FEDERAL COMMUNICATIONS COMMISSION

47 CFR Parts 0, 1, and 64

[WC Docket Nos. 24–213 and 17–97; CG Docket No. 17–59; FCC 26–49; FR ID 364473]

Improving the Effectiveness of the Robocall Mitigation Database; Call Authentication Trust Anchor; Advanced Methods To Target and Eliminate Unlawful Robocalls

AGENCY: Federal Communications Commission.

ACTION: Proposed rule.

SUMMARY: In this document, the Federal Communications Commission (Commission) proposes steps to strengthen the reliability, integrity, and effectiveness of the Robocall Mitigation Database (RMD or Database) as a core component of its illegal-call prevention framework. The Commission proposed measures aim to ensure that RMD filings are accurate, complete, and current, and to safeguard the Database so that only legitimate, transparent, and accountable providers may enter or remain listed. Specifically, the Commission proposes and seeks comment on measures to clarify which entities are required to file in the RMD, enhance the accuracy and completeness of submitted information, and specify which portions of filings may be publicly disclosed. Additionally, the Commission proposes and seeks comment on new tools to prevent bad actors and noncompliant providers from accessing or remaining in the RMD, including strengthened screening procedures for new filers, improved mechanisms for identifying noncompliant providers, expedited removal processes, and safeguards to prevent unauthorized re-entry into the Database.

DATES: Comments are due on or before October 9, 2026 and reply comments are due on or before November 9, 2026.

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

- *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.
- Filings can be sent by hand or messenger deliver, 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.
- *Accessible formats:* To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an email to *fcc504@fcc.gov* or call the Consumer & Governmental Affairs Bureau at 202–418–0530.

FOR FURTHER INFORMATION CONTACT: Chris Laughlin, Deputy Division Chief, Competition Policy Division, Wireline Competition Bureau, at (202) 418–2193 or *Chris.Laughlin@fcc.gov.* For additional information concerning the Paperwork Reduction Act proposed information collection requirements contained in this document, email *PRA@fcc.gov* or contact Nicole Ongele at (202) 418–2991.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Further Notice of Proposed Rulemaking (*FNPRM*) in WC Docket Nos. 24–213 and 17–97; CG Docket No. 17–59, document FCC 26–49, adopted on July 22, 2026 and released on July 23, 2026. The full text of this document is available online at: *https://docs.fcc.gov/public/attachments/FCC-26-49A1.pdf.*

Paperwork Reduction Act Analysis: This *FNPRM* may contain proposed new or modified information collections. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and the Office of Management and Budget (OMB) to comment on any information collections contained in this document, as required by the Paperwork Reduction Act of 1995, Public Law 104–13, see 44 U.S.C. 3501 through 3521. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107–198, see 44 U.S.C. 3506(c)(4), we seek specific comment on how we might further reduce the information collection burden for small business concerns with fewer than 25 employees.

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

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

Synopsis

I. Discussion

To improve the effectiveness of the Robocall Mitigation Database (RMD or

Database) in promoting transparency and accountability for voice service providers' practices to mitigate illegal calls, we propose rules designed to strengthen providers' filing obligations and deter bad actors and non-compliant providers from entering or remaining in the Database. We use the term ''voice service provider'' and ''provider,'' interchangeably and consistent with our proposed definition in the *Know Your Upstream Provider (KYUP) FNPRM,* 91 FR 42602 (July 9, 2026), to refer to all initiating, originating, intermediate, and terminating providers, including facilities-based providers and non-facilities-based providers (inclusive of interconnected Voice over internet Protocol (VoIP) resellers and Mobile Virtual Network Operators (MVNOs)). We intend for these rules to apply to all new and existing filings submitted in the RMD. We use the term ''filing'' to refer to the full RMD submission, even though the current rules often use ''certification'' for this purpose, as we propose to amend the rules herein to use the term ''filing.'' As the starting place for our proposed rule changes, we use the streamlined rules we proposed in the *KYUP FNPRM.* As a technical matter, the rules proposed in Appendix A, *infra,* are drafted with reference to the rules that are currently in effect and not those proposed in the *KYUP FNPRM.* However, since some of our proposed rules here rely on the proposed changes in that *FNPRM,* we incorporate those proposals by reference and have drafted our proposed rules in Appendix A accordingly. In advancing these proposals, we aim to ensure consistency across all our existing and proposed rules, which operate together to target illegal calls and promote accountability throughout the call path, including our caller ID authentication rules, traceback requirements, Know Your Customer (KYC) and KYUP obligations, and call blocking rules. We invite commenters to evaluate our proposals in the context of this comprehensive framework.

A. Strengthen Filing Obligations

We propose and seek comment on measures to strengthen providers' obligations with respect to filing in the RMD, including proposed rules regarding which entities must file, what information they must submit, and how that information is submitted and viewable by the public.

1. Which Entities Must File

In this section, we propose and seek comment on measures to codify and clarify providers' robocall mitigation filing obligations, including confirming the scope of entities that are voice service providers, the indirect applicability of these rules to foreign voice service providers, filing obligations of related entities, and the use of third parties to file in the RMD.

Confirming which entities are voice service providers. We seek comment on whether we should further explain what constitutes the provision of ''voice service'' and what it means to be a ''voice service provider'' to ensure that all entities that provide voice service are aware of their obligations to comply with RMD requirements and other obligations to combat illegal calls. Despite our recent proposals in the *KYUP FNPRM* to clarify the meaning of those terms through definitions in § 64.6300 of the Commission's rules—which govern the Commission's RMD requirements in § 64.6305 and the Commission's caller ID authentication rules—we remain concerned that some entities that are voice service providers, and therefore must comply with the Commission's rules to combat illegal calls, would still not view themselves as such. In revisiting this issue, we emphasize that we do not intend to alter the scope of entities that are voice service providers, but rather to clarify which entities are voice service providers today. We also proposed, in the *KYUP FNPRM* to harmonize our interpretation of ''voice service,'' as used for our RMD and caller ID authentication rules, with our interpretation of ''voice service,'' as used for our other rules for combatting illegal robocalls, and in revisiting this issue, we do not intend to separate those interpretations again, but rather to clarify the meaning of ''voice service,'' as it applies to all of our rules targeting illegal calls. The Commission has been clear that Congress intended the meaning of ''voice service'' to be broad, and we believe that for purposes of the Commission's rules targeting illegal calls, the meaning applies to entities regardless of the classification of their service, the technological solutions or facilities used to provide their service, the commercial name for the service they provide, or whether they hold any particular Commission authorization, license, or certification, so long as the service meets the definition of ''voice service,'' as we proposed to clarify and codify that definition in the *KYUP FNPRM.*

We believe our view is supported by a statutory interpretation of the definition of ''voice service'' in the TRACED Act, which the Commission has codified in § 64.6300 of our rules. The TRACED Act defines ''voice service'' as:

> [A]ny service that is interconnected with the public switched telephone network and that furnishes voice communications to an end user using resources from the North American Numbering Plan or any successor to the North American Numbering Plan adopted by the Commission under section 251(e)(1) of the Communications Act of 1934 [(the Act)], as amended; and [i]ncludes—transmissions from a telephone facsimile machine, computer, or other device to a telephone facsimile machine; and [w]ithout limitation, any service that enables real-time, two-way voice communications, including any service that requires internet protocol-compatible customer premises equipment and permits out-bound calling, whether or not the service is one-way or two-way voice over internet protocol.

We note, as an initial matter, that we expressed our view in the *KYUP FNPRM* that this definition ''appl[ies] to the furnishing of voice communications to an end user directly or indirectly,'' consistent with our prior interpretation of the nearly identical definition of ''voice service'' in the RAY BAUM'S Act. Thus, an entity need not provide service directly to end users to be a voice service provider.

We also believe that the definitions of key terms in the ''voice service'' definition support a broad reading. ''Service,'' in a commercial context, refers to ''business activity that involves doing things for customers rather than producing goods,'' so the term can apply to any type of commercial entity that is providing a service. ''Interconnected'' refers to ''different parts or things connected or related to each other'' and does not imply that the service uses any particular type of facilities or technological solutions. Likewise, ''furnish'' means ''to supply or provide something needed'' and is not limited to any type of facilities or technological solution. The term ''enables'' is also broad, meaning ''to make someone able to do something, or to make something possible,'' such that any type of facility or technological solution could enable a voice service. None of these definitions, nor the broader definition of ''voice service'' itself refer to any specific type of provider, require a specific service classification, or require any specific FCC authorization, license, or certification. When these definitions are taken together, we believe the broad meaning of ''voice service'' is sufficiently captured by our proposed definition of ''voice service provider'' in the *KYUP FNPRM* as ''any entity that provides voice service for a given call,'' which covers ''all initiating, originating, intermediate, and terminating providers, including facilities-based providers and non-facilities-based providers, which

includes VoIP resellers and MVNOs.'' We seek comment on that view.

Beyond the definitional interpretations, we also believe that the requirement regarding the use of North American Numbering Plan (NANP) resources is broad. It does not specify that the service obtained the NANP resources directly or indirectly, or even that the service controls the NANP resources at all, so long as the service makes use of such resources. Accordingly, we believe that if an entity provides a customer with the ability to make use of NANP resources, regardless of the facilities or technological solution used to do so, then it would qualify as a voice service if it satisfies the other parts of the definition.

In light of this analysis, we believe that in addition to traditional wireline, wireless, and VoIP services, ''voice service,'' for the purposes of our rules targeting illegal calls, includes PBXs, dialing platforms, cloud service providers, over-the-top service providers, call centers, value-added-service providers, and telephone number service providers (TNSP) to the extent the services ''furnish[ ] voice communications to an end user using resources from the North American Numbering Plan,'' including if they ''enable[ ] real-time, two-way voice communications . . . whether or not the service is one-way or two-way [VoIP].'' Additionally, to the extent an entity believes it is providing an information service, that does not mean its service is not also a voice service, as the provision or classification of a service is not determinative as to whether the entity is providing voice service for the purpose of the Commission's rules targeting illegal calls. We seek comment on our analysis and these beliefs. Does any confusion remain as to when an entity is a voice service provider? Do all of the services listed furnish voice communications that is interconnected with the PSTN (either directly or through an interconnected provider) to an end user (directly or indirectly) using NANP numbering resources, or are they capable of doing so, such that they can qualify as voice services for the purposes of our rules targeting illegal calls? Should we list which services qualify as voice services? To the extent any entities that are part of the voice ecosystem still do not believe they are voice service providers, what is the nature of their services, and is there an independent policy and legal basis for subjecting such entities to the RMD rules and/or other rules to combat illegal calls? We also seek comment on whether we should revise the definition of ''end user'' proposed in the *KYUP FNPRM* to further clarify when an entity is furnishing voice communications rather than acting as the end user.

Foreign voice service providers. We seek comment on whether further clarification is necessary with respect to when a foreign voice service provider may choose to file in the RMD and how the filing requirements apply to such providers. Under our current rules, domestic voice service providers must only accept calls that use NANP resources pertaining to the United States in the caller ID field from foreign voice service providers whose filings appear in the RMD and have not been removed. In the *KYUP FNPRM* we proposed to revise the definitions of ''foreign voice service provider'' and ''gateway provider'' to, in part, address our concern that bad actor foreign providers may be establishing nominal offices, operations, or facilities in the United States (such as a hosted server or shared address) to falsely appear as a provider with bona fide independent business operations in the United States, and thereby avoid scrutiny of the provider and their calls. For instance, we believe bad actor foreign providers are trying to avoid scrutiny by the Commission, downstream providers, and other entities in the robocall mitigation ecosystem that may arise when the providers are located in a country that is known for generating a disproportionate number of illegal calls. We also believe bad actor foreign providers are attempting to avoid their calls being viewed as foreign originated, which would invite less scrutiny when the call uses a U.S. NANP number and could allow the call to receive a different STIR/SHAKEN attestation. We believe the proposed revised definitions make clear when a provider is a foreign voice service provider versus any kind of domestic provider for the purposes of the RMD filing requirements, but we seek comment on this view. Should we expand upon these or other proposed definitions to provide additional clarity regarding which entities are foreign voice service providers for purposes of the RMD rules, and if so, how? Although foreign voice service providers' RMD filings are subject to the same requirements, removal processes, and criteria as domestic providers, they are not required to implement STIR/SHAKEN. We therefore seek comment on whether we should revise or clarify how foreign providers indicate their STIR/SHAKEN implementation status in the RMD, particularly given efforts to develop Cross Border Call Authentication (CBCA). If so, how? Below, we seek comment on whether we should establish additional RMD filing requirements to ensure that providers accurately identify when they are a foreign voice service provider.

