay services?

20. Are there changes or refinements we should make to our proposals to ensure that users of assistive devices, services, and technologies, including TRS, receive all of the benefits associated with being better able to identify callers? If so, are those changes or refinements different depending on whether the user of assistive devices, services, or technologies is making or receiving a call?

2. Requiring Originating Providers To Verify That Transmitted Caller Identity Information Is Accurate

21. We propose to require originating providers that transmit caller identity information to employ reasonable measures to verify the accuracy of the information transmitted. We believe that caller identity information is valuable to consumers only if it is accurate. Inaccurate information has the potential to cause significant harm if it leads a consumer to trust a caller making unlawful calls, and can further erode trust in the telephone network. We seek comment on this proposal.

22. What measures should be viewed as ''reasonable''? Should our codified rules prescribe specific measures or specific standards or criteria for assessing reasonableness? As part of a verification requirement, should we mandate collection and verification of specific information? If so, what specific information should be collected, and how should it be verified? Should we allow providers flexibility in how they verify caller identity information or in what information must be verified? If so, are there minimum standards or guidelines we should adopt? How can we ensure that all providers are taking necessary steps to ensure the accuracy of caller identity information? Do we need to adopt specific requirements when the originating provider is a reseller or when the caller utilizes a branded calling solution provided by a third-party vendor? Are there other requirements we could adopt that do not involve the collection and verification of specific information but still would ensure that caller identity information is accurate? For example, should we permit voice service providers contractually to require customers to provide only accurate information and names, logos, etc. that they legally are entitled to use? Are there practical, operational, or business considerations that limit the ability of an originating provider to verify the accuracy of caller identity information? Should we define what constitutes ''accurate'' information? If so, how should we define it?

23. If we adopt particular requirements, should we address differences among types or classes of callers, such as government, non-profit, business, and individual callers, or differentiate among callers based on call volume? Would originating providers be able to accurately determine the type or class of caller in all instances? For business callers, what steps should an originating provider take to ensure that business name, company logo, or other information is accurate? What steps should we take to ensure business callers are authorized to use a business name, brand name, or logo? Is it necessary to take different approaches depending on the type or size of the business? What about franchisees or individual business locations of a large, perhaps regional or national, business? For individual callers, should we require verification of the caller name against government issued identification prior to transmission of the name for this purpose? Are there alternative approaches to verifying the caller name for individual callers? If we were to differentiate among callers based on call volume, what threshold should be used to differentiate, for example, between high-volume and low-volume callers?

24. Are there situations in which an individual caller might have a valid reason to transmit something other than a legal name, such as a nickname? How can we address these situations? How should we handle multi-line accounts, including family plans, where the caller name for each individual line might be different from the subscriber's name and where verification of each name might be more difficult? If names of individuals on a family plan can be presented on called parties handsets, should we establish safeguards regarding the transmission and presentation of the names of minors? For example, should there be a broad exception for all consumers under the age of 18? Would a generic label be more appropriate for non-business calls placed by an individual caller? If so, how would a caller select this option for their personal calls? How would our proposal affect a person calling a crisis hotline, such as 988 for suicide prevention or the National Domestic Violence Hotline?

25. Should other entities share responsibility for ensuring caller identity information is accurate? For example, if a terminating provider becomes aware that an originating provider is transmitting inaccurate information, should it cease delivery of the originating provider's traffic or take other steps? Are there other enforcement requirements we should consider to similarly ensure accurate caller identity information?

26. There appear to be some industry standards and best practices that could inform our deliberations. For example, the ATIS RCD standard contains provisions related to the vetting of RCD information, and CTIA has created best practices for its branded calling solution. We seek comment on these documents and any other related industry practices, including their sufficiency, propriety, and enforceability, and on whether they mitigate the need for us to adopt requirements.

27. Should we consider measures beyond requiring that originating providers take reasonable steps to ensure caller identity information is accurate? Citing other sources, Numeracle states that ''93.4% of robocall traffic from the most prolific robocall signers now carry A-level attestations'' and ''48 percent of illegal calls are A-attested.'' Are these numbers accurate and, if so, do they buttress the view that A-level attestations mislead consumers and that we should adopt more stringent requirements for verifying caller identity information? For example, should we consider establishing a ''trusted framework'' whereby the Commission or another

entity defines who can assert caller identity is verified and when? If we were to adopt such an approach, how can we ensure that any such entity and process are competitively neutral? We believe that revisiting our know-your-customer requirements will be an important part of this effort, and we plan to do so in a separate proceeding.

3. Securely Transmitting Caller Identity Information

28. We seek comment on any requirements we should adopt to ensure that caller identity information is securely transmitted from the originating provider to the terminating provider, including whether to require the use of RCD to do so. We believe that if caller identity information is changed or tampered with in transit, then the verification efforts of the originating provider will not ultimately benefit consumers or callers. We seek comment on this belief. Is secure transmission necessary to ensure that caller identity information is not altered by bad actors and can be trusted by consumers? Are there other ways to ensure that the data transmitted is not modified or tampered with? Are there other legal requirements or benefits to ensuring the caller identity information is securely transmitted throughout the entire call path?

29. *Rich Call Data.* We seek comment on whether to require providers to use RCD whenever they transmit caller identity information. With RCD, caller identity information is placed into a PASSporT Identity token with a digital signature, just as with the originating number under STIR/SHAKEN. When the provider digitally signs the encrypted PASSporT(s) carrying both SHAKEN and RCD information, it is asserting to the truth of the information carried in the PASSport(s), including the call attestation level, calling number, and any caller identity information. The terminating provider then decrypts and verifies the digital signature and electronically validates the information. RCD thus takes advantage of the end-to-end trust provided under the STIR/SHAKEN framework. RCD requires the inclusion of a caller name, but allows for additional information, such as a link to a logo and/or a website with information about the caller, and a form of virtual business card referred to as a ''jCard.''

30. We believe that RCD provides a means to securely transmit caller identity information. Is our belief correct? Are there features of caller identity information transmission that suggest we should depart from the RCD standards? If so, how might we address them? Are there any steps we can take to make the RCD standards more secure? Alternatively, is the security of RCD generally unnecessary in this context? If so, why, and how much security is actually necessary?

31. If we were to require use of RCD, should we require the use of only one or up to all three RCD standards? Why or why not? Should we require that providers implement the ATIS standard to ensure that providers comply with vetting requirements? Are there other aspects unique to the ATIS standard that would justify its adoption? Are there omissions that would counsel against its adoption or do those omissions give providers helpful implementation flexibility? We seek comment with respect to any unique features and additional omissions in the IETF standards as well and their relevance to whether we should mandate their adoption. We also seek comment on whether we should specify that the current version of any RCD standard we require must be used. If we do specify a standard, how should we balance the evolution of standards and provide implementation timelines for updated standards looking forward?

