October 7, 2025

FCC FACT SHEET*
Call Branding FNPRM
Improving Verification and Presentation of Caller Identification Information

Further Notice of Proposed Rulemaking and Public Notice – CG Docket Nos. 17-59, 02-278, 25-307, and WC Docket No. 17-97

Background: The STIR/SHAKEN framework can help consumers identify when the number displayed for an incoming call may be spoofed (i.e., faked), but it does not let them know who is calling. In this *Further Notice of Proposed Rulemaking and Public Notice*, the Commission proposes to ensure that consumers receive accurate, verified caller name information. The Commission also proposes significant steps to stop a major source of illegal calls – those that originate from outside of the United States. These proposals advance two robocalls priorities – stopping illegal calls before they reach consumer phones and empowering consumers with more information about calls so they can better decide whether to answer them. The notice also proposes to modernize other anti-robocall protections.

What the Notice of Proposed Rulemaking Would Do:

- Propose to define "caller identity information".
- Propose to require terminating voice service providers to transmit verified caller name information to the called party whenever they transmit call authentication information indicating that the originating number is unlikely to be spoofed.
- Propose to require originating voice service providers to verify caller identity information.
- Propose to require gateway providers to mark calls that originate from outside of the United States.
- Propose to require non-gateway intermediate voice service providers within a call path to pass unaltered to subsequent providers in the call path caller identification information identifying the call as having originated from outside of the United States.
- Propose to require terminating voice service providers to transmit to called parties 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.
- Seek comment on prohibiting spoofing of United States telephone numbers for calls that originate outside the United States.
- 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.
- Propose to simplify, streamline, or eliminate certain outdated robocall rules.
- Provide public notice of intent to clean up regulatory backlog by dismissing older petitions for reconsideration and applications for review related to the Telephone Consumer Protection Act.

* This document is being released as part of a "permit-but-disclose" proceeding. Any presentations or views on the subject expressed to the Commission or its staff, including by email, must be filed in CG Docket Nos. 17-59, 02-278, and 25-307, and WC Docket No. 17-97, which may be accessed via the Electronic Comment Filing System (https://www.fcc.gov/ecfs). Before filing, participants should familiarize themselves with the Commission's *ex parte* rules, including the general prohibition on presentations (written and oral) on matters listed on the Sunshine Agenda, which is typically released a week prior to the Commission's meeting. *See* 47 CFR § 1.1200 *et seq*.

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

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97
	)	
Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991	)	CG Docket No. 02-278
	)	
Dismissal of Outdated or Otherwise Moot Robocalls Petitions	)	CG Docket No. 25-307

NINTH FURTHER NOTICE OF PROPOSED RULEMAKING IN CG DOCKET NO. 17-59; SEVENTH FURTHER NOTICE OF PROPOSED RULEMAKING IN WC DOCKET NO. 17-97; FURTHER NOTICE OF PROPOSED RULEMAKING IN CG DOCKET NO. 02-278; PUBLIC NOTICE IN CG DOCKET NO. 25-307[*]

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

Comment Date: (30 days after date of publication in the Federal Register)
Reply Comment Date: (60 days after date of publication in the Federal Register)

Deadline for Responses to Public Notice: 45 days after publication in the Federal Register

By the Commission:

TABLE OF CONTENTS

Heading Paragraph #

I. INTRODUCTION 1
II. BACKGROUND 4
A. STIR/SHAKEN Framework and Rich Call Data 9
B. Presenting Caller Name 14
C. Calls Originating from Outside of the United States 20

[*] This document has been circulated for tentative consideration by the Commission at its October 2025 open meeting. The issues referenced in this document and the Commission's ultimate resolution of those issues remain under consideration and subject to change. This document does not constitute any official action by the Commission. However, the Chair has determined that, in the interest of promoting the public's ability to understand the nature and scope of issues under consideration, the public interest would be served by making this document publicly available. The FCC's *ex parte* rules apply and presentations are subject to "permit-but-disclose" *ex parte* rules. *See, e.g.*, 47 C.F.R. §§ 1.1206, 1.1200(a). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules, including the general prohibition on presentations (written and oral) on matters listed on the Sunshine Agenda, which is typically released a week prior to the Commission's meeting. *See* 47 CFR §§ 1.1200(a), 1.1203.

D. Telephone Consumer Protection Act 22
III. DISCUSSION 23
A. Need for Improved Caller Identity Information 24
B. Defining Caller Identity Information 27
C. Transmitting Caller Identity Information to Consumers 30
1. Requiring Transmission of Caller Identity Information to Consumers when A-Level Attestations are Indicated 30
2. Requiring Originating Providers to Verify that Transmitted Caller Identity Information is Accurate 43
3. Securely Transmitting Caller Identity Information 48
D. Calls Originating from Outside of the United States 68
E. Legal Authority 87
F. Costs and Benefits 91
IV. ELIMINATING OUTDATED RULES 94
A. Telephone Consumer Protection Act Rules and Do-Not-Call Implementation Act Rules 95
1. Older Rules That Might No Longer be Necessary 95
2. More Recent Rules That Might Harm Consumers 103
B. Call Blocking Rules 109
V. PUBLIC NOTICE REGARDING OLDER PETITIONS AND APPLICATIONS RELATED TO THE TELEPHONE CONSUMER PROTECTION ACT 110
VI. PROCEDURAL MATTERS 113
A. Initial Regulatory Flexibility Act Analysis 113
B. Initial Paperwork Reduction Act Analysis 114
C. Filing Requirements—Comments and Replies 115
D. Ex Parte Rules 116
E. Providing Accountability Through Transparency Act 117
F. Additional Information 118
VII. ORDERING CLAUSES 119
APPENDIX A – PROPOSED RULES
APPENDIX B – INITIAL REGULATORY FLEXIBILITY ANALYSIS

I. INTRODUCTION

1. Consumers have the right to choose which calls they answer, but that choice is meaningful only when they know who is calling. Call authentication under the STIR/SHAKEN framework can help consumers by letting them know whether an originating number is spoofed (i.e., faked). While call authentication helps consumers, it often does not let them know who is calling.

2. In this *Notice*, we propose to require that providers give consumers accurate caller name and other information that enables them to regain control of their phones by ensuring they no longer have to guess whether a call is one they want to pick up. Specifically, we propose to require terminating voice service providers to transmit verified caller name[1] for presentation on consumers' handsets[2] whenever they transmit call authentication information indicating that the originating number is unlikely to be spoofed. We further propose ways for originating voice service providers to verify that the caller name and other information about the caller that they transmit is accurate and secure so that consumers can trust

[1] We use "caller name" to refer to the name of the caller that is transmitted for presentation on the called party's handset. Commonly used industry terms like "calling name" and "display name" generally have the same meaning.

[2] We use "handset" to refer to any user equipment a called party uses at the terminating end point of a call, including any assistive device, service, or technology used by a person with a disability. Caller identification information (see 47 CFR § 64.1600(c)) might be presented to consumers in various ways depending upon the features and functionalities of the handset and any assistive device, service, or technology the called party uses.

it. Because many unlawful robocalls originate from outside the United States, we also propose to ensure that consumers know which calls originate from a foreign country and to improve call blocking analytics by considering whether a call originated from outside of the United States.

3. As we move toward modernizing our anti-robocall protections, we also propose to simplify, streamline, or eliminate some of our possibly outdated requirements that technology and calling practices have overtaken. And we provide notice of our intent to dismiss some older petitions for reconsideration and applications for review related to the Telephone Consumer Protection Act (TCPA).[3]

II. BACKGROUND

4. In the 1980s, advances in technology enabled the originating provider to transmit the originating telephone number along with a call. This allowed terminating providers to transmit the telephone number to the called party, which could be presented with the aid of a device attached to a wireline telephone. To enhance the information provided to the called party, terminating providers began to query the Caller ID Name (CNAM) databases to identify and transmit the subscriber name associated with the number. The accuracy of the name presented to the called party depended upon the accuracy of the CNAM databases.

5. For the first time, consumers could identify the caller before deciding whether to answer the call. Unfortunately, scammers and other bad actors making unlawful calls learned to spoof telephone numbers, tricking consumers about the identity of the caller and helping unlawful callers to hide their true identities.

6. Congress, the Commission, and the industry have taken a series of steps to address spoofing which sometimes is used to make a scam call more likely to be answered. In 2009, Congress adopted the Truth in Caller ID Act,[4] which made it unlawful to use a caller identification service to transmit inaccurate or misleading information in order to "defraud, cause harm, or wrongfully obtain anything of value."[5] Subsequently, the industry developed the STIR/SHAKEN caller ID authentication framework. This made spoofing more difficult by providing a mechanism for: (a) the originating provider, using encryption, to securely transmit the originating telephone number and attest to its trust in the number's validity; and (b) the terminating provider to verify that the originating number had not been altered during transmission.

7. In 2019, Congress enacted the TRACED Act,[6] with the stated purpose of "helping to reduce illegal and unwanted robocalls."[7] Along with other provisions directed at addressing robocalls, the TRACED Act directed the Commission to require all voice service providers to implement STIR/SHAKEN in their IP networks.[8] In 2020, consistent with Congress' direction, the Commission took the first step toward rebuilding trust in caller ID information by requiring providers to implement the

[3] Telephone Consumer Protection Act, Pub. L. No. 102-243, 105 Stat. 2394 (TCPA). A few of these petitions and applications also were filed in a docket, CG Docket No. 05-338, related to the Junk Fax Prevention Act of 2005, Pub. L. No. 109-21, 119 Stat. 359 (2005) or in CG Docket No. 17-59, which generally addresses ways to eliminate unlawful robocalls. Two, apparently duplicate, petitions appear to have been filed in CG Docket No. 02-278 only, although they also reference WC Docket No. 07-135 in the caption. *See infra* para. 112 and note 133.

[4] Truth in Caller ID Act of 2009, Pub. L. No. 111-331, 124 Stat. 3572 (2010).

[5] 47 USC § 227(e)(1).

[6] *See* Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105, 133, Stat. 3274 (2019) (TRACED Act).

[7] S. Comm. on Com., Sci., & Transp., Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, S. Rep. No. 116-41, at 1 (2019).