Filing obligations of related entities. We propose to codify the existing requirement that parents, affiliates, and subsidiaries that independently meet the definition of a ''voice service provider'' must each file a separate filing in the RMD. We believe that codifying this requirement is necessary to increase accountability and prevent filers from obfuscating their relationships with other entities in the RMD, including bad actors and providers that have been removed from the RMD pursuant to a Commission enforcement action. We seek comment on this proposal and assessment. We also seek comment on potential additional or alternative requirements to differentiate entities for purposes of determining their independent RMD filing obligations. For instance, are there specific identifiers that are a necessary or sufficient indicator of an independent filing obligation, such as Operating Company Numbers (OCN), FCC Registration Numbers (FRN), Form 499–A Filer IDs, or Service Provider Code (SPC) token authorizations? An FRN ''is a 10-digit unique identifying number that is assigned to entities doing business with the Commission'' that is obtained through the Commission Registration System (CORES). CORES is the system the FCC uses to facilitate the assignment of FRNs to all persons and entities seeking to do business with the Commission. To register for an FRN through CORES, a filer must provide ''an entity's name, entity type, contact name and title, address, valid email address, and taxpayer identifying number (TIN).'' Currently, each RMD filing may only be associated with a single business-type FRN, and providers must identify any other FRNs on the RMD submission form. The RMD submission form is automatically populated with a filer's FRN and other identifying information obtained from CORES. The Commission requires telecommunications carriers and certain other providers of telecommunications (including VoIP service providers) to submit a Form 499 and report annual service revenues on the FCC Form 499–A. Additionally, we seek comment on how this proposal aligns or departs from providers' practices today, including with respect to obtaining SPC tokens. We note that 6,689 RMD filings indicate full or partial implementation of STIR/SHAKEN, but that only 2,143 providers appear on the Governance Authority's list of authorized providers.

We use the term ''Governance Authority'' to include the Policy Administrator and Certification Authorities, unless otherwise specified, even though each entity may perform specific functions. Are providers filing independently in the RMD but sharing SPC tokens? If so, is that practice permissible under the Governance Authority policies and does it cause confusion for downstream providers accepting calls from these providers or otherwise hinder efforts to combat illegal calls?

Third-party RMD submissions. We seek comment on measures to ensure transparency and accountability when providers rely on a third party to submit RMD filings on their behalf. Under our current rules, RMD filings must be signed by an officer in conformity with § 1.16 of the Commission's rules with a declaration, under penalty of perjury, that the information included in the filing is true and correct. At the same time, we are aware that some providers may rely on third parties, who may not be officers of the provider, to complete their RMD filing obligations. We seek comment on the prevalence of this practice and on the nature of these third-party arrangements. Is it more common among small providers or certain other types of providers? Are third parties who are not officers of the provider making the required declaration or are they completing the information in the filing but leaving the declaration to an officer? What is the relationship between the third parties and the providers—are the third parties acting as consultants, agents, counsel, or in some other capacity? What are the third parties' qualifications and the extent of their knowledge of providers' practices? Should we explicitly permit or prohibit the use of such third parties? Would permitting their use further remove a provider from its responsibility to abide by RMD requirements? If we permit their use, should we place any requirements or restrictions on their use? For instance, should we only permit providers to use third parties to input information in the filing but maintain the requirement that an officer of the provider make the declaration? What adjustments, if any, would we need to make in the RMD system to permit this? Should we require that providers ensure their third party provides their contact information on the RMD submission form, including their name, primary address, email address, and phone number, and if the third party is registered to do business with the Commission, the third party's FRN? Should we require that third parties be agents of the provider and modify the declaration requirement to permit that it be completed by an officer or agent of the company? Would such a change result in more filings that do not accurately reflect the information and practices of the provider or allow providers to avoid liability for the failures of the third party? Since the obligation to properly fulfill RMD filing requirements remains with providers, will that deter them from using bad actor third parties, or should we create another mechanism to prohibit providers from using bad actor third parties that we identify? Even though the RMD filing obligations remain with providers, should we grant a safe harbor to providers who have used third parties unless and until we adopt any rules concerning their use and those rules go into effect?

2. What Information Must Be Submitted

In this section, we propose and seek comment on a number of measures to codify or improve the accuracy and completeness of information that providers must submit in the RMD. Under current rules, providers must submit information that fits into five categories that we propose to codify: (1) certifications; (2) robocall mitigation information; (3) business identifying information; (4) provider type and service information; and (5) a robocall mitigation plan. Certifications are required for each role the provider plays in the call path and include certifications: that all calls it originates, carries, or processes on its network are subject to a robocall mitigation program that complies with Commission rules; that any prior filing has not been removed by Commission action and it has not been prohibited from filing in the RMD; and that identify whether it has fully, partially, or not implemented the STIR/SHAKEN caller ID authentication framework on the IP portions of its network. A provider's robocall mitigation program must include reasonable steps to avoid originating, carrying, or processing illegal robocall traffic and a commitment to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate, carry, or process calls. Additionally, providers must include a statement of their commitment to respond to traceback requests and cooperate with investigating and stopping illegal robocalls in their RMD filings. Robocall mitigation information includes information regarding any recent enforcement actions concerning illegal robocalls or a non-compliant RMD filing. Additionally, if the provider certifies to partial or no STIR/SHAKEN implementation, it must identify an applicable extension or exemption and provide a detailed explanation of why the claimed extension or exemption applies to the filer. We use the term ''exemption'' generally to refer to both exemptions and extensions from implementing STIR/SHAKEN. Business identifying information includes: business name and business address; any other business name(s) currently in use by the provider; all business names previously used by the provider; the name title, department, business address, telephone number, and email address of one person within the company responsible for addressing robocall mitigation-related issues; and information regarding principals, affiliates, subsidiaries, and parent companies. Provider type and service information includes: the provider's role(s) in the call path; whether the provider is a foreign voice service provider; and the provider's OCN, if it has one. The robocall mitigation plan must describe the specific reasonable steps the provider has taken to avoid originating, carrying, or processing illegal robocalls as part of its robocall mitigation program based on the role(s) it serves in the call chain, including: (1) a description of the affirmative, effective measures it is taking to prevent new and renewing customers from originating illegal robocalls, including a description of how it complies with its obligation to know its customers (if it is an originating provider); (2) a description of the procedures it uses to know its upstream providers; and (3) a description of any call analytic system(s) that it utilizes, including those operated by a third-party vendor. Except as discussed below, we do not intend to further modify providers' obligations under these categories, as we believe the streamlined rules, as proposed in the *KYUP FNPRM* if adopted, are sufficiently clear and precise, but we seek comment on this view.

a. Certifications

We propose and seek comment on certification and related requirements that are used to hold providers accountable, including for STIR/SHAKEN attestation, lack of candor, compliance with illegal call rules, and traceback commitments and cooperation with investigations.

STIR/SHAKEN attestation certification. We propose to require that all voice service providers that serve

end users directly certify compliance with any attestation rules adopted in response to the *KYUP FNPRM.* The *KYUP FNPRM* proposed STIR/SHAKEN attestation-level requirements and prohibitions. It also proposed to require all voice service providers that serve end users directly to make attestation-level decisions for their end users' Session Initiation Protocol (SIP) calls, Functionally, the latter proposal would only create a new attestation obligation for non-facilities-based providers, since facilities-based providers should already make attestation decisions when they serve end users directly to fulfill their STIR/SHAKEN implementation obligation. Although the proposed streamlined rules in the *KYUP FNPRM* include a provision that would require all voice service providers that serve end users directly to certify in the RMD that they are compliant with the proposed attestation requirements, we did not formally propose the certification requirement in the body of the *KYUP FNPRM* and so we do so here. We believe the proposed attestation certification is important, as it represents an acknowledgement of the new role that non-facilities-based providers would play in the STIR/SHAKEN ecosystem if the *KYUP FNPRM* proposal is adopted, and it would provide a strong basis for accountability for both facilities-based providers and non-facilities-based providers. We seek comment on this proposal and our analysis.

Lack of candor certification. We propose that providers must certify that they have not submitted false, misleading, or inaccurate information to the Commission, any agent or other third party designated by the Commission or acting on behalf of the Commission pursuant to Commission rules or direction, or the Governance Authority. The Enforcement Bureau recently issued a Show Cause Order to Mexico IP Phone, LLC on why it should not be removed from the RMD related to its submission of false information to the NANPA. Although there is a valid basis for removal under existing rules, we believe this proposal will provide a more direct basis for actions like these. We believe that such agents or designated entities include, at a minimum, the industry traceback consortium and the North American Numbering Plan Administrator (NANPA), as both of these entities, as well as the Governance Authority, serve important roles in the robocall mitigation ecosystem. We seek comment on this proposal. Should we include any other entities?

Certification of compliance with illegal call rules. We propose to require that providers certify that they are in compliance with all applicable Commission rules pertaining to robocalls and other illegal calls, including all those in Subparts L, P, and HH of Part 64 and those in Part 52. We believe that these certification obligations would give the Commission a clear and direct basis to remove providers from the RMD for submitting invalid certifications when they violate any Commission rule related to illegal calls and numbering administration. We seek comment on this proposal. Should we require providers to certify their compliance with other applicable Commission rules? Below, we seek comment on the causes for removing providers from the RMD.

Traceback commitments and cooperation with investigations. We propose to simplify providers' commitments related to responding to traceback requests and cooperation with investigating and stopping illegal calls to make it more administrable. Under our existing rules, providers are required to: (1) include in their robocall mitigation programs a ''*commitment* to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service'' to originate, carry, or process calls; and (2) include in their RMD filing a *statement* of that commitment. We propose to simplify these requirements and strengthen the cooperation obligation by establishing one requirement that providers certify on the RMD submission form that they commit to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium and another requirement that they certify to cooperate with the Commission, law enforcement, and the industry traceback consortium in investigating and stopping their network or services from being used to transmit illegal calls. We seek comment on this proposal.

We also seek comment on whether we should require providers to participate in the automated traceback response process established by the currently designated industry traceback consortium—the Industry Traceback Group (ITG)—in order to be listed in the RMD. Our understanding is that the ITG uses different methods to perform tracebacks, one of which involves using a secure platform to automate provider responses and incident reporting. As we understand it, this automated process expedites tracebacks and thereby enables the ITG to identify the source of suspected illegal calls more quickly. Given that bad actors are able to generate a significant number of illegal calls in a short timeframe, which can result in substantial harm to consumers, we believe it is important that tracebacks be completed quickly so that illegal calls can be stopped as soon as possible. We seek comment on the feasibility and costs of requiring all providers to participate in the automated traceback response process as a condition of being listed in the RMD, as well as any other benefits or drawbacks of such a requirement, including resource constraints for the ITG. As an alternative, should we simply require that providers participate in the automated traceback response process directly, rather than requiring them to participate in the process as a condition of being listed in the RMD?

b. Robocall Mitigation Information

We propose and seek comment on measures to enhance robocall mitigation information requirements, including strengthening the obligations for providers claiming STIR/SHAKEN implementation exemptions, adopting a temporary exemption for providers in the process of obtaining an SPC token, clarifying requirements related to prior enforcement actions or investigations, and requiring providers to submit additional information regarding their use of third parties.

Strengthening the requirement for claiming STIR/SHAKEN implementation exemptions. We propose to strengthen the requirement that providers identify and explain the basis for claiming a STIR/SHAKEN implementation exemption, building upon the streamlined rules proposed in the *KYUP FNPRM.* When a provider files in the RMD, it must provide a certification regarding its STIR/SHAKEN implementation status. If a voice service provider certifies to less than full STIR/SHAKEN implementation, it must identify the exemption it is claiming and the basis for the exemption.