32. We also seek comment on whether the standards are sufficiently developed and available to require their implementation. We note that the two recently published IETF standards have been in draft form for several years, and the first version of the ATIS RCD standard was adopted in 2021. To what extent have providers and vendors implemented the earlier versions of these standards, and do the recently-finalized standards require additional time to implement based on any incremental changes? Since our understanding is that some providers already use RCD as part of their branded calling solutions, we believe that the RCD standards, including the revised standards, can be implemented in a reasonable amount of time. We seek comment on this belief. We also seek comment on whether any additional features or functions of the standards need to be developed to ensure that they achieve their purpose. If not, what work must be completed prior to implementation? How can we ensure that this work is completed in a timely manner?

33. We also seek comment on the benefits and drawbacks of RCD generally. Does RCD provide particular benefits that make it superior to other caller identity information solutions? Are there any particular weaknesses we should be aware of? For example, does it present particular challenges for some providers, such as smaller providers? If we do not require use of the RCD standards, should we adopt rules that set minimum requirements based on the RCD standards? If so, what minimum requirements should we set? Should any minimum requirements vary by provider type? How would the costs associated with this option impact its implementation?

34. *Alternative Caller Identity Solutions.* We seek comment on options other than RCD for transmitting caller identity information or basing our minimum requirements on the current versions of the RCD standards. Our understanding is that there are caller identity solutions currently in the market, usually referred to as call branding or branded calling, that allow for transmission of caller identity information but that do not use the RCD standards or only use them partially along with other standards or proprietary elements. We seek comment on these solutions. Do they ensure that caller identity information is secure and cannot be modified? If so, how? Would that remain true for alternatives if implemented at a larger scale? Do they have any particular strengths or weaknesses as compared to RCD? Would allowing providers to use other solutions enable more providers to transmit caller identity information to consumers and therefore benefit more consumers or provide inconsistent service?

35. If we allow providers to use solutions other than RCD or that do not rely on the RCD standards, how can we ensure that caller identity information is securely transmitted so that consumers can rely upon it? Are there specific existing alternative solutions that offer secure transmission that we should authorize or require providers to use? If so, which solutions offer appropriate security?

36. If we allow providers to use more than one solution to fulfill their obligations, we believe that they should be interoperable so that caller identity information is not lost. How can we ensure that approved solutions are interoperable? To what extent are current alternatives interoperable? Are there requirements we could adopt to ensure that caller identity information is always passed on to the point of termination regardless of which solution a provider uses? Should we require intermediate providers to transmit caller identity information for calls that transit their networks for any IP-based caller identity solutions providers may use? What should we do if an intermediate provider is not able to comply with such

a requirement because of technical limitations?

37. *Alternative Options.* We seek comment on other approaches we could take to enable consumers to make more informed choices when their phones ring. First, we explore the option of requiring providers to implement RCD in their IP networks for all calls. Second, we seek comment on requiring caller identity verification as a condition of an originating provider giving an A-level attestation. Finally, we seek comment on any other steps we could take to improve the availability and validity of caller identity information for consumers and restore trust in the network.

38. *Requiring Implementation of RCD.* Should we require all voice service providers to implement RCD in their IP networks for all calls? What benefits or harms would consumers and providers experience? How can the Commission balance them? Currently, Commission rules require voice service providers to implement STIR/SHAKEN in their IP networks, but there is no corresponding requirement to implement RCD. Would a requirement for all providers to implement RCD in their IP networks be appropriate at this time, and if not, when would such a requirement be appropriate?

39. Should we require providers to implement the existing RCD standards? Since there are three RCD standards, should we require implementation of just one, all three, or some combination of two of the standards? Why? How would requiring implementation of one or two of the RCD standards affect providers that choose also to implement the third? If we were to adopt requirements that differ from those contained in the RCD standards, such as for verification of caller identity information or regarding the ability of callers to maintain their privacy by preventing caller identity information from being transmitted with their calls, how would that affect the choice of which RCD standard or standards to require? Would our choice of any particular standard or standards create a significant or different burden on smaller providers?

40. What measure or measures should we adopt to determine whether a provider has implemented RCD? Would any potential measure be different for resellers, originating facilities-based providers, intermediate providers, or terminating providers? If so, why? For example, would an intermediate provider properly be considered to have implemented RCD if it transmits to subsequent providers in the call path the RCD information it receives from the provider immediately before it in the call path?

41. If we do adopt an implementation mandate, how quickly can providers implement RCD throughout their IP networks? Does this answer depend upon which RCD standard or standards we require providers to implement? Are there any types of providers, such as smaller or rural providers, for which RCD implementation would be especially burdensome? If so, should we adopt a mandate that is more limited in scope with the intention of expanding it to all providers in the future? Alternatively, should we adopt an exemption for certain categories of providers or establish a longer implementation timeframe for those providers? Is there any standards work left to be done to ensure that RCD is implementable across all IP networks? Does interoperability testing need to be completed? If so, how can we ensure that this work is completed as quickly and efficiently as possible while ensuring that key steps are not skipped? If standards work or testing still is needed, are there rules short of a mandate that we could adopt to expedite this work?

42 Considering that STIR/SHAKEN and RCD work only on IP networks, we seek comment on any steps we should take, consistent with requiring RCD, to address the non-IP gap as the Commission continues to drive towards an all-IP environment. Are there requirements we could adopt that would address the fact that RCD does not work on non-IP networks? For example, are there other existing solutions that work on non-IP networks that we could require? Are these solutions interoperable with RCD or can they be made interoperable? We previously proposed to require the implementation of non-IP caller ID authentication solutions. We received limited comment on the use of RCD and alternatives on non-IP networks and now seek additional, focused comment. If we do require any or all of these solutions, are there rules we could adopt consistent with requiring RCD that would build on those solutions for caller identity information beyond the originating number? Are there methods by which RCD could work with non-IP authentication frameworks, either as currently envisioned or with minor adjustments? If not, are there equivalent options that would work with non-IP authentication frameworks? If there are equivalent options, how can we ensure that they can be used where appropriate? Would allowing providers the flexibility to use options other than RCD enable or encourage more providers to transmit verified caller identity information? Do any non-RCD solutions prevent caller identity information from reaching the terminating provider when a call transits from IP to non-IP networks? If so, are there ways we could address that problem? What is the cost to implement non-RCD solutions on non-IP networks?