[8] *See* 47 USC § 227b(b)(1)(A).

STIR/SHAKEN framework in their IP networks.[9] The Commission expanded that obligation in the following years, and all providers were required to complete implementation by June 30, 2023, subject to certain extensions.[10] A recent study suggests that large providers utilize STIR/SHAKEN on 86% of the traffic exchanged between them, but a significant number of calls arrive at terminating providers without authentication information because STIR/SHAKEN works only on IP networks and portions of the national network have not transitioned to IP.[11]

8. While STIR/SHAKEN has reduced number spoofing, legacy CNAM databases currently remain the only widespread source of caller name information, but because those databases reportedly are not reliably accurate and are subject to manipulation, concerns exist about their continued use.[12] Rich Call Data (RCD) and other potential solutions that capitalize upon the capabilities of IP networks offer alternatives to CNAM databases for transmission of caller identification information.

A. STIR/SHAKEN Framework and Rich Call Data

9. *STIR/SHAKEN Framework.* STIR/SHAKEN is a set of technical standards and protocols for IP networks that allows authenticated information about a call to travel with the call along the call path.[13] These technical standards and protocols establish how voice service providers can transmit encrypted information about a caller and its relationship to the originating phone number as a means to deter impermissible number spoofing.[14] Under STIR/SHAKEN, providers that are responsible for placing a call onto the IP network insert certain information about the call into an encrypted "PASSporT" that travels with the call. This information includes the provider's name and digital signature, the originating telephone number, and an attestation – A, B, or C – regarding the level of knowledge the provider asserts

[9] *Call Authentication Trust Anchor, Implementation of TRACED Act Section 6(a) – Knowledge of Customers by Entities with Access to Numbering Resources*, WC Docket Nos. 17-97 and 20-67, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3241 (2020) (*First Caller ID Authentication Report and Order*); *see also Call Authentication Trust Anchor*, WC Docket No. 17-97, Notice of Proposed Rulemaking, FCC 25-25, 2025 WL 1267021, at *2 (Apr. 29, 2025) (*Non-IP Authentication NPRM*) ("The Commission requires providers obligated to implement STIR/SHAKEN to follow, at a minimum, ATIS-1000074, ATIS-1000080, and ATIS-1000084, and all documents referenced therein. These documents, published and periodically amended by ATIS, establish both: (1) the technical requirements for authenticating calls; and (2) the governance system underlying STIR/SHAKEN.").

[10] *See* 47 CFR §§ 64.6301, 64.6302, 64.6303, 64.6304. Additionally, all providers that lack control over the network infrastructure necessary to implement STIR/SHAKEN are exempt from its implementation. *See First Caller ID Authentication Report and Order*, 35 FCC Rcd at 3260, para. 40.

[11] *See* TNS, *TNS 2025 Robocall Report: Top Carriers' Signed Traffic Success Enhances Robocall Mitigation Efforts*, https://tnsi.com/resource/com/tns-2025-robocall-report-unveils-new-insights-press-release (Feb. 4, 2025). The Commission recently initiated a proceeding to examine whether there exists non-IP caller ID authentication frameworks that meet the requirements in the TRACED Act and whether to require providers who have not completed their IP transitions to implement one or more of these frameworks in their non-IP networks by a date certain. *See Non-IP Authentication NPRM.*

[12] *See*, *e.g.*, Numeracle Comments, CG Docket No. 17-59, at 28 (rec. Aug. 9, 2023) ("CNAM is obsolete and insecure."); YouMail Comments, CG Docket No. 17-59, at 26-27 (rec. Aug. 9, 2023) (YouMail 17-59 Comments) ("significant variability to the accuracy of these databases" and some makers of lawful calls manipulate CNAM data, sometimes with misleading or fraudulent names, to increase probability that a call will be answered).

[13] *See, e.g.,* FCC, Wireline Competition Bureau, *Triennial Report on the Efficacy of the Technologies Used in the STIR/SHAKEN Caller ID Authentication Framework*, at 3 (Dec. 30, 2022).

[14] *Call Authentication Trust Anchor*, WC Docket No. 17-97, Eighth Report and Order, 39 FCC Rcd 12894, 12896-97, paras. 5-6 (2024). *See* IETF, *Secure Telephone Identity Revisited (stir): Documents*, https://datatracker.ietf.org/wg/stir/documents (last visited Sept. 29, 2025) (listing standards and current work-in-progress); ATIS & SIP Forum, *Joint ATIS/SIP Forum Standard—Signature-Based Handling of Asserted Information Using toKENs (SHAKEN)* (2022), https://access.atis.org/higherlogic/ws/public/download/67436. (ATIS-1000074v.003).

it has about its direct customer's identity and that customer's right to use the number transmitted.[15] A provider may assert A-level attestation when (1) it is responsible for the origination of the call onto the IP network, (2) has a direct authentication relationship with its customer and can identify the customer, and (3) has established a verified association between its customer and the telephone number used for the call. It may assert B-level (aka partial) attestation when it can satisfy elements (1) and (2), but not (3). It must assert C-level attestation when the provider is the entry point onto the IP network of a call that originated elsewhere and the provider has no relationship with the initiator of a call, such as when a provider is acting as an international gateway.[16] In instances where the authenticating provider's direct customer is another, upstream provider (e.g., a reseller), not its own end user, the authenticating provider's attestation relates to its knowledge about that upstream provider's identity and right to use the number.[17] The authenticating provider transmits the call information downstream in the PASSporT, and any intermediate providers must pass the information downstream unaltered until it reaches the terminating provider. The terminating provider must decrypt and verify the digital signature of the authenticating provider.[18]

10. STIR/SHAKEN gives consumers a greater level of trust that the phone numbers indicated for incoming calls are not spoofed.[19] Calls receiving an A-level attestation carry the best available assurance that the number has not been spoofed. Calls receiving partial (B-Level) or gateway (C-Level) attestation are not necessarily spoofed, but they lack the assurance of the highest attestation level. In addition to STIR/SHAKEN's anti-spoofing benefits, providers may use attestation information in their call analytics tools to assist with call blocking and labeling decisions.[20]

11. Terminating providers often transmit to consumers' handsets some indication that an originating telephone number received a verified A-level attestation.[21] Depending on the called party's handset and its operating system, an indicator, such as a green checkmark, might be presented to the

[15] ATIS-1000074.v.003 at 12-13.

[16] *Id.*; *see also Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Report and Order, 35 FCC Rcd 15221, 15228, n.47 (2020).

[17] ATIS-1000088, A Framework for SHAKEN Attestation and Origination Identifier at 13 (2020), https://www.sipforum.org/download/a-framework-for-shaken-attestation-and-origination-identifier-atis-1000088/?wpdmdl=3942&refresh=5f888a7c999f11602783868 ("'[C]ustomer refers to the direct customer of the originating [service provider (SP)]. Where the originating SP has assigned the calling [telephone number (TN)] or the customer has provided evidence that it has authorization to use the calling TN itself, the originating SP can mark an "A" attestation without reference to authorizations of any indirect end users (e.g., in a reseller or VASP scenario). In some other scenarios [(e.g., the reseller's end-user placed the call]. . . [,] the SP's customer should provide assurances that they can trace the identity of an indirect end user and that user's authorization to utilize a calling TN.").

[18] *Non-IP Authentication NPRM*, 2025 WL 1267021, at *3; 47 CFR § 64.6300(a); ATIS-1000074v.003 at 8-9.

[19] Phone numbers may be spoofed permissibly in certain circumstances, such as when a business chooses to present its main contact number instead of a number it uses only to make outbound calls. *See*, *e.g.*, TransNexus, *Understanding STIR/SHAKEN*, https://transnexus.com/whitepapers/understanding-stir-shaken (last visited Sept. 29, 2025).

[20] TransUnion, *What are the Attestation Levels for STIR/SHAKEN*, https://www.transunion.com/blog/what-are-the-attestation-levels-for-stir-shaken (Aug. 6, 2024) ("Today, a call's attestation value is increasingly being used as an input for service provider robocall analytic algorithms to help determine its risk level.").

[21] *See*, *e.g.*, INCOMPAS Comments, CG Docket No. 17-59, at 13 (rec. Aug. 9, 2023) (INCOMPAS 17-59 Comments); *see also* North American Numbering Council Call Authentication Working Group, Best Practices for Terminating Voice Service Providers Using Caller ID Authentication Information, at 5 (Feb. 9, 2022), https://docs.fcc.gov/public/attachments/DOC-383601A1.pdf (*Call Authentication Best Practices*) ("Usually call authentication information is displayed to the end user with a check mark (by sending 'verstat=TN-Validation-Passed' to the consumer's handset, an enterprise's PBX, etc.) or a '[V]' (by modifying the caller display name) when the call receives full attestation.").

consumer while the phone is ringing, during the call, solely in the call log after the call, or not at all.[22] While terminating providers might also transmit other information, such as a spam label, this information might not be related to the STIR/SHAKEN A-level attestation information they transmit and could be misleading or confusing to consumers.

12. *Rich Call Data.* RCD builds upon the STIR/SHAKEN framework by increasing the amount of data – in addition to the originating telephone number and the attestation level claim – that the originating provider can transmit with a call over an IP network using encryption. Like STIR/SHAKEN, RCD is implemented through a set of standards developed by the Internet Engineering Task Force (IETF) and the Alliance for Telecommunications Industry Solutions (ATIS), two industry standards-setting organizations.[23] Under the standards, caller identity information[24] transmitted using RCD can include name, photo, logo, email address, location, title, and the reason for the call, subject to data capacity limits.[25] Like STIR/SHAKEN information, terminating providers can verify that this information has not been altered during transmission and then transmit it to a consumer's handset to be presented if the handset and its operating system are configured to permit such presentation.