Currently, providers may be exempt from implementing STIR/SHAKEN pursuant to four implementation exemptions. First, because STIR/SHAKEN only works on IP-based voice networks, the TRACED Act grants an ongoing implementation extension for providers' non-IP networks. Second, pursuant to the TRACED Act, the Commission granted and has maintained an ongoing undue hardship extension for providers that cannot obtain the SPC token required to

implement STIR/SHAKEN due to the Governance Authority's policy requirements, which the Commission proposed to repeal in the *KYUP FNPRM.* Third, the Commission adopted another ongoing undue hardship extension in 2023 for small voice service providers that originate calls via satellite using U.S. NANP numbers, which the Commission sought comment on repealing in the *KYUP FNPRM.* Fourth, providers that lack control over the network infrastructure necessary to implement STIR/SHAKEN are exempt from implementing STIR/SHAKEN, which the Commission proposed to codify and rename as the ''non-facilities-based provider exemption'' in the *KYUP FNPRM.*

For providers to fulfill the obligation to identify any exemptions they are claiming and explain the basis for the exemption, the Commission has stated that they ''must both explicitly state the rule that exempts it from compliance and explain in detail why that exemption applies.'' However, Commission staff have observed, based on a preliminary review, that some RMD filings fail to identify a valid exemption and/or fail to adequately explain why an exemption applies. For example, some providers assert that an exemption applies because they are small providers or do not have access to numbering resources, neither of which are valid bases for claiming an exemption. The categorical STIR/SHAKEN implementation exemption for non-facilities-based and facilities-based small voice service providers expired on June 30, 2022, and June 30, 2023, respectively. While a prior version of the Governance Authority's token access policy required providers to ''[h]ave direct access to telephone numbers from the [NANPA] . . . and National Pooling Administrator,'' the Governance Authority updated its policy and removed this requirement in November 2020. Other providers simply state that they do not have an SPC token or that their downstream providers perform the STIR/SHAKEN authentication on their behalf, which also do not qualify as valid bases for claiming an exemption.

To help address these issues, and given our proposal in the *KYUP FNPRM* to codify all valid exemptions, we now propose to strengthen the requirements for claiming an exemption. First, we propose to codify the requirement that a provider claiming an exemption cite the specific rule for the exemption. We could change the format of the RMD submission form in several ways to enable providers to submit this information, including by implementing a new field on the form or by adding a drop-down list of currently valid exemptions. Second, we propose to codify the requirement that a provider ''explain in detail why [an] exemption applies,'' and expand it to require that the provider include the facts specific to its network and services that are relevant to the scope of the exemption(s) and any steps it has taken to confirm that it cannot implement STIR/SHAKEN, or indicate that it is a foreign voice service provider not subject to STIR/SHAKEN implementation. We seek comment on this proposal and on what specific information providers should be required to supply to ensure they demonstrate that an exemption applies.

Temporary exemption for providers in the process of obtaining an SPC token. We propose to adopt a new temporary exemption for providers that are in the process of obtaining an SPC token to ensure that providers can comply with our STIR/SHAKEN implementation certification requirement and the Governance Authority's existing token access policy. To implement STIR/SHAKEN, our rules require providers with a STIR/SHAKEN implementation obligation to obtain an SPC token, and the Commission has stated that providers are prohibited from certifying to complete or partial STIR/SHAKEN implementation in the RMD unless they have obtained an SPC token. At the same time, the Governance Authority's SPC token access policy currently requires, in relevant part, that providers ''[h]ave certified with the [Commission] that they have implemented STIR/SHAKEN or comply with the [Commission's robocall mitigation program] requirements and are listed in the [RMD].'' The Governance Authority's current SPC Token Access Policy requires providers to: (1) have a current Form 499–A on file with the Commission, (2) have been assigned an OCN, or Resp Org ID and (3) have certified with the Commission that they have implemented STIR/SHAKEN or comply with the Commission's robocall mitigation program requirements and are listed in the RMD. Thus, newly established providers are not able to comply with our certification requirement and the Governance Authority's token access policy when they are in the process of obtaining an SPC token.

To allow providers to accurately complete their STIR/SHAKEN implementation certification in the RMD and to resolve the conflict between our rules and the Governance Authority's policy, we propose to adopt a temporary exemption for providers that are in the process of obtaining an SPC token to implement STIR/SHAKEN. We propose to require providers claiming this temporary exemption to follow the strengthened requirements for claiming an exemption that we propose above, including providing a description of the steps they have taken to obtain an SPC token. We also propose to require that, at the time that such providers claim this exemption on the RMD submission form, they provide their OCN. This would be a mandatory requirement for providers to be able to claim the temporary exemption, while they are in the process of obtaining an SPC token. Currently, providers are required to provide an OCN on the RMD submission form if they have one, but having an OCN is a prerequisite to obtaining an SPC token, and we believe requiring providers to provide an OCN at the time they claim the temporary exemption will demonstrate that the provider is in fact pursuing an SPC token in good faith. We seek comment on these proposals. Should we require providers to submit any additional information regarding their registration status, and if so, what? When providers become authorized to obtain an SPC token and update their filing to indicate their implementation of STIR/SHAKEN, should we require them to insert the date they received the SPC token authorization or any related information?

We also propose to establish measures to ensure use of the exemption remains temporary and seek comment on how best to do so. For instance, should we set a specific number of days after which a filing claiming the exemption will be suspended or removed from the RMD if the provider has not updated the filing to remove the exemption and indicate that it has implemented STIR/SHAKEN? If so, how many days is sufficient to ensure that providers have sufficient opportunity to obtain an SPC token and update their STIR/SHAKEN implementation status in the RMD? Should such suspensions or removals occur automatically or be processed manually by Commission staff? Under our existing rules, providers have an ongoing obligation to update their RMD filings within 10 business days of ''any change to the information'' submitted.

Harmonizing the prior action or investigation requirements. We propose to harmonize two provisions related to prior enforcement actions or investigations. Under our current rules, voice service providers must certify ''that any prior certification has not been removed by Commission action'' and that they have ''not been prohibited from filing in the Robocall Mitigation Database by the Commission.'' At the

same time, voice service providers must state: whether, at any time in the prior two years, the filing entity (and/or any entity for which the filing entity shares common ownership, management, directors, or control) has been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.

Thus, when a provider states that it has been the subject of a formal enforcement action or investigation in the prior two years, it can create an apparent contradiction with the requirement that the provider certify that ''any prior certification has not been removed by Commission action.''

To address this contradiction, we propose to revise the first certification to simply require that a provider certify that it ''is not presently prohibited from filing in the Robocall Mitigation Database by the Commission.'' Because providers may be permitted by the Commission to file in the RMD after they have been removed by a Commission action under certain circumstances, we think this revised certification will better capture our goal of deterring providers from refiling when they are not permitted to do so. We seek comment on this proposal.

Findings of wrongdoing statement. We also take this opportunity to invite comment on whether, and to what extent, we should revise the language in the prior action or investigation statement requirement regarding the findings of wrongdoing. The current language requires providers to state the ''findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description.'' Should we simplify and clarify the language by revising it to ''due to the filing entity transmitting, or facilitating the transmittal, of illegal robocalls or spoofing . . . .''? Should we revise the language to include all illegal calls and not just illegal robocalls to provide transparency regarding all relevant wrongdoing?

Simplifying prior action and investigation description obligations. Under our current rules, providers that state they have been subject to prior actions or investigations with accompanying findings of actual or suspected wrongdoing in the prior two years must provide a description of any such action or investigation. The description must include: (1) ''[a]ll law enforcement or regulatory agencies involved;'' (2) ''the date that any action or investigation was commenced;'' (3) ''the current status of the action or investigation;'' (4) ''a summary of the findings of wrongdoing made in connection with the action or investigation;'' and (5) ''whether any final determinations have been issued.'' We believe that, as written, these required elements are unnecessarily cumbersome without a corresponding benefit. For instance, the date an action commenced may not be as relevant as the date that any findings of actual or suspected wrongdoing were issued, and if a document describing findings of wrongdoing is publicly available, the summary of such findings seems unnecessary. Additionally, because ongoing investigations are dynamic, providers may have a continuous obligation to keep their filings updated with changes under our current rules.

Accordingly, we propose to simplify the prior action or investigation certification requirement to solicit enough information to identify the enforcement action, the agency or agencies that issued it, and the nature of the findings, which we believe will reduce burdens on providers and improve administrability. Specifically, we propose to require that, except to the extent and only for the period during which an action or investigation has been designated as non-public or confidential by a law enforcement agency, regulatory agency, court, or other governmental entity that is involved, providers must provide: (1) all law enforcement or regulatory agencies involved; (2) the date any findings of actual or suspected wrongdoing were issued; (3) one or more identifier for the action or investigation, such as a file number, case number, or document number; and (4) a URL to access a publicly available document that describes the findings of wrongdoing made in connection with the action or investigation, or if no such document is publicly available, a copy of such document, or if not memorialized in a document, an accurate summary of the specific findings of wrongdoing made in connection with the action or investigation, including whether the findings constitute an actual determination of wrongdoing or a suspected determination of wrongdoing. We believe this information is sufficient for the Commission and third parties to identify and evaluate the nature of an action or investigation. We seek comment on this proposal and analysis. Should we require providers to include any additional information in their descriptions, such as details regarding prior actions or investigations involving an entity with which it shares common ownership, management, directors, or control? Should we add an additional element requiring providers to describe the actions they have taken to address or mitigate the actual or suspected determinations? While our rules require providers to state whether ''the filing entity (and/or any entity for which the filing entity shares common ownership, management, directors, or control) have been the subject of formal . . . action or investigation,'' our rules do not specifically require a description of the actions or investigations involving those entities.

Use of third parties. We propose to require that providers submit additional information in the RMD regarding their use of third parties, which we believe will enhance accountability. Specifically, we propose to require that voice service providers indicate whether or not they engage third parties for the following: (1) performing call analytics; (2) performing the technological act of signing calls to satisfy STIR/SHAKEN obligations; (3) fulfilling KYC and KYUP obligations; and (4) submitting RMD submissions to the Commission if we permit providers to use third parties for this purpose. Providers are already required to state whether they use third-party vendors for call analytics and to name such vendors in their robocall mitigation plans, but we believe this requirement has caused confusion regarding providers' obligation to disclose when they do not use a third-party vendor. We believe our proposal will clarify that providers must disclose if they do not use third parties and that moving these requirements to the RMD submission form with the other third-party disclosures will simplify and streamline the requirement. We discuss providers' separate obligation to describe their call analytics practices below. The Commission currently permits voice service providers with STIR/SHAKEN implementation obligations to engage third parties to perform the technological act of signing calls, subject to certain conditions. In the *Eighth Caller ID Authentication Order,* 90 FR 40241 (Aug. 19, 2025), the Commission declined to require providers to identify the third-party authentication solutions they used in their RMD submissions, finding that such an obligation would increase

administrative burdens for providers and offer minimal benefits. As the Commission explained, however, we would continue to monitor providers' compliance with the adopted third-party caller ID authentication requirements to ''determine whether additional information would assist our compliance reviews and enforcement activities in the future.'' With greater experience, we now believe that the benefits associated with such a requirement outweigh the costs of ensuring compliance with STIR/SHAKEN implementation obligations. We seek comment on that belief. We discuss providers' separate obligation to describe their KYC and KYUP practices below. Above, we seek comment on providers' use of third parties for submitting their RMD filings and whether we should establish and requirements or prohibitions on use of third parties for this purpose. We also propose to require providers to name any third parties they use and provide the following information for each third party: email, phone number, and, if available, website. In all cases, we reiterate that the compliance obligation remains with the provider, and not any third party, which we believe will incentivize providers to use reputable third parties. We believe that these third-party disclosure requirements will promote accountability by facilitating our ability to evaluate whether providers are engaging legitimate third parties that have adopted appropriate practices and to allow us to better identify potential causes of non-compliance when, for example, several non-compliant providers are using the same third party. We propose below that this third-party information would not be listed in the public database and would instead only be viewable by Commission staff. We seek comment on these proposals and analysis. What are the benefits and downsides of requiring providers to submit such information? If we should not require any such information, why not? Are there other uses of third parties we should require providers to disclose, such as use of third parties for call branding information?

c. Business Identifying Information

In this section, we propose and seek comment on a number of measures to codify existing requirements and expand providers' obligations to submit business identifying information to the RMD.

Principals, affiliates, subsidiaries, and parent companies. We propose to codify the existing requirement that providers submit information regarding their principals, affiliates, subsidiaries, and parent companies and to better specify what information they must provide.