43. *Requiring Caller Identity Information Verification as a Condition of A-Level Attestation.* Because we propose in this document to require originating providers to employ reasonable measures to verify the accuracy of caller identity information before transmitting it, we also take the opportunity to ask whether, alternatively, the Commission should explore making this verification requirement a condition of A-level attestation. Under current STIR/SHAKEN standards, an authenticating provider may give an A-level attestation when it has a direct authenticated relationship with the customer and can identify the customer, and when it has established that its customer has a verified association with the telephone number used for the call. The authenticating provider's customer may be a caller or another provider. The STIR/SHAKEN standards do not require the provider to verify any caller identity information the caller provides.

44. We seek comment on whether requiring caller identity verification as a condition of A-level attestation could yield greater benefits than our proposal to require originating providers to simply verify the accuracy of caller identity information. If so, how? Would such an approach effectively deter A-level attestations for calls that are spoofed? Should we consider such a requirement in conjunction with requiring the transmission of verified caller identity information as we propose above? If so, are there any changes we should make to that proposal? Could such an approach create greater or different burdens for originating providers compared to our proposal to require originating providers to verify the accuracy of caller identity information prior to transmission? What modifications could help reduce these burdens and this possibility? Is such an approach aligned with the overall goal of STIR/SHAKEN, or are there reasons to separate the caller's identity from an indicator that the number is less likely to be spoofed? If the latter, what steps could we take to ensure consistency with the goals of STIR/SHAKEN? Are there other issues we should consider?

45. We also seek comment on how providers can verify caller identity information in scenarios where the

authenticating provider does not have a direct relationship with the end-user caller. For example, how should the Commission address the ''knowledge gap'' that arises when an authenticating provider's customer is a reseller rather than the calling party? Would requiring providers to delegate certificates enable providers who have the relationship with callers to send verified caller identity information to authenticating providers. Instead of or in addition to doing so, should we remove the exemption for providers who lack control of the network infrastructure necessary to implement STIR/SHAKEN so that the reseller that has the relationship with the caller has an obligation to authenticate calls using STIR/SHAKEN? How would eliminating this exemption work in practice, and would it provide a practical means for all providers to include verified caller identity information with their attestations? Are there other ways to allow providers to assign A-level attestations and include verified caller identity information in indirect customer scenarios while maintaining the integrity of the STIR/SHAKEN framework? Are the answers to these questions different in other scenarios where the authenticating provider does not have a direct relationship with the end-user caller, such as when a user obtains a toll-free number from a Responsible Organization or obtains voice service from a voice service provider that obtains numbering resources from another voice service provider rather than from the Numbering Administrator?

46. Additionally, we seek comment on the potential short- and long- term impacts of conditioning A-level attestations on verification of end-user caller identity. In the short term, could this effectively eliminate A-level attestations in many scenarios, thereby reducing the usefulness of STIR/SHAKEN for analytics and consumer trust? Over the longer term, what processes, standards, or technical solutions would be necessary for providers to develop reliable caller identity verification practices? Should we require their adoption, and what timelines would be reasonable for development and implementation? To date, we have not raised the possibility of deviating from the standards' requirements for providers to sign a call with an A-level attestation. We seek comment on whether imposing requirements that go beyond current STIR/SHAKEN standards would conflict with the standards or pose other challenges. As the Commission continues to evaluate the effectiveness of the technologies used for call authentication frameworks, how should we balance the goals of improving caller identity assurance with the existing functionality of the STIR/SHAKEN framework?

47. *Other Options.* Are there other approaches we could take to ensure that consumers receive accurate and actionable information when calls are delivered? If so, what might these approaches be? Are any providers already taking these steps? Should we adopt any of these proposals in conjunction with one of the options discussed previously, or do they supplant our other options? How difficult would adopting these other options be for callers and providers? What benefits would they provide? Would the approach be implementable across the network or would some providers be technically unable to do so?

D. Calls Originating From Outside of the United States

48. *Identifying Foreign-Originated Calls.* We propose to require providers to identify calls that originate from outside of the United States to transmit that information over the entire call path, and to transmit to consumer handsets an indicator that the call originated from outside of the United States whenever they know or have a reasonable basis to know that a call originated from outside of the United States. Specifically, we propose to require gateway providers to mark calls that originate from outside of the United States, intermediate providers to transmit that information to downstream providers, and the terminating voice service provider to transmit to consumers' handsets an indicator that a call originated outside of the United States when they know or have reason to know that a call originated from outside of the United States, such as when a call has been marked as having originated outside of the United States by an gateway provider. We seek comment on this proposal. We also seek comment on what steps gateway providers, non-gateway intermediate providers, and terminating voice service providers would need to take to implement this proposal, if adopted. Should we establish a definition of ''foreign-originated'' for these purposes and, if so, what should be that definition?

49. We believe that transmitting such information through the entire call path and the presentation of an associated indication on the called party's handset would give both providers and consumers information to protect against scam robocalls originating outside of the United States. We seek comment on that belief.

50. We seek comment on the ability of gateway providers to determine the country of origin for a call and for providers across the call path to include the country of origin in caller identity information when transmitting a call. For example, are gateway providers able to identify a call's country of origin? Why or why not? Can gateway providers include the country of origin when transmitting a call? How can we ensure the country of origin information is transmitted securely across the entire call path? For instance, should we require a gateway provider authenticating foreign originated calls using STIR/SHAKEN to encrypt information that a call originated overseas in the PASSporT? Should we require a specific means for achieving this? Is it possible for providers to insert this information in the OrigID, and, if so, should we require that providers use a specific OrigID to indicate a call is foreign originated? Can providers user a unique OrigID for each country? Would this use of an OrigID conflict with the STIR/SHAKEN standards or impose any implementation obstacles?

51. Would we also need to require intermediate providers to pass the OrigID intact downstream and for the terminating provider to accept it before transmitting an indication that the call was foreign originated to the called party? Should we require use of non-IP solutions to ensure transmission over non-IP networks? Do terminating providers have a means of transmitting the OrigID or another indicator that the call originated outside the United States for presentation on handsets? Does the ability of terminating voice service providers to transmit to consumer handsets an indicator that a call received an A-level attestation demonstrate that they could readily transmit an indicator that a call originated from outside of the United States? Do handsets typically have a means of presenting an indication that a call was foreign originated based on any such indicator? What difference would the handset's manufacturer or operating system make in being able to present the country of origin when the phone rings compared to being able to present an indicator that the call originated from outside of the United States? Should we, and is it technically feasible to, require gateway providers to label or modify the number sent for presentation on the called party's handset for foreign-originated domestic

calls carrying U.S. NANP numbers as some countries already do?