13. RCD differs from legacy CNAM-based methods for obtaining and presenting caller name in two key ways. First, instead of the terminating provider querying a third-party database to obtain the name associated with the originating telephone number, RCD relies upon the caller's service provider to provide and transmit the caller name, along with any other caller identity information that can be transmitted using RCD. Second, RCD relies upon authentication by the originating provider and verification by the terminating provider within the STIR/SHAKEN framework.[26] RCD builds on the STIR/SHAKEN authentication foundation but is governed by a separate ATIS standard that addresses the transmission of caller identity information. Importantly, however, the determination of the attestation level still applies only to the authenticating provider's knowledge of its direct customer and that customer's right to use the telephone number it transmits. The ATIS RCD standard, however, requires

---

[22] *See, e.g.*, *Call Authentication Best Practices* at 5; TransNexus, Apple supports STIR/SHAKEN checkbox in iOS 13 (Sept. 20, 2019), https://transnexus.com/blog/2019/ios13-shaken-display ("The Apple iOS features list includes a feature for 'carrier-verified calls.' This feature will indicate calls that have been verified by STIR/SHAKEN. . . . Note that this only mentions the recent list and does not mention the call answer display."); TransUnion, What does "verified by the carrier" mean on phone calls (Jun. 7, 2024), https://www.transunion.com/blog/what-does-verified-by-the-carrier-mean-on-phone-calls ("Today, most Samsung devices display a checkmark indicating the call has been authenticated using STIR/SHAKEN.").

[23] The IETF recently published the finalized RCD in the form of two technical standards. *See* Internet Engineering Task Force, RFC 9795, Personal Attestation Token (PASSporT) Extension for Rich Call Data (July 2025), https://www.rfc-editor.org/rfc/rfc9795.pdf; Internet Engineering Task Force, RFC 9796, SIP Call-Info Parameters for Rich Call Data at 4-5 (July, 2025), https://www.rfc-editor.org/rfc/rfc9796.pdf. The RCD information specified by both standards can be conveyed to the called endpoint and viewed by the end user. However, in the case of RFC 9795, the RCD information is protected within the Identity header field, while in RFC 9796, the RCD information is considered unprotected and conveyed in the p-asserted identity header as defined in a separate RFC standard. The choice of which method is used is based on local policy as stated in an ATIS RCD standard, the latest version of which was published in April 2025. *See* ATIS-1000094v.002, Signature-based Handling of Asserted Identity Using toKENs (SHAKEN): Calling Name and Rich Call Data Handling Procedures (Revision 1). We use "Rich Call Data" or "RCD" to refer to RCD as implemented according to these IETF and ATIS RCD technical standards unless otherwise indicated.

[24] As discussed more fully in Part III.B., we use the term "caller identity information" 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 number information.

[25] *See* RFC 9795 at 7-10.

[26] *See, e.g.*, TransNexus, *Rich Call Data and Stir/Shaken*, https://transnexus.com/whitepapers/rich-call-data (last visited Sept. 29, 2025).

the originating voice service provider to vet the caller identity information it transmits.[27]

B. Presenting Caller Name

14. To help consumers identify callers more easily, the Commission sought comment in 2023 on a proposal to require terminating voice service providers to provide accurate caller name information to called parties whenever they transmit information that is used to indicate that a call received an A-level attestation.[28] The Commission also inquired about the use of CNAM databases for this purpose.[29] There was broad agreement among commenters that CNAM databases should not be used for this purpose because, they asserted, CNAM databases are error prone and unreliable.[30]

15. Commenters who supported transmitting trusted caller name information to consumers stated that having that information would make it easier for consumers to spot fraudulent calls, including ones that had received an A-level attestation.[31] Supporters urged the Commission to require use of an end-to-end verification methodology, such as RCD.[32] Others cautioned that verifying the identity of the caller does not equate to the call being lawful and noted that many calls that receive A-level attestations are spoofed, fraudulent, or otherwise unlawful.[33] Commenters noted that wireless consumers tend not to answer calls from anyone not in their contact lists, but were split over requiring voice service providers to present trusted caller name information on wireless devices.[34] Many commenters said that it was premature to adopt a proposal to require providing caller name information to consumers and urged the Commission to allow time for the industry to gain experience with RCD or other possible call branding solutions.[35] "Call branding" and "branded calling" broadly refer to the functionality provided by RCD

[27] ATIS-1000094.v.002 at 13. *See also supra* note 24.

[28] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Eighth Further Notice of Proposed Rulemaking, 38 FCC Rcd 5404, 5435-36 (2023).

[29] *Id.*

[30] *See*, *e.g.*, Numeracle Comments, CG Docket No. 17-59, at 28 (rec. Aug. 9, 2023) ("CNAM is obsolete and insecure."); YouMail 17-59 Comments at 26-27 ("significant variability to the accuracy of these databases" and some makers of lawful calls manipulate CNAM data, sometimes with misleading or fraudulent names, to increase probability that a call will be answered); US Telecom Comments, CG Docket No. 17-59, at 10 (rec. Aug. 9, 2023) (US Telecom 17-59 Comments) (CNAM databases are incomplete and unreliable, and "bad actors . . . [can] infuse misleading data."); CTIA Comments, CG Docket No. 17-59, at 7 (rec. Aug. 9, 2023) (outdated caller information) (CTIA 17-59 Comments); Twilio Comments, CG Docket No. 17-59, at 8 (rec. Aug. 9, 2023) (outdated and unvalidated data, there are multiple CNAM databases and they often contain conflicting data).

[31] *See*, *e.g.*, Ad Hoc Telecom Users Committee Comments, CG Docket No. 17-95, at 5-6 (rec. Aug. 9, 2023) ("incredibly beneficial next step to increase trust" and "reduc[es] the efficacy of scammers' robocalling tactics"); TransNexus Comments, CG Docket No. 17-59, at 2 (rec. Aug. 9, 2023) (TransNexus 17-59 Comments); INCOMPAS 17-59 Comments at 13.

[32] *See*, *e.g.*, TransNexus 17-59 Comments at 2-3; Cloud Communications Alliance Comments, CG Docket No. 17-59, at 11-12 (rec. Aug. 9, 2023); INCOMPAS 17-59 Comments at 14-15; Twilio Reply Comments, CG Docket No. 17-59, at 3-5 (rec. Sept. 8, 2023).

[33] *See*, *e.g.*, US Telecom Reply Comments, CG Docket No. 17-59, at 9 (rec. Sept. 8, 2023); National Consumer Law Center, *et al*. Reply Comments, CG Docket No. 17-59, at 8-9 (rec. Sept. 8, 2023); T-Mobile Comments, CG Docket No. 17-59, at 6-7 (rec. Aug. 9, 2023).

[34] *See*, *e.g.*, Verizon Comments, CG Docket No. 17-59, at 7 (rec. Aug. 9, 2023) (manufacturers, not voice service providers, control how wireless devices present information to consumers) (Verizon 17-59 Comments); TNS Comments, CG Docket No. 17-59, at 6 (rec. Aug. 9, 2023) (wireless consumers would benefit from receiving trusted caller information for persons not in their contact lists).

[35] *See*, *e.g.*, CTIA 17-59 Comments at 4; NCTA Comments, CG Docket No. 17-59, at 11 (rec. Aug. 9, 2023); Verizon 17-59 Comments at 1, 8; US Telecom 17-59 Comments at 12; Competitive Carriers Association Reply (continued….)

and other solutions that enable a caller to include information to convey its brand through the caller identification information presented to consumers on their handsets. This can include the caller's name, brand logo, or other information that identifies the caller with the goal of inducing the consumer to answer.[36]

16. In February 2025, the Commission encouraged providers to continue to "develop next-generation tools, such as [RCD] and branded calling solutions, to ensure that consumers receive this information," and invited industry to provide updates on progress. The Commission also noted that it might consider a mandate in the future.[37]

17. Numeracle, in a March 2025 filing, described a possible solution to validate caller name and other caller identity information using RCD. Numeracle asserts that its solution would reduce fraud resulting from manipulation of caller name data in CNAM databases and reduce instances where terminating providers identify attested calls as spam or as potentially fraudulent.[38]

18. In a May 2025 filing, TransUnion described a validation solution that enables terminating service providers to present validated information about businesses that originate calls. The validated information includes the businesses' name, logo, and call-reason information. TransUnion suggests that this would reduce both the number of fraudulent calls that are not identified as such and the number of lawful calls that incorrectly are identified as fraudulent or spam. It also highlighted the importance of ensuring that the information used to present caller name or other branding information is accurate. TransUnion did not specify whether its solution uses RCD, but asserted that its solution is based upon a combination of industry standards, including those developed by IETF, ATIS, the SIP Forum, and others.[39]

19. It appears that multiple other companies offer branded calling solutions similar to those described by Numeracle and TransUnion. For example, Hiya, Twilio, CTIA, and TNS, among others, advertise that they offer branded calling solutions.[40] It is not completely clear to what extent any of these services are proprietary or use RCD in whole or part. It is clear, however, that the capabilities described, like the solutions described by Numeracle and TransUnion, offer capabilities similar to those offered by RCD.

Comments, CG Docket No. 17-59, at 7 (rec. Sept. 8, 2023). "Call Branding" refers to solutions that enable a caller to present information about the caller, often using brand names or logos, to identify the caller. RCD could be described as a type of call branding solution in that it enables a caller to identify itself to a called party using its name, logo, and other information.

[36] *See*, *e.g.*, Twilio, *What is Branded Calling*, https://www.twilio.com/en-us/blog/insights/what-is-branded-calling (Mar. 10, 2025).

[37] *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Eighth Report and Order, FCC 25-15, 2025 WL 820883, at *9-10 (CGB Feb. 28, 2025) (*2025 Call Blocking Order*).

[38] Letter from Keith Buell, General Counsel and Head of Global Public Policy, Numeracle, to Marlene Dortch, Secretary, FCC, CG Docket No. 17-59, et al., at Attachment, p. 3 (filed Mar. 24, 2025) (*Numeracle Ex Parte*).

[39] Letter from Allison Shuster, VP and Head of U.S. Government Relations, TransUnion, to Marlene H. Dortch, Secretary, FCC, CG Docket 17-59, at Appendix A (filed May 21, 2025).