The Commission established a requirement that providers disclose information about principals, affiliates, subsidiaries, and parent companies with ''sufficient detail to facilitate the Commission's ability to determine whether the provider has been prohibited from filing in the Robocall Mitigation Database'' in the *Sixth Caller ID Authentication Order,* 88 FR 40096 (June 21, 2023), but it did not codify the requirement in its rules. Some providers appear to have been confused concerning what information must be supplied, which has resulted in deficient filings. We endeavor to resolve that confusion. *First,* we propose to codify definitions for principal, affiliate, subsidiary, and parent, and seek comment on what those definitions should be. Should we simply refer to existing definitions for these terms or establish new definitions for them? *Second,* to prevent a provider from masking its relationship with prohibited entities, we propose to codify the requirement that providers identify *all* principals, affiliates, subsidiaries, and parent companies in their filings, which we believe was already required, but may not have been clear when coupled with the ''sufficient detail'' qualification described above. However, we seek refreshed comment on the burdens of this obligation and on steps we can take to minimize those burdens, such as requiring providers to update this information less frequently. Below we seek comment on whether to change the frequency with which providers must update their RMD filings. *Third,* we propose to codify the existing requirement for providers to identify human principals, which many providers fail to do. We believe that all providers necessarily have at least one human principal—an individual who exercises influence, management, or supervisory responsibility, whether or not that individual has ownership or control of the filing entity—and therefore are already required to disclose such an individual in their RMD filing as part of the requirement to disclose principals. *Fourth,* we propose to require providers to submit specific information regarding their human principals, including their title, telephone number, email address, physical address, country of residence, and citizenship. *Fifth,* we propose to maintain the requirement for providers to identify all other principals, affiliates, subsidiaries, and parent companies, and to require providers to submit the RMD number for entities that are in the RMD or the business address for entities that are not in the RMD. We use the term ''business address'' to refer to a physical address that is a bona fide place of business and is not a virtual address, shared office location without a dedicated suite or floor. P.O. Box, mail forwarding service, hosted service location, or address shared by multiple unrelated or purportedly unrelated businesses. We believe this would provide the minimum detail necessary to facilitate the Commission's ability to determine whether the provider has been prohibited from filing in the RMD. We seek comment on these proposals and justifications.

Should we require that providers supply additional information about their principals, affiliates, subsidiaries, and parent companies to aid our oversight, such as any prior business names or trade names (DBAs)? Should we require that they provide copies of government issued identification for human principals, and if so, should we require that they submit a photo of each principal with their ID? Should providers be required to disclose only one human principal? Should they be required to disclose one or more human principals for the provider's affiliates, parents, or subsidiaries?

Registered U.S. agent. We propose to require providers to identify and provide contact information for a U.S. registered agent to aid in enforcement actions. We propose that the contact information must include a U.S. mailing address, telephone number, and email address. Although our existing and proposed RMD filing requirements include identifying and providing contact information for individuals who work for the provider, a registered agent acts as a designated point of contact with the provider for communications with law enforcement and regulatory agencies, and to receive service of legal documents. We believe that requiring designation of a U.S. registered agent will particularly support enforcement actions against foreign entities, including those that establish nominal offices, operations, or facilities in the United States (as opposed to a bona fide independent business operation) with the goal of having their calls be viewed as originating in the United States. Specifically, it would establish a reliable contact in the United States for serving legal documents and could help establish jurisdictional reach over the provider. We invite comment on this proposal and analysis, including potential costs or challenges for certain providers, such as small providers, and any alternative approaches to alleviate

those costs and challenges. Should we harmonize this requirement with the Form 499 requirements to designate an agent for service of process? Common carriers, as well as VoIP providers, must ''designate in writing an agent in the District of Columbia'' upon whom all notices, process, orders, and decisions made by the Commission may be served on behalf of that carrier in any proceeding pending before the Commission, while carriers that hold international Section 214 authorizations must designate a U.S. citizen or U.S. lawful permanent resident as their agent for service of process.

d. Provider Type and Service Information

We next propose and seek comment on measures to improve the accuracy of provider type and service information submitted to the RMD. Specifically, we propose to revise the existing requirements for providers to identify their role in the call chain and seek comment on allowing entities that identify as end users to submit RMD filings, ensuring providers accurately identify as a foreign voice service provider, and requiring providers to submit information about their numbering resources and KYUP business information.

Role in the call chain. We propose to further revise our existing requirements for providers to identify their role(s) in the call chain in line with our proposed definitions in the *KYUP FNPRM.* Our existing rules generally require providers to identify whether they are a voice service provider, gateway provider, or non-gateway intermediate provider with or without a STIR/SHAKEN implementation obligation. The *KYUP FNPRM* proposed to reinterpret the meaning of ''voice service provider'' to include gateway providers and non-gateway intermediate providers, as well as to add new definitions for facilities-based provider, non-facilities-based provider, originating provider, and terminating provider. The proposed streamlined rules in the *KYUP FNPRM* would require providers to identify which of those types of providers they are and separate out the requirement to state whether they have a STIR/SHAKEN implementation obligation. We propose to further revise those streamlined rules to better capture a provider's role(s) in the call chain, as follows:

- a voice service provider must indicate whether it is a facilities-based provider and/or a non-facilities-based provider;
- a facilities-based provider must indicate whether it is: (i) an originating or terminating voice service provider directly serving end users; (ii) an originating or terminating provider acting as a wholesale provider originating or terminating calls for end users it does not directly serve on behalf of another provider or providers; (iii) a gateway provider; and/or (iv) a non-gateway intermediate provider (Note, however, that in the *KYUP FNPRM* we sought comment on whether intermediate providers are considered facilities-based providers. If we determine they are not, we expect we would remove the intermediate provider subcategories (*i.e.,* ''(iii) a gateway provider'' and ''(iv) a non-gateway intermediate provider'') from this ''facilities-based provider'' provision and create a separate provision that requires providers to indicate if they are one of the subcategories of intermediate provider.);
- A non-facilities-based provider must indicate whether it is directly serving end users and/or whether it is a wholesale provider to another provider or providers that does not directly serve end users.

Consistent with our established approach that a provider's role is determined on a call-by-call basis, these categories are not mutually exclusive, recognizing that a provider can be a facilities-based provider for some calls and a non-facilities-based provider for other calls, and that the same is true for each sub-category. Additionally, we propose to eliminate the current requirement that providers state whether they have a STIR/SHAKEN implementation obligation, which we maintained in the proposed streamlined rules in the *KYUP FNPRM.* All voice service providers are required to implement STIR/SHAKEN unless they are subject to an exemption, and they are already required to certify to their STIR/SHAKEN implementation status in a different part of our rules. We seek comment on these proposals and analysis. Should we require providers to indicate whether they are an initiating provider, as we propose to define that term in the *KYUP FNPRM*? Are there instances when a provider will not be aware that it is acting as a wholesale provider, such as if the provider's customer resells the provider's service without the provider's knowledge? Do providers allow customers to resell service without the provider's knowledge, and if so, is that contrary to their existing requirement to know their upstream provider? Should we modify the proposed requirement to self-identify as a wholesale provider to permit providers to only indicate when they knowingly serve as a wholesale provider?

We also seek comment on whether we should add an option on the RMD submission form for entities to indicate their belief that they are an ''end user'' and not a ''voice service provider,'' to address instances when such entities feel compelled to file in the RMD. Although end users are not required to file in the RMD, and we do not condone voice service providers compelling their end users to submit RMD filings, Commission staff have observed that some entities that do not consider themselves ''voice service providers'' nevertheless submit RMD filings out of an abundance of caution or because the provider supplying them with voice service requires them to do so to transmit their calls. If we adopt such an approach, we expect that we would require such entities to describe the reason they are submitting a filing, provide a detailed explanation of why the entity does not meet the definition of a ''voice service provider'' or the definitions for the subcategories of voice service providers (*i.e.,* initiating, originating, intermediate, terminating, facilities-based, and non-facilities-based), and a description of the nature of the entity's business. We believe such a description would oblige the entity to fully evaluate and explain its role in the call chain, and to provide the Commission and stakeholders with information necessary to adequately assess whether the entity's determination is reasonable. We seek comment on this view. If there are benefits to allowing entities that believe they are end users to file in the RMD and indicate as much, what are these benefits? Conversely, are there potential downsides or unintended consequences, and if so, should we prohibit voice service providers from requiring end users to file in the RMD?

Identifying foreign voice service providers. We seek comment on whether we should establish additional RMD filing requirements to ensure that providers accurately identify when they are a foreign voice service provider. Providers submitting filings in the RMD are already required to indicate whether they are a foreign voice service provider, but as noted above, we are concerned that bad actor foreign providers are certifying that they are not foreign providers even though they do not have bona fide independent business operations in the United States. To fully address this concern, should we require providers to, for example, supply additional business information beyond what we propose or seek comment on herein? What, if any, additional

information would help distinguish bona fide independent domestic business operations from nominal offices or operations? Should we require providers to describe the nature of their U.S. offices, operations, or facilities so we can evaluate whether those operations are a bona fide independent domestic business operation? Should providers be required to provide information regarding their use of hosted servers or shared addresses? Should providers be required to disclose whether any parent company was created, incorporated, or organized abroad or has common ownership or management with a company that was created, incorporated, or organized abroad? How would any such additional requirements dovetail with the proposed revised definition for ''foreign voice service provider'' in the *KYUP FNPRM.*

Numbering resources information. In the *Robocall Numbering Policies NPRM,* 91 FR 25312 (May 8, 2026), we sought comment on measures to increase the transparency about which providers have access to numbers, which we believed would improve our numbering administration and help us deter illegal calls. We seek comment on whether, and the extent to which, we should require providers to submit information about their access to and use of numbering resources in the RMD. For instance, should we require providers to disclose whether or not they have access to numbers directly or indirectly and, if indirectly, from which provider(s) they procured numbers? Should we require them to disclose the block(s) or range(s) of numbers to which they have access? Should we require providers that make numbers available on a wholesale basis to resellers to disclose the providers to which they have resold numbers, and if so, should we require them to disclose the block(s) or range(s) provided to each reseller, as well as the OCNs for the resellers if they have one? Should we inquire about any affiliation that a provider might have with an entity to which they are selling or from which they are buying numbers? What are the benefits and drawbacks of any such requirements, particularly for robocall mitigation and numbering administration? We note that some such information is subject to confidentiality under our rules and seek comment on how to address that confidentiality if we require any numbering information to be submitted in the RMD. Below we seek comment on which information submitted in the RMD should be viewable in the publicly facing Database and which should only be viewable by Commission staff. To what extent would requiring the submission of any such numbering information in the RMD be duplicative of providers' reporting requirements to the NANPA, and what, if any, benefits or burdens would result from such duplicative reporting?

Nature of services. We propose to require providers to submit a general description about the nature of their voice services, including the types of services they offer and the types of customers they serve or intend to serve. We believe this information will help us better understand the types of voice services and business arrangements in the ecosystem, whether providers' robocall mitigation programs are sufficient for the types of services they provide, and whether providers are validly claiming an exemption from the STIR/SHAKEN implementation obligation. We seek comment on this proposal and assessment. Should we establish more specific requirements for what the description must include?

Additional provider information. We seek comment on requiring providers to submit additional information about their businesses in the RMD that largely aligns with the KYUP information we proposed in the *KYUP FNPRM,* or an explanation for why they cannot supply such information. The *KYUP FNPRM* proposes to require that providers obtain information categorized under six types, some of which is already required by our existing RMD rules and some of which is addressed by the discussion above. The following is the remaining information by type that we believe may be beneficial for providers to submit in the RMD. We exclude the ''financial information'' type, as we do not believe there is need to require providers to submit such information in the RMD. We note below when such information relates to an existing RMD filing requirement and we seek comment on whether a requirement to collect such information should replace or augment the existing requirement.