52. We seek comment on the impact, if any, on the ability of voice service providers to implement our proposals for calls that originate from outside of the United States but that legitimately spoof a North American Numbering Plan (NANP) number, such as when a domestic business has offshored call center operations and chooses to present a domestic NANP number as the originating number or for consumers to call back. Are there any different or unique factors we should consider for calls that originate outside of the United States but legitimately spoof a NANP number, especially a domestic NANP number?

53. Similarly, we seek comment on whether we should exempt from our proposals calls that originate on devices subscribed to United States mobile and/or VoIP service and that are roaming outside the United States. For example, United States VoIP consumers may seek to use nomadic capabilities of their service to place calls using their United States telephone number while traveling abroad. Do service providers have the means to distinguish United States mobile and/or VoIP service roaming calls from other calls that originate outside the United States?

54. We further propose to require voice service providers that use reasonable analytics to block calls to include whether a call originated from outside of the United States as a factor in their analytics. We seek comment on this proposal. We seek comment on what steps providers would need to take to include this information in their analytics and whether this requirement would further protect consumers against scam robocalls originating outside of the United States. Do those steps differ depending upon whether providers who use analytics know only that the call originated from outside of the United States versus the specific country from which a call originated? Can current or potential Artificial Intelligence capabilities play a role in these analytics or in verifying caller identity information?

55. Are there countries from which a greater volume of scam or otherwise potentially unlawful calls originate or countries that otherwise pose a greater risk to consumers? If so, which countries and why? What volume of scam or otherwise potentially unlawful calls originates from each country? How does that compare to the total volume of calls that originate from each country? Based on annual data, what is the total number of calls that originate from outside of the United States? Of those calls, what percentage are scam calls, spam calls, use an autodialer, and/or use an artificial or prerecorded voice? For each of these types or categories of calls, what methodology was used to identify and categorize the calls?

56. How should foreign-origin indicators appear on consumer devices without confusing consumers? What, if anything, are providers already doing to protect consumers from scams or otherwise potentially unlawful calls that originate from outside of the United States or from specific countries? What challenges do providers face when dealing with detecting, blocking, or labeling such calls? Are there other actions that the Commission could take to address these calls?

57. *Using Phone Number Requirements to Identify Foreign-Originated Calls.* We seek comment on whether we should establish numbering requirements that would help enable consumers to identify foreign-originated calls. For instance, should we designate a specific area code for foreign-originated calls? What challenges would arise from moving existing foreign users of United States NANP numbers to a newly-designated area code? Would designating an area code for foreign-originated calls provide a clear and useful signal to terminating end-users that the call originated from outside of the United States and not from the domestic marketplace? How should numbering resources in such area codes be assigned? Are any special considerations necessary for routing calls to and from such numbers? How should calls among such numbers and other United States NANP numbers be categorized for intercarrier compensation purposes (*e.g.,* should all such calls be treated as interstate interexchange calls)? Are there any technical or administrative barriers to doing so?

58. If we establish a designated area code for foreign-originated calls, we seek comment on whether we should require that gateway providers block any foreign-originated calls carrying United States NANP numbers for presentation on the called party's handset that are not from that area code. We believe that marketplace developments and the continued evolution of similar rules in other countries may provide real-world evidence of the effectiveness and administrability of such a requirement in the United States. For example, in 2024, the UK's Ofcom released revised guidance stating that calls from outside of the UK carrying a UK ''presentation'' number (*i.e.,* the number to be presented to the called party) will be blocked except where the call is made by a UK customer who has the right to use the number. Under OfCom's guidance, the gateway provider is responsible for compliance with the guidance. OfCom also notes that one way foreign-originating providers can demonstrate to UK gateway providers that a call is being made by a UK customer is by providing the gateway provider with evidence of direct or indirect number assignment. We seek comment on OfCom's approach and any similar approaches adopted in other countries to block foreign-originated calls that terminate within the domestic marketplace. Should exceptions to blocking be made for certain traffic, such as mobile roaming traffic, that carries different presentation numbers? Should we instead require gateway providers to use heightened due diligence or mitigation techniques on calls from area codes other than the one designated for foreign-originated calls?

59. *Identifying the Source of Unlawful Foreign-Originated Calls.* We seek comment on how to better identify the source of unlawful calls that originate from outside of the United States. In this context, the source of an unlawful call includes the country from which the call originated, the originating voice service provider, and the maker of the call.

60. To what extent can providers, including United States gateway providers and foreign intermediate providers, identify the originating caller or provider of a foreign-originated call? Does existing routing technology, which is often designed to reduce costs and avoid congestion, prevent providers from identifying the source of a call? Could traceback efforts be streamlined if calls originating from outside of the United States involved fewer voice service providers in the call path before the call reaches the United States? How can the number of voice service providers in the call path outside of the United States be reduced? What factors contribute to how many voice service providers are in the call path outside of the United States? What can we do to mitigate or eliminate those factors? Are there international agreements or memoranda of understanding that might provide mechanisms for reducing the number of voice service providers in the call path before a call reaches the United States or that we should otherwise be mindful of as we consider our proposals?

61. What other tools could we use to help identify the sources of foreign-originated calls? For instance, could we implement a chain of agreements requirement whereby gateway providers

accept traffic only from foreign providers that agree to cooperate with traceback requests and that, in turn, only accept calls from providers that agree to the same conditions? How many providers upstream of the gateway provider could such a requirement effectively reach? Similarly, how can we promote implementation of STIR/SHAKEN or other interoperable call authentication solutions in other countries and to achieve cross-border authentication? Could we require gateway providers to accept only calls with United States NANP number that have been authenticated? Would this enable United States providers to identify the source of calls? We also seek comment on potential collaboration with foreign governments to identify the sources of calls or more broadly mitigate unlawful foreign-originated calls.

62. Do the answers to the questions posed above differ depending on whether the goal is to identify the country of origin, the originating voice service provider, or the maker of the call? If so, how? How can the process of identifying the source of a call that originates from outside of the United States be automated or made a part of transmitting a call? Is there a way or a basis to treat calls differently depending on whether the origin of the call is known or on the specific origin of the call? For example, should a factor in call analytics be that a call originated from a country, voice service provider, or maker known to be a source of unlawful calls or should calls be blocked from entering the United States if the origin of the call is not known?