[40] Hiya, *Turn more calls into conversations with Hiya's Branded Call,* https://work.hiya.com/complimentary-call-inspection?utm_source=bing&utm_medium=cpc&utm_campaign=Branded-Call-Call-Inspection-US+SA+NZ&utm_term=set%20up%20business%20caller%20id&b=&utm_adgroup=Branded-Call&utm_content=Call-Inspection (last visited Sept. 29, 2025); Twilio, *Introducing Enhanced Branded Calling* (July 7, 2025), https://www.twilio.com/en-us/changelog/introducing-enhanced-branded-calling-, CTIA, *New Consumer Tool, Branded Calling ID to launch on Verizon's Network*, https://www.ctia.org/news/new-consumer-tool-branded-calling-id-to-launch-on-verizons-network (Sept. 15, 2025); TNS, *Enterprise Branded Calling*, https://tnsi.com/enterprise-branded-calling (last visited Sept. 29, 2025).

C. Calls Originating from Outside of the United States

20. Many robocalls originate from outside of the United States.[41] These calls include lawful calls, such as those made on behalf of a business that has offshored its call center operations.[42] They also include a substantial volume of scam or otherwise unlawful calls.[43] Unlawful robocalls that originate in foreign countries present unique and difficult challenges, including the difficulty of locating and taking legal action against the scammers.[44]

21. The Commission has acted in the past to address these robocalls, including by creating the Robocall Mitigation Database and by requiring international gateway providers, which serve as the points of entry into the United States, to take actions intended to make analytics more effective and to aid traceback efforts aimed at locating unlawful robocallers.[45] More remains to be done, however. For instance, RCD and other call branding solutions enable information about the location of the caller to be transmitted to the terminating provider and, in turn, provided to a called party.

D. Telephone Consumer Protection Act

22. The 1991 TCPA generally restricts robocalls and robotexts. Over the years, the Commission has implemented it over the course of multiple rulemakings. The rules govern many aspects of robocalling, including call abandonment, company-specific do-not-call lists, and other requirements.

III. DISCUSSION

23. 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

24. 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.[46] However, consumers often cannot be sure who is calling unless a number is

[41] *See, e.g.*, *Advanced Methods to Combat Unlawful Robocalls*, CG Docket No. 17-59, Report and Order, 37 FCC Rcd 6865 (2022) (*2022 Gateway Provider Order*).

[42] The Commission accordingly has acknowledged that blocking calls is "a serious and complicated action that must be precisely and judiciously applied to avoid blocking lawful traffic." *Id.* at 6897, para. 73. As discussed in section III.D., however, we seek comment on whether to prohibit spoofing of United States numbers for calls that originate outside of the United States.

[43] *Id. See also* resources available at the Industry Traceback Group, https://tracebacks.org/resources (last visited Sept. 29, 2025).

[44] *Id.*at 6865, para. 1.

[45] *See generally id.*

[46] *See*, *e.g.*, *First Caller ID Authentication Report and Order*, 35 FCC Rcd at 3252, para. 25.

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.

25. 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.

26. 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.[47] 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.[48] 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.[49] As many as 88% of enterprise calls are not answered,[50] 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.[51] 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.[52]

B. Defining Caller Identity Information

27. We propose to define "caller identity information" as having the same meaning given the term "caller identification information" in our rules,[53] but excluding the originating telephone number or portion thereof and billing number information.[54]

28. 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

[47] First Orion, *Press Release* (Oct. 26, 2021), https://firstorion.com/press-release-consumer-survey-brand-impact-report/; First Orion, *2021 Brand Impact Report*, https://content.firstorion.com/rs/548-FGN-268/images/BrandImpactReport_2021.pdf (last visited Sept. 29, 2025).

[48] HIYA, *State of the Call 2024*, available at https://www.hiya.com/state-of-the-call (last visited Sept. 29, 2025).

[49] *Id*.

[50] Letter from Allison Shuster, VP and Head of U. S. Government Relations, TransUnion, to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59 (filed May 21, 2025) (TransUnion Ex Parte).

[51] TNS, *Press Release* (May 8, 2025), https://tnsi.com/resource/com/consumers-prefer-to-engage-with-businesses-that-brand-calls-press-release (*TNS Press Release*).

[52] *Id*.

[53] *See* 47 § CFR 64.1600(c).

[54] *See* 47 CFR § 64.1600(g)(1) - (2) and (5).

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,"[55] which our rules define to include certain enumerated items and "[o]ther information regarding the source or apparent source of a telephone call"[56] and refer to any service or device used to provide caller identification information to a consumer as a "caller identification service."[57]

29. In the context of the TRACED Act[58] and the STIR/SHAKEN framework, however, "caller ID authentication" often is used to refer more narrowly to the originating telephone number alone.[59] 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 *Notice* 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

30. 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.

31. 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?[60]

32. 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

[55] 47 USC § 227(e)(8)(A); 47 CFR §§ 64.6300(b), 64.1600(c).

[56] 47 CFR § 64.1600(g).

[57] *See* 47 § CFR 64.1600(d).

[58] *See* 47 USC § 227b.

[59] *See*, *e.g.*, 47 CFR §§ 64.6300-63.5308. While these rules include by reference the definition of "caller identification information" contained in 47 CFR § 64.1600(c), the STIR/SHAKEN framework that these rules require voice service providers to implement requires attestation only of the originating telephone number.

[60] The Commission considered a similar issue in 2020 and declined at that time to mandate specifications voice providers must use if they choose to present STIR/SHAKEN verification results. At that time, it reasoned that verification display practices were "in their early stages of development" and expressed a desire to avoid interfering with market forces it hoped would drive presentation efforts. Given developments in the nearly six years since, however, we now believe that the proposed mandate would be appropriate. *See First Caller ID Authentication Report and Order*, 35 FCC Rcd at 3266-67, para. 54 n.200.

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.[61] 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.[62] Is our belief correct?

33. 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?

34. 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?

35. *Minimum Caller Identity Information.* Current call branding solutions generally include caller name and the option for branding, such as logos.[63] 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?

36. 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?[64] 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.[65]

37. *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

[61] TransUnion, *Why is Branded Calling Important* (June 7, 2024), https://www.transunion.com/blog/why-is-branded-calling-important.

[62] *TNS Press Release*.

[63] *See, e.g.,* CTIA 17-59 Comments at 7 (noting that branded calling solutions that rely on the STIR/SHAKEN framework include the "authentication, verification, and transport of calling name, call reason, and other enhanced caller identity information").

[64] *See* 47 USC § 227(e)(2) (prohibition on inaccurate or misleading caller identification information does not prevent or restrict any person from blocking the capability of any caller identification service to transmit caller identification information).

[65] ATIS-1000094, 14 ("The TSP shall not convey any rich call data to the called party device if the calling party has requested privacy (e.g., the received terminating INVITE request contains a Privacy header field with a privacy type of 'id'").

comment on the capabilities of the various types of handsets to present caller identity information to consumers.

38. 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.[66] 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?

39. 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?

40. *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?[67] 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?

41. 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

[66] *See, e.g.,* ATIS-100081, Technical Report on a Framework Display of Verified Caller ID (2018) (describing the technical standards for presentation of caller ID authentication and caller name information); Letter of Allison Shuster, TransUnion, to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59, Attach. A. at 6. (May 21, 2025) (explaining that the vast majority of handsets are able to present caller information).

[67] TRS is a telecommunications transmission service; it is not a telecommunications service, an information service, or voice-over-Internet-Protocol. 47 USC § 225(a)(3).

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?

42. 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

43. We propose to require originating providers[68] that transmit caller identity information to employ reasonable measures to verify the accuracy of the information transmitted.[69] 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.

44. 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

[68] In this context, an originating provider includes the voice service provider that originates a call from a direct-end-user customer, providers of call branding solutions, or anyone else who obtains the caller identity information that is transmitted from the originating end of a call.

[69] This would be in addition to existing requirements and thus would not replace them. For example, this would not replace existing standards regarding when to grant an A-level attestation. Nor would it replace a provider's obligations under section 64.1200(n)(4) of our rules. *See* 47 CFR § 64.1200(n)(4).

solution provided by a third-party vendor?[70] 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?

45. 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?

46. 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?[71] 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?

47. 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.[72] 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.

3. Securely Transmitting Caller Identity Information

48. 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

[70] We note that the ATIS RCD standard appears to allow for the signing of an RCD PASSporT with a delegate certificate, which can be obtained by an end user or provider upstream of the authenticating provider. ATIS-1000094v.2 at 12 ("A non-SHAKEN VoIP Entity shall perform RCD authentication as described in Clause 5.2.1 with the restriction that it shall construct an "rcd" PASSporT (i.e., the option to populate "rcd" PASSporT claims in a "shaken" PASSporT shall not be used by non-SHAKEN entities)….The resulting "rcd" PASSporT shall be signed with the credentials of a delegate certificate held by the non-SHAKEN VoIP Entity.").

[71] Some providers, particularly wireless providers, allow for the account holder of a multi-line account, such as a family plan, to determine the caller name associated with each line. This currently often is done through self-service, without any verification of the names provided.

[72] *See* ATIS 1000094v2; CTIA, *Branded Calling ID Best Practices*, https://api.ctia.org/wp-content/uploads/2022/11/Branded-Calling-Best-Practices.pdf (last visited Sept. 29, 2025).

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?

49. *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.[73] 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.[74] 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."[75]

50. 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?

51. 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?[76] 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

[73] *See supra* note 23 describing the two recently published IETF RCD standards (RFC 9795 and RFC 9796) and the recently published ATIS RCD standard, ATIS 1000094v.2.

[74] *See* RFC 9795 and RFC 9796.

[75] *See* RCD 9795 at 2-6 (providing overview).