- General business information, including:
  - supporting records for legal business name (*e.g.,* government record, government identification, lease, utility statement, search result from a government website, or report from a legitimate private database that validates company information) (Providers are currently required to submit business name(s).);
  - any prior business names or trade names (DBAs) the company has used in the last three years (Providers are currently required to submit other business names *in use* by the provider.);
  - a physical address that is a bona fide place of business for the upstream provider and is not a virtual address, shared office location without a dedicated suite or floor, P.O. Box, mail forwarding service, hosted server location, registered agent, or address shared by multiple unrelated or purportedly unrelated businesses (Providers are currently required to submit their primary address. Additionally, this description differs slightly from the *KYUP FNPRM* which proposed that providers obtain a physical address that is ''a *real* place of business'' from upstream providers, rather than ''a *bona fide* place of business,'' but the change is for clarity and is not intended to be substantive.); and
  - contact information, including a business telephone number and email address (Providers are currently required to submit the name, title, department, business address, telephone number, and email address of one person within the company responsible for addressing robocall mitigation-related issues.);
- Internet commercial presence information, such as website, social media, or apps;
- Ownership and affiliate information, including:
  - information about owners and company leadership (including ultimate beneficial owners and authorized business representatives), including their name, title, business telephone number, business email address, work address, country of residence, citizenship, and copies of government issued identification (Above, we propose to codify the requirement that providers identify principals, which may include owners and company leadership, and to require that providers submit additional information about each principal.);
  - additional information about the company's parents, affiliates, and subsidiaries, including their business names, trade names (DBAs), place of incorporation, and principal places of business (Above, we propose to codify the requirement that providers identify parents, affiliates, and subsidiaries, and that providers submit additional information about each one.);
  - names, addresses (including country), email addresses, and ownership stake for all individuals with 10% or more direct or indirect ownership of the company; and
  - whether or not the provider or its parents, affiliates, subsidiaries, principals, owners, or leadership, and other companies where any such persons have served as a principal,

owner, or leader, have been the subject of any criminal or regulatory investigations or actions in the past five years and the nature of such investigations or actions;

- Operational information, including:
  - place of formation and corporate formation records, including proof of good standing;
  - location of its principal operations, how long the company has been operating, and whether the company has any foreign ownership or management; and
  - business registration number in its jurisdiction (such as federal or state Employer Identification Numbers (EINs) for U.S. providers and the foreign-equivalents for foreign providers);
- Service information, including (Above, we propose to require that providers describe the nature of their services.):
  - whether it relies on non-Internet Protocol (IP) technology; and
  - whether another voice service provider has refused or discontinued service to the provider for any of the reasons described in the *KYUP FNPRM* and the reason(s) for such refusal or discontinuance. (This description differs from the *KYUP FNPRM,* which proposed that providers obtain information as to whether another voice service provider has refused or discontinued service to the upstream provider generally. At least in the context of the RMD, we believe this information should be limited to the refusal and discontinuance reasons set out in the *KYUP FNPRM.*)

We believe that requiring providers to submit this information could enhance our ability to evaluate providers and their practices, and ultimately reduce the need for extended reviews and investigations. We also believe it could enhance the ability of other providers to perform KYUP obligations, particularly if we adopt our KYUP proposals in the *KYUP FNPRM.* Additionally, we think the incremental costs of any such requirements are likely negligible if we adopt our KYUP proposals, as providers will need to compile and supply this information to their downstream providers already. We seek comment on these views and other benefits or drawbacks to providers submitting this information in the RMD.

e. Robocall Mitigation Plan

In this section, we propose and seek comment on measures to strengthen the robocall mitigation program and plan obligations for all voice service providers. As part of our efforts to improve the reliability of RMD filings, we invite comment on the extent to which any of the information required under our proposals should be provided on the RMD submission form instead of in the robocall mitigation plan.

Heightened robocall mitigation program requirement. We propose to enhance the general requirement that providers implement a robocall mitigation program to align with our expectations set out in existing and proposed rules. Under the Commission's current rules, voice service providers are required to ''implement an appropriate robocall mitigation program'' that includes ''reasonable steps'' to avoid, as applicable, the origination, carrying, or processing of illegal robocall traffic. The proposed streamlined rule in the *KYUP FNPRM* would require that each voice service provider take ''reasonable steps to prevent its network or services from being used to transmit illegal robocalls.'' We propose to further revise the streamlined rule in the following two ways.

First, we propose to require that all voice service providers implement a robocall mitigation program that includes ''affirmative, effective measures'' rather than just ''reasonable steps.'' Although the Commission has previously declined to replace the ''reasonable steps'' general mitigation standard with the ''affirmative, effective measures'' standard, we now believe the existing requirement is too lax, as it allows providers to skate by without adopting meaningful robocall mitigation practices. Specifically, we do not believe the ''reasonable steps'' requirement compels providers to institute an ongoing effort to ensure that the measures that comprise their robocall mitigation program are effective. Our revised requirement would also align with providers' existing general KYC obligation and our recently proposed heightened general KYUP obligation, thereby promoting regulatory consistency and administrability. We seek comment on this proposal and analysis. If we adopt such an approach, should we provide additional guidance to voice service providers about what measures would be deemed ''affirmative'' and ''effective,'' and if so, what should that guidance include?

Second, we propose to amend the rule to require that providers' mitigation measures be designed to prevent their network or services from being used to transmit all illegal calls and not just illegal *robo*calls. When the Commission first developed the RMD to collect robocall mitigation program information for providers that received a STIR/SHAKEN implementation exemption, it followed the TRACED Act's usage of the term ''robocall mitigation program.'' However, the Commission has frequently stated its intent to combat all illegal calls, and not just calls that meet the technical definition of a robocall, which may only include certain scam, fraud, and otherwise impermissible calls. For example, a recent survey indicates that once a scammer has made initial contact with a victim—which can occur through various channels—further communication frequently involves phone calls that might or might not meet the legal definition of a ''robocall.'' Indeed, the Commission's KYC rule requires providers to take affirmative, effective measures to prevent new and renewing customers from using their networks to originate ''illegal calls,'' its KYUP rule requires providers to take reasonable and effective steps to ensure that upstream providers are not using them to carry or process a high volume of ''illegal traffic,'' and its call blocking rules also refer to the general categories of illegal calls or illegal traffic. Given the Commission's emphasis on combatting all illegal calls, and that the Commission and stakeholders often use the term ''robocall'' colloquially to refer to all illegal calls, we believe that responsible providers already design their robocall mitigation programs to prevent their networks or services from being used to transmit all illegal calls, and not just illegal robocalls. To the extent that is not the case, we propose to amend the robocall mitigation plan rule to require that providers implement measures to address all ''illegal calls.'' Below, we propose to extend this change throughout § 64.6305. We believe this proposal would promote regulatory consistency within our rules targeting illegal calls. We seek comment on this proposal and analysis.

Strengthened robocall mitigation plan requirements. We propose to strengthen the existing requirement that providers submit a description of their robocall mitigation program (*i.e.,* a robocall mitigation plan) to sync the rule with our proposed heightened robocall mitigation program standard, ensure providers take their robocall mitigation program obligations seriously, and provide a firmer basis for holding providers accountable. Under our current rules, providers must submit with their RMD filing a robocall mitigation plan that describes the specific reasonable steps they have taken to avoid, as applicable, originating, carrying, or processing illegal robocall traffic as part of their robocall mitigation program, including a description of how they comply with

KYC and KYUP requirements and the analytics systems they use to identify and block illegal traffic. Voice service providers must describe how they are complying with their existing obligation to ''[t]take affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal traffic.'' Voice service providers and non-gateway intermediate providers must describe any KYUP procedures in place, and gateway providers must provide a description of how they comply with their KYUP obligations. We first propose to align the rule with the proposal above by requiring that providers describe the affirmative, effective measures they use to prevent their network and services from being used to transmit illegal calls. We also propose to raise the standard for the level of information that providers must include in the descriptions of their robocall mitigation programs by requiring that such descriptions be detailed. We seek comment on these proposals.

We also seek comment on whether we should require that providers submit more specific information about how they comply with KYC and KYUP obligations, particularly in light of our proposals in the *KYC FNPRM,* 91 FR 30596 (May 26, 2026), and *KYUP FNPRM.* For example, should we require voice service providers to describe their customer identification, verification, and retention practices? Should we require providers to describe specific processes and procedures for each of the five categories of baseline KYUP measures—information collection, compliance review, information verification, monitoring, and responsive action—proposed in the *KYUP FNPRM.* Or should we only require that providers describe the KYC and KYUP practices they use beyond any measures the Commission ultimately adopts?

We further propose to require that providers describe the specific call analytics measures they use to identify and block illegal calls and whether or not each measure is performed by the provider or a third party. Above, we propose to require that providers disclose the third parties they use for call analytics on the RMD submission form. We seek comment on what level of detail we should require providers use to describe their call analytics measures that would balance the need for more rigorous review of providers' robocall mitigation plans with concerns that too much detail might provide bad actors with a roadmap to evade analytics-based blocking. Finally, we propose to codify the requirement that providers describe any contractual provisions with end-users or upstream providers addressing robocall mitigation and seek refreshed comment on whether we should require providers to submit specific contractual provisions.

We also seek comment on whether we should require that providers submit any additional or more specific information in their robocall mitigation plans. To date, the Commission has not mandated that providers include specific measures in their mitigation plans, finding that providers require ''flexibility in determining which measures to use to mitigate illegal calls on their networks.'' However, Commission staff frequently identify robocall mitigation plans with minimal information and are concerned that the providers behind those filings may not have implemented adequate robocall mitigation programs. Should the level of detail we require be based on risk, and should we require that providers explain the assessment of their risk? Should we define risk categories for different types of providers or service offerings? The Commission previously declined to impose heightened mitigation obligations solely for VoIP providers, acknowledging that there was evidence that such providers were ''disproportionately involved in the facilitation of illegal robocalls,'' but opting to apply obligations to ''providers regardless of the technology used.'' Should we require that providers include metrics on the effectiveness of their robocall mitigation programs or details about how they follow permissive and required call blocking rules? What would be the benefits and costs of any such requirements?

3. Submitting and Viewing Information

In this section, we propose and seek comment on how providers should submit information to the RMD, the conditions when such information may be public, and when providers must update information and recertify their filings.

a. How Information Is Submitted

Format for each category of information. As it stands today, providers submit information in their RMD filing by inputting the information where required in the RMD form or by uploading a PDF. We propose to designate that the information in the categories of certifications, robocall mitigation information, business identifying information, and provider type and service information must be submitted in the RMD form and that the robocall mitigation plan continue to be uploaded as a PDF. We seek comment on this proposal. Is there certain information in the first four categories that we should require or that providers should be able to submit in their robocall mitigation plans or in a separately uploaded document? We note that our proposal would reorganize where providers submit some information they are currently required to supply, and we encourage commenters to review the proposed rules in Appendix A, which shows the complete list of existing and proposed information by category.

Machine-readable PDFs. We also propose to codify that providers must submit a PDF of their robocall mitigation plans in machine-readable format. Today, providers are required to submit a PDF of their robocall mitigation plan in the RMD. Commission staff use technicals tools to analyze the contents of these PDFs to ensure that they contain the information required by Commission rules. However, some providers submit PDFs that are not machine-readable or searchable, hindering our compliance review process. We think that providers typically have the means to submit robocall mitigation plans in machine-readable format and that some providers may be submitting non-readable PDFs to intentionally stifle our oversight. We acknowledge that the *2026 Broadband Label Order* is repealing a machine-readability requirement, but we do not believe our proposal to establish a machine-readability requirement here is in conflict with the proposal there. The *2026 Broadband Label Order* is repealing a requirement that providers make the contents of labels available in a *separate* machine-readable spreadsheet file format hosted at a dedicated URL, which is distinct from the label that consumers view in their browser that is inherently readable. We do not propose here to create a new requirement that providers submit information in robocall mitigation plans in a separate machine-readable format, merely that they ensure the PDFs they are already required to submit remain machine readable. We seek comment on this proposal and these views.

b. Public, Non-Public, and Confidential Information

One of the primary goals of the RMD is to promote transparency about providers and their robocall mitigation practices, and so we believe that, as a baseline, information we require providers to submit in the RMD should

be made available to the public. At the same time, ''we are committed to ensuring that rules designed to protect consumers from illegal calls do not inadvertently create new risks by mandating the collection, retention, and sharing of sensitive business and personal data without corresponding safeguards.'' We note that providers may also request confidential treatment of information pursuant to § 0.459 of the Commission's rules consistent with the RMD *Protective Order,* which governs the treatment of confidential or highly confidential information included in robocall mitigation program descriptions. Nonetheless, the Commission may make public information that is otherwise confidential when, after balancing the various factors involved, it concludes that it is in the public interest to do so. At the time the Wireline Competition Bureau (Bureau) issued the *Protective Order,* it made clear that ''certifications, contact information, and other data submitted to the Robocall Mitigation Database are public and cannot be marked as confidential.''