63. *Spoofing of United States Numbers for Foreign-Originated Calls.* We seek comment on whether we should continue to permit callers to spoof NANP United States telephone numbers for calls that originate from outside of the United States for calls that are made by or made on behalf of a person, usually a business, that is authorized to use the spoofed number. Callers sometimes spoof the originating number for a call for legitimate reasons. For example, a business might have its main contact number or a toll-free number sent for presentation on call recipients' handsets. Or a doctor placing a call to a patient from a personal phone might prefer to have the patient's handset present the number of the medical office. As long as the caller spoofs a number that it is authorized to use, this type of spoofing is permitted.

64. Should we prohibit spoofing of United States telephone numbers on calls that originate from outside of the United States? Does the practice mislead consumers about a call's origin? Does it make consumers more susceptible to unlawful calls involving spoofing, such as by increasing their trust in calls that originate from outside of the United States? How many calls that originate from outside of the United States spoof a United States telephone number? Of those, how many are unlawfully spoofed? Do calls that originate from outside of the United States and spoof a United States number carry a greater risk of being unlawful, such as being a scam, than calls that originate from within the United States and spoof a United States number? What is the magnitude of that risk?

65. Are there other factors that we should consider? If we were to prohibit spoofing of United States numbers for calls that originate from outside of the United States, what, if any, changes would be required to existing technical standards, such as STIR/SHAKEN or RCD? How would such a prohibition impact businesses that have offshored certain operations, including call centers? Would this prohibition encourage businesses to invest in the United States or return jobs to the United States? What effect, if any, would this prohibition have on calls that originate from other countries that are part of the NANP? And if we adopt our proposal to require voice service providers to transmit to handsets an indicator that a call originated from outside of the United States, would that indicator be sufficient to alert the called party when the call appears to originate from a United States number?

66. Should spoofing or other use of NANP United States numbers for calls originating from outside of the United States be addressed in memoranda of understanding or other collaborative efforts among the United States and other countries? If so, what should the content of such memoranda be? Should calls be treated differently depending on whether the country of origin has entered into a memorandum of understanding or other agreement with the United States? If so, how?

E. Legal Authority

67. We seek comment on our authority to adopt these proposals and on our authority regarding other actions on which we seek comment above, including under the Truth in Caller ID Act, the TRACED Act, and section 251(e) of the Communications Act. We also seek comment on any other bases of authority for our proposals and other actions on which we seek comment.

68. The Truth in Caller ID Act defines caller identification information as including both the originating telephone number and ''other information regarding the origination of the call.'' It also prohibits any person from ''caus[ing] any caller identification service to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value'' and directs the Commission to prescribe implementing regulations. We believe that requiring originating providers to verify caller identity information—a subset of caller identification information—will reduce opportunities for bad actors to manipulate caller identification information. We seek comment on this reasoning and on whether our proposed rules and other actions on which we seek comment are consistent with the Truth in Caller ID Act. If our proposals or other actions do not align with the Truth in Caller ID Act's scienter and intent elements, are there ways our proposals and other actions can be structured to come into alignment?

69. We believe that the TRACED Act provides additional authority for our proposals and other actions on which we seek comment. In it, Congress directed the Commission to require implementation of the STIR/SHAKEN framework in IP networks and granted us the authority to ''revise or replace'' call authentication frameworks after assessing the efficacy of such frameworks following notice and an opportunity to comment. Although the TRACED Act requires us to conduct formal triennial assessments and submit a report to Congress, we believe the statute provides authority to conduct ongoing assessments and take responsive action in the interim, so long as we provide notice and opportunity to comment. We can use comments in this proceeding as part of a future assessment to evaluate STIR/SHAKEN's effectiveness and need for revision. The TRACED Act also grants us authority over non-IP networks, including to require robocall mitigation programs. We also believe that we have authority under the TRACED Act to promulgate rules governing when providers may block calls based on call authentication information. We seek comment on our belief that these provisions provide authority for our proposals and other actions on which we seek comment. We also seek comment on our authority under section 4(d) of the TRACED Act, which provides that ''[n]othing in this section shall preclude the Commission from initiating a rule making pursuant to its existing statutory authority.'' We believe that this provision confirms that

the TRACED Act, despite its specificity, does not limit the Commission's ability to exercise its broader statutory authorities, including those discussed herein, to address the same matters as the TRACED Act, provided that our exercise of broader authorities cannot conflict with Congress' directives in the TRACED Act. We seek comment on this belief.

70. We also seek comment on whether our exclusive jurisdiction over the United States portion of the North American Numbering Plan pursuant to section 251(e) provides authority for our proposals and other actions on which we seek comment. The Commission previously has found that section 251(e) provides ample authority to take actions to ''prevent the fraudulent abuse of NANP resources'' and that unlawfully spoofed originating telephone numbers are an abuse of those resources. We believe that our proposals and other actions here similarly are aimed at preventing abuse of NANP resources. We also believe that it is within our authority more generally to prohibit actions resulting in the presentation of NANP numbers in a manner that misleads consumers or aids in making scam and other unlawful calls more believable. We further believe that our authority extends to requiring providers to take actions that prevent the authentication and presentation of NANP numbers in combination with caller identity information from being misleading. We note that the Commission long has invoked these statutory provisions to adopt rules regarding caller identification obligations. We seek comment on these beliefs and on whether section 227(e) provides authority to adopt rules aimed at averting misleading caller identification information even if the statutory scienter and intent requirements of the Truth in Caller ID Act are not met.

F. Costs and Benefits

71. This document proposes to require terminating providers to transmit to consumer handsets verified caller identity information whenever they transmit an indicator that a call has received an A-level attestation and similarly to transmit an indicator that a call originated from outside of the United States when they know or have a reasonable basis to know that a call originated from outside of the United States. In addition, this document proposes to require originating providers that transmit caller identity information to employ reasonable measures to verify that that the information is accurate and for gateway providers to mark calls that originate from outside of the United States. This document further proposes to require intermediate providers across the entire call path to transmit information that a call originated from outside of the United States. This document also seeks comment on requirements to ensure that caller identity information is securely transmitted over the entire call path, including whether to require providers to use RCD to securely transmit this information, and on prohibiting spoofing of United States telephone numbers on calls that originate from outside of the United States, including where the caller is authorized to use the spoofed number. Further, this document seeks comment on the impact of our proposals on people with disabilities who use assistive devices, services, and technologies, and on providers of TRS and other services.