[76] As we understand it, RFC 9795 is the "lead" IETF RCD standard governing transmission of caller identity information while RFC 9796 also provides for the use of optional parameters to enhance security for information in transit and to provide a specific approach to delivering the information from the terminating provider to the end-user. Is this accurate? The ATIS RCD standard, ATIS 100094v.002, describes implementation approaches for the IETF standards. We note that of the three standards, only the ATIS RCD standard requires that the call receive an A-level attestation before caller identity information can be included in the call. *See* ATIS-1000094v.002 at 13. Similarly, the ATIS RCD standard requires vetting of caller identification information, while RFC 9795 only suggests doing so as a best practice. *Compare* RFC 9795 at 22 ("[A]s a best practice, the accuracy and legitimacy of Rich Call Data information that is included in the claims is RECOMMENDED to follow a trust framework that is out of scope of this document. As with telephone numbers for the STIR framework, the authentication of Rich Call Data should follow some type of vetting process by an entity that is authoritative over determining the accuracy and legitimacy of that information."); *with* ATIS-1000094.v.002 at 13 ("The authentication service shall populate the information contained in or referenced by the 'rcd' claim based on vetted information. The source of the vetted information may be the contents of the 'rcd' claim in a verified 'rcd' PASSporT that complies with the Enhanced JWT Claim Constraints extension of the signing delegate certificate (*see* Clauses 5.3.1 and 5.3.2.3), or another source currently outside the scope of this document.")

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?

52. 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.[77] 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?

53. 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?

54. *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.[78] 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?

55. 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

[77] The initial version of the ATIS RCD standard, ATIS-1000094, was published in 2021. *See* ATIS & SIP Forum, ATIS-1000094, Signature-based Handling of Asserted Information using toKENs (SHAKEN): Calling Name and Rich Data Handling Procedures (2021), https://www.sipforum.org/activities/nni-task-force-introduction (last visited Sept. 29, 2025). The 2021 ATIS RCD standard references the two IETF draft RCD standards. *See id*. at 1. The development of the draft-ietf-stir-passport-rcd, PASSporT Extension for Rich Call Data standard, which would be finalized as RFC 9795, began in March 2016. *See* IETF, PASSporT Extension for Rich Call Data, https://datatracker.ietf.org/doc/draft-ietf-stir-passport-rcd/26/ (last visited Sept. 29, 2025) (showing development timeline). The development of the draft-wendt-sipcore-callinfo-rcd, SIP Call-Info Parameters for Rich Call Data standard, which would be finalized as RFC 9796, began in November 2019. *See* IETF, SIP Call Info Parameters for Rich Call Data, https://datatracker.ietf.org/doc/rfc9796, (last visited Sept. 29, 2025) (showing development timeline).

[78] *See, e.g.,* TransUnion, *Branded Calling for Business*, https://www.transunion.com/faq/branded-calling-for-businesses, (last visited Sept. 29, 2025) ("We fully support that approach, particularly because our branded calling solution leverages rich call content to supplement the delivery of call authentication 'Out-of-Band' — allowing the carrier receiving the call to verify it and retrieve the rich call content that will appear on the consumer's mobile phone display.")

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?

56. 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?

57. *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.

58. *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?

59. 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?

60. 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?

61. 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?

62. 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.[79] We received limited comment on the use of RCD and alternatives on non-IP networks and now seek additional, focused comment.[80] 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?

63. *Requiring Caller Identity Information Verification as a Condition of A-Level Attestation*. Because we propose in this *Notice* 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.[81] 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.

64. 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?

65. 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

[79] *Non-IP Authentication NPRM*, 2025 WL 1267021 at *15-16, paras. 42-46.

[80] *See e.g.,* TransNexus Comments, CG Docket No. 17-97, at 5 (noting that it is important that RCD information is preserved during transmission to the terminating provider); TransNexus Reply Comments, CG Docket No. 17-97 at 19 (Aug. 15, 2025) (supporting preservation of call authentication information).

[81] *See* ATIS-100074v.003 at 12.

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?

66. 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,[82] how should we balance the goals of improving caller identity assurance with the existing functionality of the STIR/SHAKEN framework?

67. *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

68. *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.

69. We believe that transmitting such information through the entire call path and the

[82] *Wireline Competition Bureau Seeks Comment on Two Periodic TRACED Act Obligations Regarding STIR/SHAKEN Caller ID Authentication*, WC Docket No. 17-97, Public Notice, DA 25-763 (WCB 2025).

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.

70. 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?[83] 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?[84]

71. 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?[85]

72. 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

[83] The OrigID is one of the mandated fields sent in the SHAKEN PASSporT along with the attestation-level indicator, destination telephone number, originating telephone number and timestamp. *See* ATIS-1000074.v.003 at 13.

[84] For example, we note that, as conceived, the OrigID is meant to be used by the authenticating provider to label a portion its network (e.g., a wholesale customer) as determined by each authenticating provider, and each OrigID is unique only within that provider's network; other providers could use the same OrigID. *See* ATIS-1000074.v.003 at 13 ("The purpose of the origination identifier is to assign an opaque identifier corresponding to all or part of the originating service provider's network (data centers, IBCF nodes, access networks, IMS core complexes, etc.), customers, customer or interconnecting service provider nodes, classes of customer devices, or other groupings that a service provider might want to use to indicate common call sources for determining things such as reputation or traceback identification of customers or gateways.").

[85] For example, Germany and France appear to require that the caller ID display information be suppressed for such calls in some cases. *See* Immervox, Calling Germany, New Regulations Released 1 December (Oct. 21, 2021), https://immervox.com/about/news/calling-germany-new-regulations-introduced-1-december/#:~:text=October%2021%2C%202022,will%20be%20displayed%20as%20anonymous. (noting German restriction, that France imposed a similar restriction in 2019, and that such restrictions are "increasingly common.").

calls that originate outside of the United States but legitimately spoof a NANP number, especially a domestic NANP number?

73. 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?

74. 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?

75. 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?

76. 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?

77. *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.[86] For instance, should we designate a specific area code for foreign-originated calls?[87] 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?

78. If we establish a designated area code for foreign-originated calls, we seek comment on

[86] In the NPRM attached to the *2022 Gateway Provider Order*, we sought comment on a variety of possible changes to our numbering rules to prevent the misuse of numbering resources to originate illegal robocalls, particularly those originating abroad. *See 2022 Gateway Provider Order*, 37 FCC Rcd at 6748-49, paras. 219-221. To the extent our inquiries here overlap with those, we seek to refresh the record.

[87] If we determine that mobile or VoIP roaming calls are excluded from our proposals, these services necessarily would not be subject to any requirement to use a specific area code.

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.[88] Under OfCom's guidance, the gateway provider is responsible for compliance with the guidance.[89] 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.[90] 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?

79. *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.

80. 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?

81. 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?[91] Could we require gateway providers to accept only calls

[88] Ofcom, Tackling Scam Calls, Updating our CLI Guidance to expect providers to block more calls with spoofed numbers at 8 (July 29, 2024), statement-tackling-scam-calls.pdf (*OfCom Guidance Statement*).

[89] *Ofcom Guidance Statement* at 17-18.

[90] *OfCom Guidance Statement* at 23-24 ("One way in which providers can demonstrate this for calls which use UK CLI as a Presentation Number is by seeking assurance from the non-UK network that the caller is using a CLI that they have permission to use (either because they have been directly assigned that number or has been given permission by a third party who has been assigned that number). For calls using a UK CLI as a Network Number, providers will need to seek assurance that the caller is using a number that has been allocated to the originating CP or one that has been ported into the originating CP's network.").

[91] ATIS has established a mechanism for cross-border STIR/SHAKEN implementations, other countries have required implementation of STIR/SHAKEN, and additional industry efforts have recently been undertaken. *See*

(continued….)

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.

82. 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?

83. *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.[92]

84. 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?

85. 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?[93] And if we adopt our proposal to require voice service providers to transmit to handsets an

---

ATIS & SIP Forum, Mechanism for Cross-Border Signature-based Handling of Asserted information using toKENs (SHAKEN), ATIS-1000087v.002 (Feb. 7, 2024); Canadian Radio-television and Telecommunications Commission, 2021-123, STIR/SHAKEN implementation for Internet Protocol-based voice calls (Apr. 6, 2021), https://crtc.gc.ca/eng/archive/2021/2021-123.pdf (requiring implementation of STIR/SHAKEN by Canadian providers); ATIS.org, ATIS, iconectiv Trial Industry Robocall Initiative With Bandwidth, Microsoft to Mitigate Unwanted Robocalls Globally (Aug. 15, 2024), https://atis.org/press-releases/atis-iconectiv-trial-industry-robocall-initiative-with-bandwidth-microsoft-to-mitigate-unwanted-robocalls-globally/ (announcing trial of cross-border authentication).

[92] *See*, *e.g.*, FCC, *Consumer Guide: Caller ID Spoofing*, https://www.fcc.gov/consumers/guides/spoofing (last visited Sept. 29, 2025); TransNexus, *Understanding STIR/SHAKEN*, https://transnexus.com/whitepapers/understanding-stir-shaken (last visited Sept. 29, 2025).

[93] "The 'North American Numbering Plan' is the basic numbering scheme for the telecommunications networks located in American Samoa, Anguilla, Antigua, Bahamas, Barbados, Bermuda, British Virgin Islands, Canada, Cayman Islands, Dominica, Dominican Republic, Grenada, Jamaica, Montserrat, Sint Maarten, St. Kitts & Nevis, (continued….)

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?

86. 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

87. 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.[94] We also seek comment on any other bases of authority for our proposals and other actions on which we seek comment.

88. 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."[95] 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"[96] and directs the Commission to prescribe implementing regulations.[97] 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?

89. 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.[98] Although the TRACED Act requires us to conduct formal triennial assessments and submit a report to Congress,[99] 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.[100] The TRACED Act also grants us

St. Lucia, St. Vincent, Turks & Caicos Islands, Trinidad & Tobago, and the United States (including Puerto Rico, the U.S. Virgin Islands, Guam, the Commonwealth of the Northern Mariana Islands)." 47 CFR § 52.5(d).

[94] Truth in Caller ID Act of 2009, Pub. L. No. 111-331, 124 Stat. 3572 (2010) (Truth in Caller ID Act); TRACED Act; 47 U.S.C. § 251(e).

[95] 47 U.S.C. § 227(e)(8).

[96] *Id*. § 227(e)(1).

[97] *Id*. § 227(e)(3).

[98] *Id*. § 227b(b)(1), (4)(B).

[99] *Id.* § 227b(b)(4)(A)-(C).

[100] *Id.* § 227b(b)(4)(C). Our next assessment must be completed by December 30, 2025.

authority over non-IP networks, including to require robocall mitigation programs.[101] 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."[102] 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.