In light of these goals and the revisions to RMD filing obligations since the *Protective Order* (including those we propose above), we take this opportunity to propose and invite comment on what information providers submit in the RMD should be available in the public-facing RMD versus what information should only be viewable by Commission staff. Specifically, we propose that the contact and other identifying information for human principals, the business address for non-human principals, affiliates, subsidiaries, and parent companies that are not in the RMD, and information about providers' use of third parties should not be made public. We also propose, above, that providers need not disclose information about prior actions or investigations that have been designated as non-public or confidential by a law enforcement agency, regulatory agency, court, or other governmental entity involved in the action or investigation. We seek comment on this proposal and on whether any other information should not be public. Should we issue or implement additional protective measures for information we determine should not be public?

c. Filing Updates and Recertification

We seek comment on whether we should modify our requirements that set out providers' obligations to update their RMD filings. Under our current rules, providers are obligated to update their filings within 10 business days of ''any change in the information'' submitted, which we believe includes updating the information to reflect changes effectuated as a result of modification to or expiration of Commission rules. Entities and individuals registered in CORES must also update information submitted in CORES to obtain an FRN within 10 business days of any change to that information, which includes information in the RMD that is automatically populated from CORES. They are also required to recertify annually by March 1 that any information submitted to the RMD is true and correct. We believe requirements like these are important to ensuring that RMD filings remain accurate and up-to-date. We also believe, however, that many providers fail to make necessary updates or complete recertifications by the deadlines, thereby requiring us to initiate enforcement activities. We seek comment on ways we can modify the requirements so that providers take these obligations seriously while preventing the obligations from being overly burdensome and allowing for focused review by Commission staff. For instance, should we eliminate the requirement that providers update their filings within 10 business days and instead require that providers update and affirmatively recertify their filings more frequently, such as once a quarter or every six months? If so, should we suspend filings when a provider fails to make updates or complete recertifications using any suspension process we may adopt, as we seek comment on below? Below, we seek comment on whether a provider's RMD filing should be automatically suspended if the provider fails to complete an annual recertification on or before March 1. Are there alternative approaches we should consider? We also seek comment on whether we should specifically state that providers must update their information by established deadlines to account for modification to or expiration of Commission rules.

We seek comment on any procedures or safeguards that should apply before a provider is permitted to delete a filing. Today, providers are permitted to delete their RMD filing if they determine that they are no longer required to have a filing in the RMD. This might occur, for example, if a provider discontinues the provision of voice service or if two voice service providers merge and only one RMD filing is needed for the merged entity. When a filing is deleted, it is no longer visible to the public, which could cause confusion for downstream providers. We are also concerned that bad actors may use the ability to delete filings to circumvent enforcement actions. Should we limit the circumstances in which providers may delete their filings, such as by requiring them to meet specific criteria? If so, what should those criteria be? Should we prevent providers from deleting their filings when the provider is subject to a Show Cause Order issued by the Enforcement Bureau? Are there alternative approaches we should consider? For instance, should we adopt a process that allows providers to suspend, rather than delete, their RMD filings? If so, are any additional safeguards or procedures necessary?

B. Keeping Bad Actor Providers Out of the RMD

We aim to enhance the measures used to ensure that the RMD only includes filings from legitimate providers that are willing and able to comply with the Commission's robocall mitigation, caller ID authentication, traceback, and other illegal call requirements. First, we propose and seek comment on measures to further prevent non-compliant and fraudulent filings from entering the Database in the first instance. Second, we propose and seek comment on tools to better identify non-compliant and fraudulent filings already in the Database, including through enhanced information sharing and technical review of filings. Third, we propose and seek comment on causes and processes for removing bad actor and non-compliant providers, while maintaining clear and administrable protections for providers that make good-faith efforts to comply. Fourth, we seek comment on mechanisms to keep removed providers out of the RMD. We also seek comment on audit requirements and resources for administering the RMD. We believe it is necessary to address these issues using targeted measures to improve the integrity of the Database and reduce opportunities for bad actors to misuse it.

1. Preventing Bad Actor Providers From Getting Into the RMD

We seek comment on how we can prevent non-compliant and fraudulent filings from entering the Database in the first instance, which we believe has a number of benefits, including reduced enforcement burdens, improved reliability of Database information, and reduced ability of bad actor providers to use the Database to obtain access to the U.S. voice network.

Delegation to the Bureau. The Commission has previously delegated authority to the Bureau to implement

and manage the technical and operational aspects of the RMD, including the authority to establish the form and format of submissions to the Database, to make any necessary changes to the RMD portal and submission interface, and to implement any technical data validation solution that it determines is likely to produce benefits that outweigh the solution's costs. In addition, the Bureau has existing authority to develop and administer recordkeeping and reporting requirements for telecommunications carriers, providers of interconnected VoIP services, and providers of broadband service under § 0.91 of the Commission's rules. We believe that these existing delegations are broad and include authority for the Bureau to develop and implement additional measures to prevent non-compliant and fraudulent filings from entering the Database. But to the extent any further clarity is needed, we propose to expressly delegate these functions to the Bureau. We further propose to direct the Bureau to develop these measures in consultation with the Office of Managing Director (OMD), the Office of Economics and Analytics (OEA), and the Enforcement Bureau. This will allow Commission staff to adapt more quickly to evolving bad actor tactics by making practical enhancements to the Database and associated filing and review workflows. The Commission has been continuously upgrading its processes and enhancing measures, both technical and operational, to help weed out bad actors from all parts of the call path and this includes a review of the current RMD processes to mitigate against fraud, waste, and abuse. We seek public comment on best practices, both technical and operational, that have been successful in systems to detect fraud, waste, and abuse, and that will aid in the Commission's efforts to identify indicia that a provider's filing may be non-compliant or that the provider may be attempting to evade Commission rules. For example, such tools could include expedited processes to identify filings that list the same address, telephone number, email address, principal, affiliate, subsidiary, parent company, OCN, or third-party filing consultant as a provider whose filing was previously removed from the Database; filings that certify to STIR/SHAKEN implementation but do not appear consistent with information available from the Policy Administrator; or filings that include robocall mitigation plans that are identical or substantially similar to plans filed by unrelated providers. To aid in the effort, we note that the Policy Administrator maintains a publicly available list of providers authorized to participate in STIR/SHAKEN, which a validation tool could reference to verify a provider's registration status.

''*Appearance*'' *in the Database.* We also propose to establish a new rule that a filing does not ''appear'' in the Database unless and until the filing has been accepted and published in the Database. We further propose to codify that the Bureau may reject, withhold publication of, or place into a pending status any new or updated filing that appears non-compliant, appears to have been submitted in evasion of the Commission's rules or orders, or otherwise requires further analysis before it can be accepted and published in the Database because it appears it would qualify for one of the causes for removal or other enforcement action discussed below. This authority would include, for example, filings that appear to have been submitted by, on behalf of, or for the benefit of a provider whose filing was previously removed from the Database, unless the provider has obtained any consent required under our reinstatement rules. We seek comment on this proposal. Should we describe in our rules the specific circumstances in which the Bureau would be permitted to reject, withhold publication of, or place into a pending status a filing, or should we delegate authority to the Bureau to establish those parameters? Should we otherwise limit the Bureau's authority to reject, withhold, or apply a pending status to a submitted filing? What notice and opportunity to cure, if any, should the Bureau provide to the filing party before rejecting publication? Should the Bureau be permitted to reject publication immediately where a filing is facially or materially deficient, unauthorized, or submitted in apparent evasion of a Commission order, while allowing filers to seek review or resubmit a corrected filing? Should we establish a deadline or shot clock for the Commission to make a final determination regarding filings that have been placed in a pending status? We seek comment on how to ensure that the publication process prevents non-compliant or fraudulent filings from appearing in the Database while preserving a workable path for legitimate providers to correct ministerial or inadvertent errors.

Letter of credit requirement. We seek comment on whether we should require entities that file in the RMD to obtain and submit a standby letter of credit from a bank meeting our capital requirements, along with a bankruptcy opinion of counsel, in support of their RMD filings. The Commission has used letters of credit in other contexts when it has imposed performance obligations. We believe requiring entities to furnish a letter of credit when filing in the RMD could have several benefits. First, the due diligence performed by financial institutions could aid in screening out bad actors seeking to file in the RMD without being a significant barrier to low-risk legitimate voice service providers. Second, the simple act of obtaining a letter of credit could deter both new and existing bad actor providers from filing in the RMD, and thereby keep them from participating in the U.S. voice network. Third, it could increase the likelihood that the Commission could collect forfeiture penalties ordered to be paid by a court from bad actors, thus deterring providers from violating our robocall mitigation rules. Finally, a letter of credit requirement could prevent bad actors from refiling immediately in the RMD under a different name after they have been removed from the Database by an enforcement action, because they would need to secure a new letter of credit. We believe each of these benefits would increase the integrity of the RMD, thereby helping ensure that only legitimate and responsible providers are participating in the U.S. voice ecosystem, and ultimately delivering benefits to consumers and other providers, alike.

We also seek comment on whether a letter of credit requirement, if we adopt one, should be limited to certain entities or to certain circumstances. For instance, should the requirement only apply to foreign voice service providers? Should it only apply to entities filing in the RMD for the first time or should it apply to all RMD filers, including those with existing RMD filings? Should the letter of credit be waived if a company meets certain requirements, such as operating for a period of three years? Would a period of three years properly balance our desire to reduce costs and regulatory burdens with our desire to discourage bad actors from filing in the RMD? For providers in operation for fewer than three years, should we require that the financial institution certify annually within the first three years that the letter of credit remains in effect or should we require that a current, drawable letter of credit be refiled annually? What evidence should we require a provider to submit to establish that it has been in operation for three years?

We further seek comment on how to implement a new letter of credit requirement, if adopted. Should we

decline to accept and publish an RMD filing unless Commission staff has verified that the letter of credit has been issued for an acceptable amount in an acceptable form by an acceptable bank? Should we require providers to submit a letter of credit only after their filings are accepted into the system and the Bureau has not otherwise rejected, placed in a pending status, or withheld the filings from publication based on an apparent cause for removal or other enforcement action? Should we give providers a period of time to submit the required letter of credit after the filing is accepted but before it is published, such as 14 days, 30 days, or some other period? What amount should we require for the letter of credit, and should that amount vary based on the size of the provider, the amount of traffic it transmits, its reported revenues for the most recent year, or some other benchmark? What should be the term of the letter of credit? What eligibility requirements should a financial institution be required to satisfy in order to qualify as an acceptable issuer for a letter of credit? For instance, should we require that financial institutions meet the ''well-capitalized'' criteria established by federal bank supervisory agencies as we do in the Universal Service High Cost Program? Would a requirement that the bank must be registered in the SWIFT financial network be sufficient or would some alternative requirement better identify trusted financial institutions? Are there other circumstances, beyond collecting forfeiture penalties ordered to be paid by a court, that the Commission would be permitted to draw upon the letter of credit?

Alternatives. We also seek comment on whether there are viable alternatives to a letter of credit that we could impose to deter bad actors from entering the RMD, such as requiring surety bonds or other similar instruments or requiring third-party audited financial statements. The Commission has required financial assurances in the satellite context, including surety bonds backed by statutory licensing and administrative authority, and has considered but declined to substitute letters of credit where bankruptcy risk could undermine the Commission's ability to draw on the financial assurance. The Commission also sought comment in a recent *FNPRM,* 91 FR 21761 (Apr. 23, 2026), on bond- or fee-based approaches, potentially related to the RMD, to deter bad actors and take the profit out of unlawful calls originating from outside of the United States. Are there other mechanisms we could use to vet entities before they enter the RMD, such as based on the KYUP requirements we proposed in the *KYUP FNPRM*? For instance, is vetting RMD applicants a task for which the NANPA (in connection with its duty administering numbering resources) or a similarly situated entity, may be suited, subject to an appropriate contract amendment and compensation? What are the potential benefits and drawbacks or unintended consequences of any given approach?

2. Identifying Bad Actor Providers in the RMD

We propose and seek comment on measures designed to enhance our ability to identify non-compliant and fraudulent filings that are in the RMD, including technical measures, expediting the traceback process, information sharing with the Governance Authority, and Foreign Adversary Control attestations.

Technical measures. To enhance measures to identify non-compliant and fraudulent filings already in the Database, we propose to explicitly direct the Bureau to consult with OMD, OEA, and the Enforcement Bureau, as necessary, to develop and implement technical tools to identify and target filings that are deficient, facially deficient, or materially deficient, filings that lack candor, duplicate filings, dummy filings (these are filings that are not associated with an existing provider and that bad actors may be submitting to the Database so that providers whose filings have been removed from the Database can quickly restart the transmission of illegal calls under the business name associated with the dummy filing), filings submitted by related entities, filings associated with known bad actors, and other filings that contain indicia of non-compliance with our rules (such filings may include those that contain independent bases for removal or that contain information that suggests the filing is being used as a vehicle to evade the Commission's caller ID authentication, robocall mitigation, traceback, or other rules aimed at combatting illegal calls). We further propose to direct the Bureau to ensure that any technical measure that it implements complies with all relevant federal data and privacy statutes, along with any other relevant government guidance, such as those addressing use of artificial intelligence. The Commission has already recognized the value of technical validation tools in improving Database integrity, and it has delegated authority to the Bureau to implement a technical data validation solution if the Bureau determines that the benefits would outweigh the costs. We seek comment on these proposed directions to the Bureau to further delineate the scope of its delegated authority. How should the Bureau weigh benefits in the form of reductions in the required staff resources associated with administration of the Database or improved ability to leverage the available information in the Database to general additional actionable insights? Are there experiences at other federal agencies that might provide relevant examples? We also seek comment on technical approaches or best practices currently in use by industry to analyze RMD filings and whether there are means to cross-reference data in RMD filings, the ITG, and third-party sources to maximize the utility of these various resources to identify bad actors.