72. We seek comment on the costs and benefits of these proposals. By giving consumers better and verified information about the identity of those who call them, we believe that our proposals would help consumers avoid scam, fraudulent, and otherwise unlawful calls. These proposals also are expected to help businesses reach more consumers over the phone for legitimate purposes. Because these proposed requirements apply only when a terminating provider chooses to transmit to consumer handsets an indicator that a call received an A-level attestation or when an originating provider chooses to transmit caller identity information, we expect the benefits to extend gradually to consumers and businesses as more providers choose to transmit verified caller identity information. We expect that providers will transmit verified caller identity information when the benefits of doing so outweigh the associated costs and seek comment on the costs to implement the proposals discussed above. We note that our proposals rely upon the already-implemented STIR/SHAKEN framework and upon the existing RCD standards, which builds upon the STIR/SHAKEN framework to enable secure transmission of additional data. Thus, the ingredients that underlie our proposals already exist. We recognize, however, that verifying information to ensure its accuracy and that ensuring interoperability might necessitate some additional costs. We seek comment on our views, including cost estimates from providers over the entire length of the call path and from providers of TRS and other assistive devices, services, and technologies. Will smaller providers face unique challenges implementing our proposals?

73. This document also seeks comment on the alternative approach of requiring implementation of RCD in IP networks. We seek comment on the costs and benefits of requiring implementation of RCD in IP networks. We note that the particular RCD standard or standards that providers would be required to implement have not yet been determined. Therefore, we seek comment on the costs and benefits of all possible standards for implementation. The document also seeks comment on requiring caller identity information verification as a condition of A-level attestation. We seek comment on the costs and benefits of this approach. We further seek comment on the costs and benefits, including the potential for job creation and investment in the United States, of prohibiting spoofing of domestic United States numbers for calls that originate from outside of the United States, including when the caller is authorized to use the spoofed number.

II. Eliminating Outdated Rules

74. We seek comment on whether some of our calling-related rules can be simplified, streamlined, or eliminated, perhaps because they are outdated or have not been enforced for a substantial amount of time.

A. Telephone Consumer Protection Act Rules and Do-Not-Call Implementation Act Rules

1. Older Rules That Might No Longer Be Necessary

75. *Call Abandonment Rules.* We seek comment on whether to eliminate our rules prohibiting callers from disconnecting an unanswered telemarketing call prior to at least 15 seconds or four rings, and from abandoning more than three percent of all telemarketing calls. The Commission adopted these rules in response to the Do-Not-Call Implementation Act (DNC Act), which, among other things, required the Commission to ''maximize consistency'' between its rules and a portion of the Federal Trade Commission's (FTC's) Telemarketing Sales Rule (TSR). The FTC's current TSR contains comparable provisions to these two Commission rules.

76. The Commission adopted the rules in 2003 to ensure consumers do not answer calls only to get silence, or to be hung up on, largely as a result of the predictive dialers callers used at the time. Today's predictive dialers appear to leverage advances in technology, including Artificial Intelligence, to drive

efficiencies. Their evolution, along with marketers' incentives to avoid negative consumer impressions via dead air and abandoned calls, may mean our rules are no longer necessary.

77. We seek comment on whether the calling practices these rules target are no longer a significant source of consumer frustration. Have changes since 2003 rendered the rules unnecessary? Would eliminating the rules relieve callers of the burden of tracking their calls to comply, and to be prepared in the event the Commission were to ask about them? Would consumers be harmed by elimination of these rules? Does the DNC Act require us to retain these rules and does the Commission's differing jurisdiction from the FTC favor retaining or deleting these rules? Are there any other factors affecting whether these rules may or should be deleted? For example, would application of the FTC's corresponding rules to only those callers over which the FTC has jurisdiction result in potential confusion among callers and consumers regarding the applicable standard for call abandonment?

78. *Artificial and Pre-Recorded Voice Caller Identification Rules.* We propose to amend and streamline the rule requiring a caller making artificial or pre-recorded voice calls to include a telephone number other than a 900 number or any other number for which charges exceed local or long distance transmission charges. This rule should be updated to reflect changes in the telecommunications marketplace that could result in a consumer making a return call and incurring charges that exceed typical ''local or long distance'' charges. For telemarketing and certain other calls to consumers' residential numbers, the number provided must be able to accept DNC requests during regular business hours. We propose to modernize this rule to require only that such callers identify themselves with their telephone number to enable called consumers to know who is calling. We seek comment on this proposal. Does this change better reflect the modern telecommunications marketplace where, for example, ''local or long distance charges'' are far less common? To the extent consumers use these numbers to contact callers, how would our proposal benefit or harm them? Some parties state that the current rule aids robocall enforcement by facilitating the identification of illegal calls. Would our proposed approach, or other alternatives, similarly advance those enforcement interests?

2. More Recent Rules That Might Harm Consumers

79. *Consent Revocation Rules.* We seek comment on ways we can modify the requirement that a caller must treat an opt-out request made in response to one type of call to be an opt-out request for all types of calls or to modify it to give consumers greater control over their right to stop unwanted calls. The Consumer and Governmental Affairs Bureau delayed until April 11, 2026 implementation of this rule ''to the extent that it requires callers to treat a request to revoke consent made by a called party in response to one type of message as applicable to all future robocalls and robotexts from that caller on unrelated matters.''

80. Does the rule unduly restrict consumers' ability to receive wanted calls? For example, does it unduly restrict consumers' ability to receive calls from healthcare providers that might have multiple locations or practice specialties or from pharmacies? What about banks or other financial institutions where consumers might have different types of accounts or other businesses that have multiple locations, operating units, or lines of business? How does this affect consumers who both are customers of a business and are employees, job applicants, or contractors of that same business? Does this requirement place an undue burden on callers to modify their communications systems or is an all-or-nothing requirement less burdensome to implement? Would requiring consumers to revoke consent separately for each business unit, location, practitioner, or other sub-division of a caller create an undue burden under this rule modification? How can we modify the rule so that consumers continue to receive calls they want and in so doing ensure that callers honor consent revocation for those they do not, including empowering consumers to specify the scope of their revocations?

81. We also propose to amend § 64.1200(a)(10). For example, commenters in the Delete Proceeding asked us to permit callers to designate the exclusive means by which consumers may revoke prior express consent rather than requiring callers to honor all revocation requests made using ''reasonable means.'' We seek comment on this proposal. At the same time, we seek comment on whether there are less restrictive ways for consumers to revoke consent that nevertheless avoid the potential ambiguity of the current reasonable-means standard.

82. Are there any methods of revoking consent that should be required, even if other methods are permitted? Are there any that should be prohibited? What standards, if any, should we establish to ensure that revocation methods clearly are disclosed to consumers? Is there a significant risk that callers will demand revocations to be made by unduly complex, difficult, or cumbersome methods that could prevent or deter consumers from revoking consent effectively? Is there a significant risk that consumers would be less likely to give prior express consent? Would amending the rule as suggested provide more certainty to callers and consumers by making the rule less vague? Would it improve efficiency for callers or consumers?