90. 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.[103] 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.[104] 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.[105] 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

91. This *Notice* 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 *Notice* 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 *Notice* further proposes to

[101] *See Id.* § 227b(b)(1)(B), (b)(2)(B), (b)(5)(B),(C), (E)-(F). Section (b)(5)(C) states, "the Commission shall require any provider of voice service subject to such delay [of STIR/SHAKEN implementation] to implement an appropriate robocall mitigation program to prevent unlawful robocalls from originating on the network of the provider." The Commission has extended the robocall mitigation program requirement to all providers, regardless of their STIR/SHAKEN implementation status, relying, *inter alia*, on its authority in section 251(e) and the Truth in Caller ID Act. *Call Authentication Trust Anchor*, WC Docket No. 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd 2573, 2617, para. 92 (2023).

[102] TRACED Act § 4(d).

[103] 47 USC § 251(e).

[104] *Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, 36 FCC Rcd 1859, 1911, para. 99 (2020) (*Second Caller ID Authentication Report and Order*).

[105] For example, in the *Second Caller ID Authentication Report and Order*, the Commission found that section 251(e) provided authority for rules applying to intermediate providers, as well as originating and terminating providers, while the TRACED Act provided authority to adopt rules implementing section 4(b)(1)(B) for originating and terminating providers. *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1875, paras. 33-35.

require intermediate providers across the entire call path to transmit information that a call originated from outside of the United States. This *Notice* 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 *Notice* 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.

92. 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?

93. This *Notice* 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 *Notice* 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.

IV. ELIMINATING OUTDATED RULES

94. 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

95. *Call Abandonment Rules*. We propose 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.[106] We seek comment on this proposal. The Commission adopted these rules in response to the Do-Not-Call Implementation Act (DNC Act),

[106] 47 CFR §§ 64.1200(a)(6), (7).

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).[107] The FTC's current TSR contains comparable provisions to these two Commission rules.[108]

96. We believe that the calling practices these rules target might no longer be a significant source of consumer frustration. That might be because calling practices involving the use of predictive dialers have evolved to become more efficient, rendering our rules no longer necessary to protect consumers. We also believe that eliminating these rules would relieve callers of the burden of tracking their calls to comply with the rule, and to be prepared in the event the Commission were to ask about them. We seek comment on these beliefs. Does the DNC Act require us to retain these rules? Does the Commission's differing jurisdiction from the FTC favor retaining or deleting these rules?[109] 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?

97. *Company-Specific DNC Rules*. We also propose to delete the rules requiring callers to record a subscriber's do-not-call request and place the subscriber's name, if provided, and telephone number on the company's DNC list to avoid calling that number.[110] We seek comment on this proposal. In adopting rules to implement the National Do-Not-Call (DNC) Registry in conjunction with the FTC in 2003, the Commission described the National DNC Registry and company-specific DNC rules as supplementing or complementing each other.[111]

98. These DNC requirements effectively work in different ways. The company-specific DNC rules permit consumers to stop telemarketing calls from individual callers on a case-by-case basis. The National DNC registry prohibits telemarketing calls from all callers except those that the consumer acts to permit on a case-by-case basis.[112] With this understanding, the Commission retained its company-specific rules in 2003 with modifications to lessen the burdens on callers. In doing so, the Commission noted both comments describing limits on the effectiveness of the company-specific DNC rules and the FTC's decision to retain company-specific DNC requirements following implementation of the National DNC Registry.[113]

99. In light of the two decades of experience with the National DNC Registry and company-specific DNC requirements supplementing each other, we believe that our more general anti-robocall rules might provide consumers sufficient protection. These other anti-robocall rules include those that require companies to honor consent revocation and implement the National DNC Registry.[114] In addition, the protections afforded by the National DNC Registry extend beyond telemarketing calls made using an

[107] *Rules and Regulations Implementing the Do-Not-Call Implementation Act*, Report and Order, 18 FCC Rcd 14014 (2003) (*DNC Act Order*); Do-Not-Call Implementation Act, Pub. L. No. 108-10, 117 Stat. 557 (2003), codified at 15 U.S.C. § 6101 *et seq*. We use "DNC" generically to mean "do-not-call".

[108] The relevant portion of the TSR can be found at 16 CFR § 310.4(b).

[109] The FTC has no jurisdiction over intrastate telemarketing calls and limited jurisdiction over common carriers. See *DNC Act Order*, 18 FCC Rcd at 14023, para. 9. *See also FTC v. AT&T Mobility LLC*, 883 F.3d 848 (9th Cir. 2018) (holding that common carrier classification for purposes of the FTC Act depends on activity, not status).

[110] 47 CFR § 64.1200(b)(3), (d).

[111] *DNC Act Order*, 18 FCC Rcd at 14014, 14067, paras. 1, 90.

[112] *Id.* at 14033-34, para. 26.

[113] *Id.* at 14065-70, paras. 86-96.

[114] 47 CFR §§ 64.1200(a)(10), 64.1200(c)(2). The National DNC Registry included over 253 million active registrations during fiscal year 2024. *See* FTC, *National Do Not Call Registry Data Book for Fiscal Year 2024* (Nov. 2024), https://www.ftc.gov/reports/national-do-not-call-registry-data-book-fiscal-year-2024.

autodialer and artificial or prerecorded voice message to include live solicitation calls.[115] We note that the TCPA directs the Commission to "compare and evaluate alternative methods and procedures (including . . . company-specific 'do-not-call' systems)" but does not require the Commission to implement such methods.[116] Further, the company-specific DNC rules impose unique burdens on callers, such as specific personnel training requirements.

100. We seek comment on these views. Is the National DNC Registry sufficient to ensure legitimate telemarketers are not contacting enrolled consumers without the need for company-specific DNC requirements? Are there reasons why consumers want or need the option to use the company-specific DNC requirements to opt out of calls from certain telemarketers as opposed to using the National DNC Registry and opting into calls from certain telemarketers? For example, should we retain section 64.1200(b)(3)'s requirement for artificial or prerecorded voice messages made pursuant to an exemption, or that include an advertisement or constitute telemarketing, to provide an automated opt-out mechanism for the called person to make a do-not-call request or otherwise revoke consent?[117] Are there circumstances in which such automated opt-out mechanisms are beneficial to consumers in ways that are not addressed by the National DNC Registry or other rules? Do the rules help consumers in ways our other anti-robocall rules do not? If they remain necessary, should we consider streamlining them? What is the burden on callers to comply with the rules?

101. How should the FTC's analogous rules factor into our decision? The DNC Implementation Act requires us to maximize consistency with the FTC rules. We do not read that to mean that we should refrain from modernizing our rules, i.e., we do not believe Congress intended us to freeze the rules to ensure consistency with the FTC. In addition to consulting with the FTC, we seek public comment on this view and on potential complications that could stem from having different FCC and FTC rules. For example, could the different requirements confuse or otherwise create challenges for callers and/or consumers?

102. *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.[118] For telemarketing and certain other calls to consumers' residential numbers, the number provided must be able to accept DNC requests during regular business hours.[119] 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.[120] 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? How might this affect any action we might take with respect to the potential elimination of the company-specific DNC rules, as discussed above?

2. More Recent Rules That Might Harm Consumers

103. *Consent Revocation Rules*. We propose to delete 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,

[115] *DNC Act Order*, 18 FCC Rcd at 14116, para. 166.

[116] 47 U.S.C. § 227(c)(1)(A).

[117] *See* 47 CFR § 64.1200(b)(3).

[118] 47 CFR § 64.1200(b)(2).

[119] *Id*.

[120] *See* 47 U.S.C. § 227(d)(3)(A) (requiring only the provision of a telephone number or address of the caller).

which harms consumers, or to modify it to give consumers greater control over their right to stop unwanted calls.[121] 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."[122]

104. We believe the rule unduly restricts consumers' ability to receive wanted calls, and seek comment on that view. 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? [123] 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?[124] How does this affect consumers who both are customers of a business and are employees, job applicants, or contractors of that same business? [125] 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?

105. We also propose to amend section 64.1200(a)(10). For example, commenters in the Delete Proceeding[126] 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."[127] 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

[121] 47 CFR § 64.1200(a)(10) requires a caller to treat a consumer's revocation of consent as revoking consent for all calls from the caller, irrespective of subject. It also requires a caller to honor all revocation requests made using any "reasonable means".

[122] *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, CG Docket No. 02-278, Order, DA 25-312, 2025 WL 1077219 at *1 (CGB 2025); *see also* Letter from Jonathan Thessin, Vice President and Senior Counsel, American Bankers Association, and Patrick Crotty, Senior Attorney, National Consumer Law Center, to Brendan Carr, Chairman, FCC, CG Docket No. 02-278 (filed Sept. 18, 2025).

[123] *See*, *e.g.*, Retail Industry Leaders Association Comments, GN Docket No. 25-133, at 3 (prescription refill reminders, medication availability notices, and timely and critical updates on any potential drug interactions or recalls) (rec. Apr. 11, 2025) (RILA 25-133 Comments); National Association of Chain Drugstores, GN Docket No. 25-133, at 1-2 (rec. Apr. 11, 2025) (revoking consent to appointment reminders also revokes consent to marketing messages and informational messages about prescriptions or other health alerts) (NACDS 25-133 Comments).

[124] *See, e.g.*, American Bankers Association et al. Comments, CG Docket No. 02-278, GN Docket No. 25-133, at 7-9 (filed Apr. 12, 2025); Letter from Michael Pryor, Counsel, ACA International, to Marlene H. Dortch, Secretary, FCC Comments, (Jun. 6, 2025) (echoing banks' concerns about TCPA rules).

[125] *See*, *e.g.*, RILA 25-133 Comments at 5-6 (revoking consent as a customer of a business also revokes consent as to communications as an employee (e.g., notices about company policies, training sessions, and important deadlines for benefit enrollment, performance reviews, and other HR-related matters) or job applicant (e.g., job openings, interview schedules, application status).

[126] *In Re: Delete, Delete, Delete*, GN Docket No. 25-133, Public Notice, DA 25-219, 2025 WL 820901 (Mar. 12, 2025).