Expediting the traceback process. We also seek comment on the value of having the ITG expedite the traceback process and the best approaches for doing so. How long does a typical traceback take and how long would it take if all providers in the call path were part of the ITG's existing automated traceback process? Are there other technical solutions or processes to expedite the traceback process? Do we have the authority to direct the ITG to adopt any such process, and if so, should we do so? If not, should we encourage the ITG to adopt such processes, and if so, how? What are the costs and benefits of the existing mechanisms and how would they compare to any alternative mechanisms? Does the ITG have any resource constraints that we should consider, and if so, how could they be mitigated?

Information sharing with the Governance Authority. We also seek comment on whether the Commission should establish better information sharing with the Governance Authority. The Commission has recently strengthened requirements for providers with STIR/SHAKEN implementation obligations, including requiring such providers to obtain their own SPC token and digital certificate and certify to either complete or partial implementation in the Database only if they have obtained an SPC token and digital certificate and sign calls with their own certificate. In addition, the *KYUP FNPRM* proposes additional measures to strengthen the Governance Authority's oversight, including improved policies for issuing and revoking SPC tokens and more robust information sharing with the ITG and call analytics providers. We seek comment on whether the Governance Authority should provide this type of information and other related data to the Commission to assist in identifying non-

compliant and fraudulent Database filings, including OCNs associated with authorized providers, more specific information about SPC token issuances and revocations, additional information about authorized Certification Authorities, and information concerning providers suspected of misusing SPC tokens or applying improper attestations. Should the Commission require the Governance Authority to direct the Policy Administrator to include the OCNs associated with authorized providers on its public list of authorized providers, or should such information be shared with the Commission on a non-public basis? Would inclusion of OCNs help distinguish providers with similar names and help identify filings that falsely or inaccurately claim STIR/SHAKEN implementation? We seek comment on the costs and benefits of such information sharing.

Foreign Adversary Control Attestations. To ensure that the Commission and the public are aware of the Foreign Adversary Control status of all domestic voice service providers, we propose to modify Schedule A of our Foreign Adversary Control rules to include published Robocall Mitigation Database filings, the filer of which is a domestic voice service provider. In the *Foreign Adversary Control Report and Order,* 91 FR 18670 (Apr. 10, 2026), the Commission took steps to address the significant threats that U.S. communications networks face from foreign adversaries and entities with ties to foreign adversaries by requiring all carriers holding domestic 214 authority and interconnected VoIP providers that hold direct access to numbering resources authorizations to submit Foreign Adversary Control attestations and disclosures. These attestation requirements, however, do not cover all voice service providers that transmit voice calls that reach U.S. consumers, as they do not all necessarily hold either authorization. For example, an interconnected VoIP provider that does not have a direct access to numbering resources authorization is not by that fact alone prohibited from originating, carrying, or terminating voice calls in the United States. As the Commission has noted with respect to VoIP providers in particular, ''VoIP providers that do not also provide telecommunications service likely do not hold any other Commission licenses or authorizations that would require them to make the same foreign adversary attestation and disclosures [required of] other communications providers operating in the United States.'' Particularly given the prevalence and problem of foreign-originated illegal calls aimed at U.S. consumers, we propose to close this loophole by requiring all domestic voice service providers with a filing that appears in the RMD to attest to Foreign Adversary Control (*i.e.,* that it is or is not owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary) and to comply with any applicable additional disclosures and reporting requirements as set forth in our Foreign Adversary Control rules. We believe this requirement would ensure that the Commission and the public are aware of the Foreign Adversary Control status of *all* domestic voice service providers that have access to the U.S. voice network. We seek comment on this proposal and analysis. Should we also require providers to certify on the RMD submission form that they have completed the Foreign Adversary Control attestation and that the attestation was negative?

3. Tools for Removal of Bad Actor Providers From the RMD

We propose and seek comment on the tools we use to remove bad actor and non-compliant providers' filings from the RMD. Voice service providers must submit and maintain accurate and complete filings in the RMD. Providers that fail to submit or maintain a compliant filing may be subject to removal from the RMD or a Commission forfeiture. Among others, the Commission has adopted a $10,000 base forfeiture for submitting false or inaccurate information to the Database and a $1,000 base forfeiture for failing to update Database information within 10 business days, and found that these violations continue until cured. Because downstream providers may only accept voice calls directly from another provider if that provider's filing appears in the Database and has not been removed pursuant to an enforcement action, removed providers are effectively prevented from transmitting voice calls on the U.S. voice network. A provider whose filing has been removed is not permitted to re-file in the Database unless and until both the Bureau and Enforcement Bureau consent. In certain limited circumstances, the Bureaus may consent to provisionally reinstate removed providers and require them to bring their filings into compliance or face removal again. Although the Commission's removal actions have been effective at removing bad actor and non-compliant providers' filings (the Commission has removed over 1,400 deficient filings since January 2025), we believe codifying and enhancing removal procedures will enable us to more effectively expel such providers from the voice ecosystem. Accordingly, we aim to codify and clarify removal procedures, focusing on the causes for removal or other enforcement action, removal processes, a grace period for annual recertifications, suspensions, filing status indicators and traffic acceptance requirements, and removal notices.

Causes for removal or other enforcement action. We propose to codify the causes for which a provider may be subject to an enforcement action, including removal of the provider's filing from the Database, to put providers on clear notice, strengthen the foundation for our enforcement actions, and enhance the integrity and reliability of the Database and the U.S. voice network. Specifically, we propose that the Enforcement Bureau retain the discretion to initiate an enforcement action against any voice service provider, including removal of the provider's filing from the Database, for the following reasons:

- *deficient RMD filing* because the information it contains is incomplete or insufficient, but not substantially and materially so (The Commission's rules already specify that filings may be removed when they are deficient after notice and an opportunity to cure, but we intend to recodify this basis in the same section as the other removal causes we establish, and to address notice and cure requirements independently, as discussed below. Additionally, the Commission has explained that a filing may be deficient when, for example, it describes a mitigation program that is unreasonable, or if the Commission determines that the provider knowingly or negligently carries or processes illegal robocalls in contravention of its RMD filing, but we believe this revised deficiency cause, along with the facial deficiency removal cause, will capture the full scope of potential deficiencies.);
- *facially deficient RMD filing* because it lacks required information or certifications or the information it contains is invalid, non-responsive, or illegible (The Commission has previously described facially deficient filings as those where ''the provider has failed to submit even the most basic information required . . . .'' It has specifically stated that a filing is facially deficient where the provider submits a robocall mitigation plan that fails to provide any information about the specific reasonable steps the provider is taking to mitigate illegal robocalls, as required. It also provided a non-

exhaustive list of examples for why a filing would be facially deficient, including instances where the provider only submits: (1) a request for confidentiality with no underlying substantive filing; (2) only non-responsive data or documents (*e.g.,* a screenshot from the Commission's website of a provider's FCC Registration Number data or other document that does not describe robocall mitigation efforts); (3) information that merely states how STIR/SHAKEN generally works, with no specific information about the provider's own robocall mitigation efforts; or (4) a certification that is not in English and lacks a certified English translation. The Commission has also removed filings that lack a robocall mitigation plan or other required information.);

- *materially deficient RMD filing* because it contains information that is substantially and materially incomplete or insufficient, contains material internal inconsistencies, or contains information that is materially inconsistent with information the provider has reported elsewhere or with reliable external sources (*e.g.,* CORES, the Governance Authority, the NANPA);
- *lack of candor,* including submission of false, misleading, or inaccurate information to the Commission, the Governance Authority, the Policy Administrator, any Certification Authority, or any agent or other third party designated by the Commission or acting on behalf of the Commission pursuant to Commission rules or direction, including the NANPA and the industry traceback consortium;
- *annual recertification violations,* including failure to complete the recertification, failure to complete the recertification on time, and failure to pay the required annual recertification fee;
- *accepting calls from a prohibited provider,* including a provider that does not have a filing that appears in the Database, whose filing has been removed from the Database, or that is subject to a mandatory blocking order (The Commission's rules already specify that filings may be removed for this reason, but we intend to recodify this cause in the same section as the other removal causes we establish);
- *traceback violations,* including failure to respond to traceback requests, repeated appearance in tracebacks, or submission of incomplete or inaccurate information in traceback responses;
- *enabling transmission of illegal calls,* including knowingly or negligently initiating, originating, carrying, processing, or terminating illegal calls (The Commission has previously directed that providers must comply with the practices described in their robocall mitigation plans and that such plans will be deemed deficient if the provider knowingly or through negligence originates, carries, or processes unlawful robocall campaigns.);
- *inadequate robocall mitigation* measures, including failure to implement a robocall mitigation program that complies with Commission rules or failure to comply with the robocall mitigation practices described in the provider's robocall mitigation plan;
- *failure to cooperate with a Commission investigation,* including failure to respond to a subpoena, letter of inquiry, cease-and-desist letter, or notice of suspected illegal traffic;
- *impersonation,* including the unauthorized use of another person or entity's identifying information in an RMD filing;
- *STIR/SHAKEN implementation violations,* including failure to implement STIR/SHAKEN in accordance with Commission rules, improper attestations, and unauthorized authentication practices;
- *national security and law enforcement concerns,* including when a provider, or the provider's subsidiary or affiliate, is identified on the Covered List, is identified as having foreign adversary control through the Foreign Adversary Control System, is subject to a Commission action revoking or terminating a license or authorization on national security or law enforcement grounds, is excluded from obtaining a license or authorization on national security or law enforcement grounds, is otherwise subject to a final Commission determination that its continued participation in the U.S. communications ecosystem poses unacceptable risks, and when the provider is owned or controlled by, under common ownership or control with, or acting on behalf of an entity that is subject to any such a determination;
- *final Commission enforcement actions* with accompanying findings of actual wrongdoing related to facilitating illegal calls or spoofing, including a final determination order under § 64.1200(n)(3), a forfeiture order involving illegal calls or spoofing (if the forfeiture is paid or ordered to be paid by a court), revocation of a Commission authorization, or a final order finding that the provider has failed to comply with KYC, KYUP, STIR/SHAKEN, call blocking, traceback, numbering, or robocall mitigation requirements; and
- *repeat violations for reinstated providers,* including when the provider is removed for one basis but, after reinstatement, commits a violation under the same or another basis.

We seek comment on codification of each of these proposed causes for removal or other enforcement action, including whether we should provide additional guidance explaining what actions or omissions fall within each of these causes. For instance, should removal for lack of candor require a showing that the false statement was material, repeated, or made with intent to deceive? Or is negligent submission of materially inaccurate information sufficient where the provider fails to correct the information after notice? Is failure to respond to a single traceback request sufficient for removal or must it be accompanied by other indicia of bad faith? Should the Commission instead establish a threshold, such as repeated failures to respond to tracebacks within a defined period? Should the rule distinguish between late responses, incomplete responses, false responses, and non-responses? Should failure to participate in automated traceback processes constitute a cause for removal or other enforcement action, if we require providers to participate in the automated traceback process? Should the Commission require evidence that the provider knowingly enabled the transmission of illegal calls, or should a ''knew or should have known'' standard apply? In the *Sixth Caller ID Authentication Order,* the Commission declined to adopt one commenter's proposed standard for assessing forfeiture and removal liability for transmitting illegal traffic based on whether the provider ''knew or should have known'' that a call was illegal, concluding that such a standard was not realistic and could lead to significant market disruptions. We seek comment now on whether we should revisit this determination in light of the Commission's efforts in this proceeding to strengthen the foundation of our enforcement efforts and restore trust in the voice ecosystem. Should use of traceback data for identifying providers that enabled the transmission of illegal calls be limited to identifying originating or gateway providers that may be subject to removal? Are there additional causes for removal that we have not considered?