83. *Fraud Alert Call Rules.* We seek comment on whether to eliminate the rule limiting financial institutions to calling only the number provided by the consumer when making a fraud alert or similar call pursuant to a TCPA exception to the general consent requirement. The Commission did not explain why it imposed the limitation, but we believe it was likely to ensure that financial institutions would not call or alert the wrong consumers. We now believe that allowing an exception for fraud alert and similar calls only when a financial institution calls the number provided by the consumer might unduly restrict critical calls about the consumer's financial accounts. We believe that financial institutions have incentives to ensure they are calling only their customer. We seek comment on this view.

84. Are there significant concerns about misdirected calls or about financial information being improperly disclosed if we were to broaden the exception for fraud alert and similar calls to cover calls to numbers other than those provided by consumers? Does the ability of financial institutions to obtain prior express consent for such calls, and thus to make calls outside the exception, resolve these concerns? Are there applicable federal or state laws or best practices with which we should align our proposal to alleviate any such concerns? Would it improve the ability of financial institutions to reach consumers and reduce consumers' exposure to fraud? How does the risk of misdirected calls weigh against the benefits of allowing financial institutions to better reach consumers? Are there other factors we should consider?

3. Call Blocking Rules

85. *Call Blocking Rules.* We propose to eliminate the rules permitting voice

service providers to block calls that are on a do-not-originate list or that purport to be from a NANP number that is invalid, unallocated, or unused. Because the Commission has adopted rules that require voice service providers to do what these rules merely permit, we believe that these provisions will become outdated when the new rules become effective. We seek comment on this proposal.

Initial Regulatory Flexibility Analysis

86. 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 Further Notice of Proposed Rulemaking (*FNPRM)* assessing the possible significant economic impact on a substantial number of small entities. The Commission requests written public comments on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments specified on the first page of the *FNPRM.* The Commission will send a copy of the *FNPRM* including this IRFA, to the Chief Counsel for the SBA Office of Advocacy. In addition, the *FNPRM* and IRFA (or summaries thereof) will be published in the **Federal Register**.

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

87. The Commission initiates this proceeding to enhance consumer protection against potentially unlawful and fraudulent robocalls. While the existing STIR/SHAKEN call authentication framework indicates whether a caller is authorized to use a particular number, it does not identify who is calling, meaning consumers often cannot determine the caller's identity unless the number is in their contact list or they otherwise recognize it. Additionally, consumers may not understand this limitation, mistakenly believing that A-level attestation provides assurance that a call is lawful rather than a scam or otherwise unlawful.

88. To address these issues, this document proposes the following: (1) When a voice service provider provides caller identification service and includes in the caller identification information for a call an indication that the call has received A-level attestation, the voice service provider must include a verified caller name in the caller identification information; (2) a voice service provider that transmits caller identity information for an originating telephone call must employ reasonable measures to verify that the caller identify information is accurate; and (3) voice service providers that are the entry point into the United States for calls that originate from outside of the United States and know or have a reasonable basis to know that a call originated from a country other than the United States must include in the caller identification information for that call an indication that the call originated from a country other than the United States. These measures are intended to restore consumer confidence in caller ID information and reduce the burden on consumers of screening unlawful or potentially unlawful calls.

89. We also propose to modernize anti-robocall protections by eliminating outdated requirements that have been superseded by technological advances and calling practices and to enhance regulatory certainty by dismissing older pending petitions and applications related to TCPA implementation.

B. Legal Basis

90. The proposed action is authorized pursuant to sections 1–4, 201(b), 202(a), 227, 227b, and 251(e)of the Communications Act of 1934, as amended, and 47 U.S.C. 151–154, 201, 202, 227, 227b, and 251(e).

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

91. 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 (SBA). 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. The SBA establishes small business size standards that agencies are required to use when promulgating regulations relating to small businesses; agencies may establish alternative size standards for use in such programs, but must consult and obtain approval from SBA before doing so.

92. Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe three broad groups of small entities that could be directly affected by our actions. 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, ''small organizations'' are not-for-profit enterprises that are independently owned and operated and not dominant their field. While we do not have data regarding the number of non-profits that meet that criteria, over 99 percent of nonprofits have fewer than 500 employees. Finally, ''small governmental jurisdictions'' are defined as cities, counties, towns, townships, villages, school districts, or special districts with populations of less than fifty thousand. Based on the 2022 U.S. Census of Governments data, we estimate that at least 48,724 out of 90,835 local government jurisdictions have a population of less than 50,000.

93. The rules proposed in this document will apply to small entities in the industries identified in the chart below by their six-digit North American Industry Classification System (NAICS) codes and corresponding SBA size standard. Based on currently available U.S. Census data regarding the estimated number of small firms in each identified industry, we conclude that the proposed rules will impact a substantial number of small entities. Where available, we also provide additional information regarding the number of potentially affected entities in the above identified industries.

TABLE 1—CENSUS BUREAU DATA BY NAICS CODE TABLE

Regulated industry (NAICS classification)	NAICS code	SBA size standard	Total firms	Small firms	% Small firms in industry
Telephone Apparatus Manufacturing	334210	1,250 employees	189	177	93.65
Wired Telecommunications Carriers	517111	1,500 employees	3,054	2,964	97.05
Wireless Telecommunications Carriers (except Satellite)	517112	1,500 employees	2,893	2,837	98.06

TABLE 1—CENSUS BUREAU DATA BY NAICS CODE TABLE—Continued

Regulated industry (NAICS classification)	NAICS code	SBA size standard	Total firms	Small firms	% Small firms in industry
Telecommunications Resellers	517121	1,500 employees	1,386	1,375	99.21
Satellite Telecommunications	517410	$47 million	275	242	88.00
All Other Telecommunications	517810	$40 million	1,079	1,039	96.29

TABLE 2—TELECOMMUNICATIONS SERVICE PROVIDER DATA

2024 Universal service monitoring report telecommunications service provider data (data as of December 2023)	SBA size standard (1,500 employees)		
Affected entity	Total # FCC Form 499A filers	Small firms	% Small entities
Competitive Local Exchange Carriers (CLECs)	3,729	3,576	95.90
Incumbent Local Exchange Carriers (Incumbent LECs)	1,175	917	78.04
Interexchange Carriers (IXCs)	113	95	84.07
Local Exchange Carriers (LECs)	4,904	4,493	91.62
Toll Resellers	411	398	96.84
Wired Telecommunications Carriers	4,682	4,276	91.33
Wireless Telecommunications Carriers (except Satellite)	585	498	85.13
Wireless Telephony	326	247	75.77

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

94. 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.