[127] *See*, *e.g.*, SunCoast Credit Union Comments, GN Docket No. 25-133, at 2; U.S. Chamber of Commerce Comments, GN Docket No. 25-133, at 11; NTCA-The Internet and Television Association Comments, GN Docket No. 25-133, at Appendix, p. 13; NACDS 25-133 Comments at 1-2; National Automobile Dealers Association Comments, GN Docket No. 25-133, at 2-3; Reasonable Enterprises Against Consumer Harassment Comments, GN Docket No. 25-133, at 10-11; National Taxpayers Union Foundation Reply Comments, GN Docket No. 25-133, at 7-8; American Bankers Association, et al. Comments, GN Docket No. 25-133, at 10-12; Information Technology Industry Council Reply Comments, GN Docket No. 25-133, at 7-8.

potential ambiguity of the current reasonable-means standard.

106. 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?

107. *Fraud Alert Call Rules*. We propose and seek comment on eliminating 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.[128] We 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.[129] We seek comment on this view.

108. 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?

B. Call Blocking Rules

109. *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.[130] 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.[131] We seek comment on this proposal.

V. PUBLIC NOTICE REGARDING OLDER PETITIONS AND APPLICATIONS RELATED TO THE TELEPHONE CONSUMER PROTECTION ACT

110. As part of our effort to efficiently manage dockets and resources and reduce backlog, we

[128] 47 CFR § 64.1200(a)(9)(iii)(A). This includes calls or messages relating to transactions and events that suggest a risk of fraud or identity theft; possible breaches of the security of customers' personal information; steps consumers can take to prevent or remedy harm caused by data security breaches; and actions needed to arrange for receipt of pending money transfers. *Id*. at § 64.1200(a)(9)(iii)(C).

[129] *See*, *e.g.*, American Bankers Association, et al. Comments, GN Docket No. 25-133, at 15-17.

[130] 47 CFR §§ 64.1200(k)(1), (2)(i)-(iii).

[131] *See Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Sixth Report and Order in CG Docket No. 17-59, Fifth Report and Order in WC Docket No. 17-97, Order on Reconsideration in WC Docket No. 17-97, Seventh Further Notice of Proposed Rulemaking in CG Docket No. 17-59, and Fifth Further Notice of Proposed Rulemaking in WC Docket No. 17-97, 37 FCC Rcd 6865 (2022) (*Gateway Provider Order*); *2025 Call Blocking Order*, 2025 WL 820883, at *3-5. The rules become effective on December 15, 2025. *Effective Date for Rule Requiring All Providers to Block Using a Do-Not-Originate List Set for December 15, 2025*, 90 Fed. Reg. 44580 (Sept. 16, 2025).

seek to assess whether the Petitioners and Applicants who filed the petitions and applications listed below continue to be interested in pursuing them. Parties filed these petitions between 2012 and 2021 and they have gone without advocacy for several years. In addition, the specific matters to which they relate likely have been mooted or outdated by advancements in technology, changes in consumer preferences, or changes in regulations that have occurred since.

111. Consistent with our past practice,[132] we therefore plan to dismiss the Petitions and Applications below with prejudice unless a Petitioner or Applicant files a letter in the relevant docket or dockets within 45 days of the date of Federal Register publication of this *Notice* specifying that it objects to the dismissal of its Petition or Application and the reasons for such objection. Upon release of this *Notice*, the Office of the Secretary will send copies hereof to the Petitioners and Applicants at the last available mailing address associated with the Petitions and Applications.

112. The Petitions and Applications,[133] along with related information, are:

Petitioner/Applicant	**Petition/Application**	**Date Filed**	**Docket(s)**
MarketLink, Inc.	Petition for Reconsideration	July 11, 2012	CG Docket No. 02-278
Professional Association for Customer Engagement (PACE)	Petition for Reconsideration	July 11, 2012	CG Docket No. 02-278
SatCom Marketing, LLC	Petition for Reconsideration	July 11, 2012	CG Docket No. 02-278
American Bankers Association	Petition for Reconsideration	August 7, 2015	CG Docket No. 02-278
American Bankers Association	Petition for Reconsideration	August 10, 2015	CG Docket No. 02-278
Mortgage Bankers Association	Application for Review	December 16, 2016	CG Docket No. 02-278
Professional Association for Customer Engagement (PACE)	Petition for Reconsideration	April 25, 2019	CG Docket No. 17-59
Competitive Carriers Association, et al.	Petition for Reconsideration	April 25, 2019	CG Docket No. 17-59
Career Counseling Services, Inc.	Application for Review	January 8, 2020	CG Docket Nos. 02-278, 05-338
National Consumer Law Center, et al.	Application for Review	July 24, 2020	CG Docket No. 02-278

[132] *See, e.g., Consumer and Governmental Affairs Bureau Seeks to Determine Parties' Continuing Interest in Specific Petitions for Preemption of State Consumer Protection Requirements*, Public Notice, 35 FCC Rcd 10441 (CGB 2020); *Consumer and Governmental Affairs Bureau Dismisses Nine Petitions for Preemption of State Consumer Protection Requirements*, Public Notice, 35 FCC Rcd 14621 (CGB 2020). *See also Amendment of Certain of the Commission's Part 1 Rules of Practice and Procedure and Part 0 Rules of Commission Organization*, Report and Order, 26 FCC Rcd 1594 (2011) (adopting procedures to terminate dormant proceedings, but interested parties should have an opportunity to comment before any particular proceeding is terminated).

[133] The petitions filed by American Bankers Association appear to be duplicates. Both reference CG Docket No. 02-278 and WC Docket No. 07-135, but were filed only in CG Docket No. 02-278.

Anderson + Wanca	Application for Review	October 5, 2020	CG Docket Nos. 02-278, 05-338
Cin-Q Automobiles, Inc.	Application for Review	October 21, 2020	CG Docket Nos. 02-278, 05-338
Broadnet Teleservices, LLC	Petition for Reconsideration	January 14, 2021	CG Docket No. 02-278

VI. PROCEDURAL MATTERS

A. Initial Regulatory Flexibility Act Analysis

113. The Regulatory Flexibility Act of 1980, as amended (RFA),[134] requires that an agency prepare a regulatory flexibility analysis for notice-and-comment rulemaking proceedings, unless the agency certifies that "the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities."[135] Accordingly, the Commission has prepared an Initial Regulatory Flexibility Analysis (IRFA) concerning potential rule and policy changes contained in this *Notice*. The IRFA is set forth in Appendix B. The Commission invites the general public, in particular small businesses, to comment on the IRFA. Comments must be filed by the deadlines for comments on this *Notice* indicated on the first page of this document and must have a separate and distinct heading designating them as responses to the IRFA.

B. Initial Paperwork Reduction Act Analysis

114. This *Notice* may contain proposed new or modified information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens and pursuant to the Paperwork Reduction Act of 1995, Public Law 104-13, invites the general public and the Office of Management and Budget (OMB) to comment on these information collection requirements. 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.

C. Filing Requirements—Comments and Replies

115. Pursuant to sections 1.415 and 1.419 of the Commission's rules, 47 CFR §§ 1.415, 1.419, interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS).[136]

- Electronic Filers: Comments may be filed electronically using the Internet by accessing the ECFS: https://www.fcc.gov/ecfs.
- Paper Filers: Parties who choose to file by paper must file an original and one copy of each filing.

[134] 5 U.S.C. §§ 601 *et seq.*, as amended by the Small Business Regulatory Enforcement and Fairness Act (SBREFA), Pub. L. No. 104-121, 110 Stat. 847 (1996).

[135] *Id.* § 605(b).

[136] *See Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998).

- 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 e-mail to fcc504@fcc.gov or call the Consumer and Governmental Affairs Bureau at (202) 418-0530.

D. Ex Parte Rules

116. The proceeding this *Notice* initiates shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules.[137] Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda, or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with rule 1.1206(b). 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 in the docket established for this 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

E. Providing Accountability Through Transparency Act

117. 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.[138]

F. Additional Information

118. For further information about this *Notice*, contact John B. Adams, Special Counsel, Consumer Policy Division, Consumer and Governmental Affairs Bureau, at johnb.adams@fcc.gov.

[137] 47 CFR § 1.1206.

[138] 5 U.S.C. § 553(b)(4). The Providing Accountability Through Transparency Act of 2023, Pub. L. No. 118-9 (2023), amended the Administrative Procedure Act to add a requirement to publish a short summary, in plain language, of each notice of proposed rulemaking.

VII. ORDERING CLAUSES

119. Accordingly, **IT IS ORDERED**, pursuant to sections 1-4, 201(b), 202(a), 227, 227b, and 251(e) of the Communications Act of 1934, as amended, 47 U.S.C §§ 151-154, 227, 227b, 251(e), and sections 1.106, 1.115, 1.411 – 1.413, and 1.421 of the Commission's rules, 47 CFR §§ 1.106, 1.115, 1.411-1.413, 1.421, that this Ninth Further Notice of Proposed Rulemaking in CG Docket No. 17-59; Seventh Further Notice of Proposed Rulemaking in WC Docket No. 17-97; Further Notice of Proposed Rulemaking in CG Docket No. 02-278; and Public Notice in CG Docket No. 25-307 **IS ADOPTED**.

120. **IT IS FURTHER ORDERED**, pursuant to sections 1.415 and 1.419 of the Commission's Rules, 47 CFR §§ 1.415, 1.419, that interested parties may file comments on the rulemaking portion of this Ninth Further Notice of Proposed Rulemaking in CG Docket No. 17-59; Seventh Further Notice of Proposed Rulemaking in WC Docket No. 17-97; Further Notice of Proposed Rulemaking in CG Docket No. 02-278; and Public Notice in CG Docket No. 25-307 on or before 30 days after publication in the Federal Register, and reply comments on or before 45 days after publication in the Federal Register. Comments and reply comments on the rulemaking portion **SHALL BE FILED** in CG Docket No. 17-59, WC Docket No. 17-97, and CG Docket No. 02-278.

121. **IT IS FURTHER ORDERED** that the Commission's Office of Managing Director, Reference Information Center **SHALL SEND** a copy of this Ninth Further Notice of Proposed Rulemaking in CG Docket No. 17-59; Seventh Further Notice of Proposed Rulemaking in WC Docket No. 17-97; Further Notice of Proposed Rulemaking in CG Docket No. 02-278; and Public Notice in CG Docket No. 25-307, including the Initial Regulatory Flexibility Certification, to the Chief Counsel for Advocacy of the Small Business Administration.

122. **IT IS FURTHER ORDERED** that the Commission's Office of the Secretary **SHALL SEND** a copy of this Ninth Further Notice of Proposed Rulemaking in CG Docket No. 17-59; Seventh Further Notice of Proposed Rulemaking in WC Docket No. 17-97; Further Notice of Proposed Rulemaking in CG Docket No. 02-278; and Public Notice in CG Docket No. 25-307 to the Petitioners and Applicants whose Petitions for Reconsideration and Applications for Review are listed in the table in paragraph 112 at the mailing address in each Petition or Application.

123. **IT IS FURTHER ORDERED**, pursuant to sections 1.106, 1.115 and 1.419 of the Commission's rules, 47 CFR §§ 1.106, 1.115, 1.419, that each petitioner or applicant that filed the petitions and applications listed in the table in paragraph 112 and that objects to its Petition for Reconsideration or Application for Review being dismissed with prejudice, within 45 days of the date of Federal Register publication of this Ninth Further Notice of Proposed Rulemaking in CG Docket No. 17-59; Seventh Further Notice of Proposed Rulemaking in WC Docket No. 17-97; Further Notice of Proposed Rulemaking in CG Docket No. 02-278; and Public Notice in CG Docket No. 25-307 **SHALL FILE** in CG Docket No. 25-307 a letter specifying that it objects to the dismissal of its Petition or Application and the reasons for such objection.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

APPENDIX A

Proposed Rules

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

PART 64 – Miscellaneous Rules Relating to Common Carriers

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

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

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

2. Amend § 64.1200 by removing and reserving subparagraphs (a)(6), (a)(7), (a)(9)(iii)(A), (a)(10), revise first sentence of subparagraph (b)(2), removing and reserving subparagraphs (b)(3), (d), (k)(1), (k)(2)(i), (k)(2)(ii) and (k)(2)(iii), revising subparagraph (k)(3)(ii).

§ 64.1200 Delivery restrictions.

(a) *****

(6) Remove and reserve

(7) Remove and reserve

(8) ***

(9) ***

(iii)***

(A) Remove and reserve.

*****

(10) Remove and reserve

* * * * *

(b) * * *

(1) ***

(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 * * *

(3) Remove and reserve

* * * * *

(d) Remove and reserve

* * * * *

(k) * * *

(1) Remove and reserve

(2)* * *

(i) Remove and reserve

(ii) Remove and reserve

(iii) Remove and reserve

(3) ***

(i) ***

(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. In § 64.1600, add 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.

APPENDIX B

Initial Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[1] the Federal Communications Commission (Commission) has prepared this Initial Regulatory Flexibility Analysis (IRFA) of the policies and rules proposed in the *Further Notice of Proposed Rulemaking* (*Notice)* 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 *Notice.* The Commission will send a copy of the *Notice* including this IRFA, to the Chief Counsel for the SBA Office of Advocacy.[2] In addition, the *Notice* and IRFA (or summaries thereof) will be published in the Federal Register.[3]

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

2. 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.

3. To address these issues, this *Notice* 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.

4. 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

5. 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

[1] 5 U.S.C. §§ 601 *et seq*., as amended by the Small Business Regulatory Enforcement and Fairness Act (SBREFA), Pub. L. No. 104-121, 110 Stat. 847 (1996).

[2] *Id.* § 603(a).

[3] *Id*.

Rules Will Apply

6. 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.[4] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[5] In addition, the term "small business" has the same meaning as the term "small business concern" under the Small Business Act (SBA).[6] 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.[7] 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.[8]

7. 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.[9] In general, a small business is an independent business having fewer than 500 employees.[10] These types of small businesses represent 99.9% of all businesses in the United States, which translates to 34.75 million businesses.[11] Next, "small organizations" are not-for-profit enterprises that are independently owned and operated and not dominant their field.[12] 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.[13] Finally, "small governmental jurisdictions" are defined as cities, counties, towns, townships, villages, school districts, or special districts with populations of less than fifty thousand.[14] 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.[15]

8. The rules proposed in the *Notice* will apply to small entities in the industries identified in

[4] 5 U.S.C. § 603(b)(3).

[5] *Id*. § 601(6).

[6] *Id*. § 601(3) (incorporating by reference the definition of "small-business concern" in the Small Business Act, 15 U.S.C. § 632). Pursuant to 5 U.S.C. § 601(3), the statutory definition of a small business applies "unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the Federal Register."

[7] 15 U.S.C. § 632.

[8] 13 CFR 121.903.

[9] 5 U.S.C. § 601(3)-(6).

[10] *See* SBA, Office of Advocacy, *Frequently Asked Questions About Small Business* (July 23, 2024), https://advocacy.sba.gov/wp-content/uploads/2024/12/Frequently-Asked-Questions-About-Small-Business_2024-508.pdf.

[11] *Id*.

[12] 5 U.S.C. § 601(4).

[13] *See* SBA, Office of Advocacy, *Small Business Facts, Spotlight on Nonprofits* (July 2019), https://advocacy.sba.gov/2019/07/25/small-business-facts-spotlight-on-nonprofits/.

[14] 5 U.S.C. § 601(5).

[15] *See* U.S. Census Bureau, 2022 Census of Governments –Organization, https://www.census.gov/data/tables/2022/econ/gus/2022-governments.html, tables 1-11.

the chart below by their six-digit North American Industry Classification System (NAICS)[16] codes and corresponding SBA size standard.[17] 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[18]	Small Firms[19]	% Small Firms in Industry
Telephone Apparatus Manufacturing[20]	334210	1,250 employees	189	177	93.65
Wired Telecommunications Carriers[21]	517111	1,500 employees	3,054	2,964	97.05
Wireless Telecommunications Carriers (except Satellite)[22]	517112	1,500 employees	2,893	2,837	98.06
Telecommunications Resellers[23]	517121	1,500 employees	1,386	1,375	99.21
Satellite Telecommunications[24]	517410	$47 million	275	242	88.00

[16] The North American Industry Classification System (NAICS) is the standard used by Federal statistical agencies in classifying business establishments for the purpose of collecting, analyzing, and publishing statistical data related to the U.S. business economy. *See* www.census.gov/NAICS for further details regarding the NAICS codes identified in this chart.

[17] The size standards in this chart are set forth in 13 CFR 121.201, by six digit North American Industrial Classification System (NAICS) code.

[18] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, *and 2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM.

[19] *Id.*

[20] Affected Entities in this industry include Multi-Line Telephone System Manufacturers Importers Sellers or Lessors.

[21] Affected Entities in this industry include Competitive Local Exchange Carriers (CLECs), Incumbent Local Exchange Carriers (Incumbent LECs), Interexchange Carriers (IXCs), and Local Exchange Carriers (LECs, Other Toll Carriers).

[22] Affected Entities in this industry include Wireless Carriers and Service Providers and Wireless Communications Services.

[23] Affected Entities in this industry include 800 and 800-Like Service Subscribers, IMTS Resale Carriers, Local Resellers, Payphone Service Providers, Prepaid Calling Card Providers, Toll Resellers, and Wireless Resellers.

[24] Affected Entities in this industry include Fixed Satellite Small Transmit/Receive Earth Stations, Fixed Satellite Very Small Aperture Terminal (VSAT) Systems, and Mobile Satellite Earth Stations.

All Other Telecommunications[25]	517810	$40 million	1,079	1,039	96.29

Table 2. Telecommunications Service Provider Data

2024 Universal Service Monitoring Report Telecommunications Service Provider Data [26] **(Data as of December 2023)**	**SBA Size Standard (1500 Employees)**		
Affected Entity	**Total # FCC Form 499A Filers**	**Small Firms**	**% Small Entities**
Competitive Local Exchange Carriers (CLECs)[27]	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)[28]	4,904	4,493	91.62
Toll Resellers	411	398	96.84
Wired Telecommunications Carriers[29]	4,682	4,276	91.33
Wireless Telecommunications Carriers (except Satellite)[30]	585	498	85.13
Wireless Telephony[31]	326	247	75.77

D. Description of Economic Impact and Projected Reporting, Recordkeeping, and

[25] Affected Entities in this industry include Internet Service Providers (Non-Broadband), Non Licensee Owners of Towers and Other Infrastructure, and Telecommunications Relay Service (TRS) Providers.

[26] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2024), https://docs.fcc.gov/public/attachments/DOC-408848A1.pdf.

[27] Affected Entities in this industry include all reporting local competitive service providers.

[28] Affected Entities in this industry include all reporting fixed local service providers (CLECs & ILECs).

[29] Local Resellers fall into another U.S. Census Bureau industry (Telecommunications Resellers) and therefore data for these providers is not included in this industry.

[30] Affected Entities in this industry include all reporting wireless carriers and service providers.

[31] Affected Entities in this industry include Cellular/PCS/SMR - Specialized Mobile Radio Licensees and SMR (Dispatch).

Other Compliance Requirements for Small Entities

9. 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.[32]

10. The *Notice* 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.

11. The *Notice* 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.

12. The *Notice* 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.

13. 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.

14. 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 *Notice* are ultimately adopted.

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

15. 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.[33] 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."[34]

[32] 5 U.S.C. § 603(b)(4).

[33] 5 U.S.C. § 603(c).

[34] *Id.* § 603(c)(1)-(4).

16. In the *Notice*, 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.

17. 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.

18. 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.

19. Additionally, the Commission proposes to eliminate several outdated robocall requirements that may represent unnecessary burdens on small entities, including call abandonment rules and certain company-specific do-not-call requirements that technology and calling practices have overtaken.

20. The Commission expects to more fully consider the economic impact and alternatives for small entities following review of comments filed in response to the *Notice* 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

21. None.