95. The *NPRM* seeks comment on proposals that may establish new information collection, reporting, recordkeeping, or compliance requirements for small entities. Specifically, it proposes to require terminating voice service providers that indicate a call has received A-level attestation to also provide verified caller identity information for such calls. This could require affected small entities to implement systems and processes to provide verified caller names or other caller identity information when they choose to provide A-level attestation indicators to consumers.

96. This document also proposes to require originating voice service providers that transmit caller identity information to take steps to verify that the information is accurate. This may require affected small entities to establish verification procedures, maintain records of verification activities, and implement systems to ensure caller identity information transmitted with calls is accurate before transmission.

97. This document also proposes that voice service providers that are the entry point into the United States for calls that originate from outside of the United States and know or have a reasonable basis to know that a call originated from a country other than the United States must include in the caller identification information for that call an indication that the call originated from a country other than the United States. To comply with this requirement, affected small entities may need to establish procedures indicating when a call originated from a country other than the United States.

98. The Commission also proposes to modernize anti-robocall protections by eliminating outdated requirements that have been superseded by technological advances and calling practices and to enhance regulatory certainty by dismissing older pending petitions and applications related to TCPA implementation. If adopted, this may reduce the recordkeeping and compliance burden on small entities.

99. The Commission invites comment on the costs and burdens of these proposals on small entity voice service providers, telemarketing bureaus, equipment manufacturers, and other affected small entities. The Commission expects that information received in comments, including cost and benefit analyses where requested, will help the Commission identify and evaluate relevant compliance matters for small entities that may result if the proposals and associated requirements discussed in the document are ultimately adopted.

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

100. 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.''

101. In the *NPRM,* the Commission seeks comment on several approaches that may minimize impacts on small entities. First, the Commission proposes that the caller identity information requirements would apply only when a terminating provider chooses to transmit for presentation on consumers' handsets an indication of A-level attestation, rather than mandating that all providers provide such indicators. This approach allows small entities flexibility in deciding whether to provide attestation indicators and thus

whether to be subject to the associated caller identity requirements.

102. Second, the Commission seeks comment on alternative technical solutions beyond Rich Call Data (RCD) for securely transmitting caller identity information. This approach would provide small entities with flexibility to choose cost-effective solutions that work with their existing network infrastructure rather than mandating a single technical standard that might be burdensome for smaller providers.

103. Third, the Commission seeks comment on whether certain categories of calls or providers should be exempted from caller identity verification requirements, which could reduce compliance burdens on small entities that primarily handle such calls.

104. Additionally, the Commission proposes to eliminate several outdated robocall requirements that may represent unnecessary burdens on small entities, including call abandonment rules that technology and calling practices have overtaken.

105. The Commission expects to more fully consider the economic impact and alternatives for small entities following review of comments filed in response to the *NPRM* and this IRFA. The Commission's evaluation of this information will shape the final alternatives it considers, the final conclusions it reaches, and any final actions it ultimately takes in this proceeding to minimize any significant economic impact that may occur on small entities.

F. Federal Rules That May Duplicate, Overlap, or Conflict With the Proposed Rules

106. None.

List of Subjects in 47 CFR Part 64

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

Federal Communications Commission.

Marlene Dortch,

Secretary.

Proposed Rules

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

PART 64—MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

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

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

Subpart L—Restrictions on Telemarketing, Telephone Solicitation, and Facsimile Advertising

■ 2. Amend § 64.1200 by
■ a. Removing and reserving paragraphs (a)(6) and (7), (a)(9)(iii)(A), (a)(10);
■ b. Revising the first sentence of paragraph (b)(2);
■ c. Removing and reserving paragraphs (k)(1), (k)(2)(i) through (iii); and
■ d. Revising paragraph (k)(3)(ii).

The revisions read as follows:

§ 64.1200 Delivery restrictions.

* * * * *

(b) * * *

(2) During or after the message, state clearly the telephone number (other than that of the autodialer or prerecorded message player that placed the call) of such business, other entity, or individual; and * * *

* * * * *

(k) * * *

(3) * * *

(ii) Those analytics include consideration of caller identification authentication information and information that a call originated from outside of the United States, where such information is available;

* * * * *

Subpart P—Calling Party Telephone Number; Privacy

■ 3. Amend § 64.1600 by adding paragraphs (s) and (t) to read as follows:

§ 64.1600 Definitions.

* * * * *

(s) The term ''caller identity information'' has the same meaning given the term ''caller identification information'' in 47 CFR 64.1600(c) as it currently exists or may hereafter be amended, but excludes the information contained in 47 CFR 64.1600(g)(1)–(2) and (5).

* * * * *

■ 4. Add § 64.1607 to subpart P to read as follows:

§ 64.1607 Verification, Transmission, and Presentation of Caller Identity Information.

(a) When a voice service provider includes in caller identification information transmitted to a called party an indication that the call has received an A-level attestation pursuant to the Caller Identification Authentication requirements contained in subpart HH of this part, the voice service provider must include verified caller name in the caller identification information transmitted to the called party.

(b) A voice service provider that transmits caller identity information for an originating telephone call must employ reasonable measures to verify that the caller identity name is accurate.

(c) Gateway providers must include in the caller identification information for a call that originates outside the United States an indication that the call originated from outside of the United States.

(d) Non-gateway intermediate providers within a call path must pass unaltered to subsequent providers in the call path caller identification information identifying the call as having originated from outside of the United States.

(e) When a voice service provider is the terminating voice service provider for a call and knows or has a reasonable basis to know that a call originated from outside of the United States, such as when the caller identification information it receives for that call includes an indication that the call originated from outside of the United States, the voice service provider must include in the caller identification information transmitted to the called party for that call an indication that the call originated from outside of the United States.

[FR Doc. 2025–22063 Filed 12–4–25; 8:45 am]

BILLING CODE 6712–01–P

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 64

[WC Docket Nos. 12–375, 23–62; FCC 25–75; FR ID 319623]

Incarcerated People's Communication Services; Implementation of the Martha Wright-Reed Act; Rates for Interstate Inmate Calling Services

AGENCY: Federal Communications Commission.

ACTION: Proposed rule.

SUMMARY: In this document, the Federal Communications Commission (Commission) seeks additional comment and data from stakeholders on adopting permanent audio and video IPCS rate caps and on whether and how the Commission should refine its IPCS data collections going forward to provide the data needed to ensure rate caps are just and reasonable and fairly compensate IPCS providers. It also seeks comment on how and when the Commission should structure a permanent rate