Removal processes. We next propose and seek comment on enhancing and codifying the procedures for removing providers' filings from the Database and on codifying which procedures apply to each cause for removal. To date, the

Commission has used the following procedures for RMD removal:

- *Three-Step Removal Process*—For most filing deficiencies, the Commission uses a three-step process under which: (1) the Bureau or the Enforcement Bureau first notifies the provider that its filing is deficient, explains the nature of the deficiency, and provides an opportunity to cure; (2) if the provider fails to cure, the Enforcement Bureau issues an order finding that a provider's filing is deficient based on the available evidence and directing the provider to, within 14 days, cure the deficiency and notify the Enforcement Bureau that the deficiency has been cured or explain why its filing should not be removed; and (3) if the provider fails to cure or provide a sufficient explanation within the 14-day period, the Enforcement Bureau issues an order removing the filing from the Database.
- *Two-Step Removal Process*—For filings where the Commission has found that the provider has ''willfully'' violated the RMD filing rules, such as by submitting a filing that contains a facially deficient robocall mitigation plan, and therefore an expedited removal process is warranted, the Commission uses a two-step process under which: (1) the Enforcement Bureau issues a notice to the provider explaining the basis for the violation and providing an opportunity for the provider to resolve the violation or explain why there is no violation within 10 days; and (2) if the violation is not resolved or the provider fails to establish that there is no violation within that 10-day period, the Enforcement Bureau issues an order removing the filing from the Database. The Enforcement Bureau recently used this expedited procedure to remove a voice service provider for failure to cooperate with a Commission investigation because the failure to cooperate demonstrated that its filing (which included a commitment to cooperate with Commission investigations) was deficient and the deficiency was willful.

We propose that the Three-Step Removal Process should apply only to deficient RMD filings, as we propose to codify that cause for removal or enforcement above, except that the Enforcement Bureau should have the discretion to use this process for all other causes for removal. We believe that these deficient RMD filings contain deficiencies that are non-willful, non-substantial, non-material, and typically inadvertent, and therefore that the harms associated with filings containing such deficiencies are minimal. Additionally, such deficiencies may involve disputed facts or assertions, and therefore, we also believe that providers should have ample opportunity to explain and resolve these issues. We seek comment on this proposal and assessment. Should we establish a minimum notice and cure period under the first step, and if so, what should that period be? Should the Bureaus have discretion to shorten the notice and cure period under the first and/or second step where the deficiency is readily curable or accompanied by other indicia of non-compliance, or where the provider fails to respond?

We propose that the Two-Step Removal Process should apply to all other causes for removal, as we propose to codify those causes above, unless the Enforcement Bureau determines that the Three-Step Removal Process should apply. We believe each of these causes are serious violations of Commission rules and significant threats to the integrity of the Database and the U.S. voice ecosystem. We also believe each of those causes are, by definition, willful acts or omissions because they are objective and readily verifiable such that a responsible actor would know that its act or omission constitutes a violation, and therefore that expedited removal for these causes under the Two-Step Process is warranted. We also propose to change the 10-day cure/response period under the Two-Step Process to five (5) days to enhance our ability to quickly remove providers that willfully violate our rules. We seek comment on these proposals and analysis. What are the legal and practical implications of this process? Should we establish a threshold number of violations over a defined period for certain causes, such as failing to respond to tracebacks or applying improper STIR/SHAKEN attestations, before the violation is considered willful and subject to the Two-Step Removal process? Is five (5) days sufficient time for an affected provider to cure its filing, respond to the Commission, and/or notify its customers before its filing is removed and downstream providers must cease accepting the provider's voice calls? Should the length of the cure/response period vary by the removal cause, and if so, what periods should apply to which causes?

We also seek comment on whether to adopt a One-Step Removal Process for egregious conduct or circumstances where further pre-removal process would be unnecessary, impracticable, or contrary to the public interest, including circumstances in which public health, interest, or safety require immediate removal. Under such a process, the Enforcement Bureau could issue an order removing a provider's filing from the Database after a certain number of days without a pre-removal cure/response period. The order would describe the cause(s) for removal and would establish notice of the impending removal to the provider, which could seek reconsideration, review, or reinstatement after removal. Would an effective date for any such removal order of five (5) days be sufficient to allow the affected provider time to notify its customers before its filing is removed and downstream providers must cease accepting the provider's voice calls? We further seek comment on the conduct or circumstances under which the One-Step Removal Process should be available. For example, should this process be available where the provider has engaged in repeated or continuing violations under any of the causes for removal or other enforcement action discussed above? Or, should a single violation under certain causes, such as lack of candor, impersonation, or national security and law enforcement concerns, warrant the One-Step Removal Process? What would be the legal and practical implications of a one-step removal process? What safeguards, if any, should apply, and how quickly should a provider be permitted to seek reinstatement after removal?

We also seek comment on whether there are any alternative removal approaches we could use to expedite the removal of bad actor and non-compliant providers' filings. For instance, to the extent the Enforcement Bureau engages in ongoing communications with providers attempting to cure their filings today, should providers have a set number of opportunities—*e.g.,* three strikes—to fully cure their filings before removal? Would such a strict requirement be more reasonable given our proposals to clarify providers' filing obligations? Should such a requirement only apply to material violations?

Suspensions. We seek comment on whether we should establish a process to suspend a provider's filing from the Database when a provider's filing or conduct presents a cause for removal or other enforcement action. We believe a suspension could serve as both a temporary remedy and intermediate step before removal.

We seek specific comment on whether suspensions should apply when a provider fails to complete its annual recertification by the applicable deadline. Should the RMD system automatically suspend any filing that has not been recertified and for which

any required fee has not been paid by the deadline or after any grace period we may adopt, or should suspension occur only after Bureau review and notice to the provider? If the process is automatic, what safeguards should apply to prevent suspension due to system error, payment-processing delays, or circumstances outside the provider's control? Should the Bureau provide advance reminders, a notice of missed deadline, or a short cure period before suspension? Should suspension only occur after repeated failure to complete an annual recertification or pay the associated fee by the applicable deadline, and if so, how many failures should be permitted before suspension occurs? Under what circumstances should suspensions be lifted? For instance, should we allow providers to complete their certifications and pay any fees after the deadline and lift the suspension when they do? If so, should we configure the system to automatically lift the suspension upon recertification and payment, or should the Bureau manually lift the suspension after completion of these steps and Bureau review? Should we block providers from completing their recertifications and paying any fees after the deadline and only allow them to request approval to complete these steps to lift the suspension? Should a filing be removed if the provider fails to complete recertification and pay any required fee within a specified period after suspension—*e.g.,* 14 days or 30 days—and if so, are any additional findings, procedures, or safeguards necessary before imposing any such consequence? Should repeated violations result in automatic removal, and if so, after how many times?

We also seek comment on whether the Bureau or the Enforcement Bureau should be able to suspend a filing while reviewing, investigating, or pursuing enforcement for other causes for removal or enforcement action. Which causes, if any, are appropriate for suspension? For instance, should suspension be permitted where the provider's continued appearance in the Database presents heightened risks to consumers, the integrity of the Database, national security, law enforcement, or the U.S. voice network? Should the Enforcement Bureau be required to initiate a removal after a certain amount of time following a suspension, and if so, how soon after suspension must the removal process begin? Should a suspension remain in place until the provider cures the underlying violation, responds adequately to a Bureau or Enforcement Bureau inquiry, resolves any pending investigation or removal process, or obtains Bureau and Enforcement Bureau approval? Should the Commission establish maximum suspension periods, after which the Bureau or Enforcement Bureau must either lift the suspension, extend it for good cause, or complete a removal process? Should failure to cure, respond, or otherwise resolve the underlying issue within a specified period result in removal under the applicable removal process? Should repeated suspensions for the same or similar conduct be a cause for removal or other enforcement action, or should such conduct warrant automatic removal after a certain number of times, and if so, how many times? Should repeated violations warrant heightened scrutiny, forfeiture, or denial of future reinstatement?

We seek comment on various ways to implement and effectuate suspension. Should a suspended filing remain visible in the Database but be clearly marked as ''suspended,'' ''under review,'' ''past due'' (in the case of filings that missed the recertification deadline), or some other indicator, or should it be removed from public view unless and until the provider cures the basis for suspension? Should suspensions have the same downstream-provider consequences as removals—*i.e.,* downstream providers could not accept voice calls from a suspended provider—or should suspensions instead trigger permissive blocking or enhanced due diligence by downstream providers? Should the effect of suspension vary depending on the basis for suspension, such that missed recertification or fee payment has different downstream consequences than suspension based on other causes for removal or serious misconduct?

We seek comment on legal implications of any such suspension approach. What notice, opportunity to respond or cure, evidentiary showing, or review rights must apply, if any, prior to suspension? For annual recertification, do pre-deadline general or individualized notices or reminders provide sufficient notice? Should the process differ where suspension is used as a temporary protective measure pending further review, where the provider has already received notice of the underlying conduct through another Commission process, or where public health, interest, safety, national security, law enforcement, or consumer-protection concerns require faster action? What appeal or review rights should apply to automatic or Bureau-initiated suspensions?

Annual recertification requirement modifications. We seek comment on whether we should establish a set grace period for providers that fail to complete annual recertifications by the March 1 deadline to avoid immediate cause for suspension or removal. Are there meaningful benefits of providing a grace period that outweigh the downsides? For instance, would this benefit responsible providers with legitimate customers by providing them with an opportunity to complete their recertification and avoid interruption to the service they provide to end users or other customers? What are the potential downsides? Would providers begin treating the grace period as effectively a new deadline? In addition to the annual general notice of the recertification deadline, should the Commission provide direct notice to providers prior to each annual recertification deadline or immediately upon closing of the recertification window when any grace period we may establish has begun? If we adopt a grace period, how long should it be? Should providers that complete recertification during a grace period be deemed fully compliant, or should filing during the grace period be treated as a violation with certain potential enforcement consequences, even if no consequences occur in the first instance? If so, what should those potential consequences be? We also seek comment on whether any grace period should be available only for first-time or inadvertent failures, and whether repeated late recertifications should result in heightened scrutiny, forfeiture, removal, denial of reinstatement, or other consequences.

We seek comment on whether an annual recertification in the RMD should have a one-year term that expires on March 1 of the following year (or after any grace period, if we adopt one), and therefore that providers would need to perform the annual recertification prior to the deadline for their filing to appear in the Database for the following year. We envision that this would differ from a suspension for failing to complete the annual recertification, which we seek comment on above, because it would not be a response to a filer failing to recertify but would instead be a pre-established term that applies to all new filings. This requirement would effectively place the onus on providers to take action to have their filings remain in the RMD rather than placing the onus on the Commission to take action to remove providers' filings from the RMD. As such, we think such a requirement would enhance providers awareness of

their RMD obligations and increase the integrity of the Database while conserving Commission resources. We seek comment on the benefits and drawbacks of any such requirement.

We propose to codify the requirement that providers must submit the $100 annual recertification fee at the time they complete their recertification. When the Commission established the annual recertification fee requirement in the *RMD Order,* 91 FR 343 (Jan. 6, 2026), it provided that the filing and the applicable filing fee would be submitted at the same time, but it did not codify that timing requirement in the rules. We note that the fee requirement has not yet gone into effect. The Commission will publish a notice in the **Federal Register** announcing when it has completed these steps and when the application fee requirement will become effective. For consistency with the requirement established in the *RMD Order* and administrative convenience, the Database will be configured such that providers will not be able to complete their annual recertification until they have paid the annual recertification fee. To the extent applicable, appropriate procedures will be adopted for exemptions to our fee requirements. Accordingly, if we implement a grace period for the annual recertification, any providers that use the grace period will also pay the fee at the time they file the annual recertification. We believe codifying the timing requirement in our rules will provide greater clarity to providers on the fee requirement. We seek comment on this proposal and assessment. Should we establish any additional rules related to the fee requirement that differ from the Commission's general procedural rules applicable to fees? The RMD recertification fee will be listed in § 1.1105, 47 CFR 1.1105, *Schedule of charges for applications and other filings for the wireline competition services.* Given how the Database will be configured, should we clarify that certain other rules are moot or otherwise inapplicable? In light of how the Database will be configured, should we clarify the recertification fee is late for purposes of the late payment penalty only for those who file after the grace period has expired? Section 159a(c)(1) requires the Commission to impose a late payment penalty of 25 percent of unpaid fees to be assessed on the first day following the deadline for payment of the fees. Section 159a(c)(2) requires the Commission to assess interest at the rate set forth in 31 U.S.C. 3717 on all unpaid fees, including the 25 percent penalty, until the debt is paid in full.

Filing status indicators and call acceptance requirements. We seek comment on whether, instead of hiding removed or suspended filings from view in the public database, they should remain viewable in the public database and we should establish new filing status indicators. Would appropriate indicators be ''removed,'' ''suspended,'' and ''published'' or ''active''? Would maintaining public viewing of removed and suspended filings better enable downstream providers to identify providers from which they are no longer permitted to accept voice calls and otherwise support their KYUP efforts? How should we modify our rule in § 64.6305(g) that directs providers to only accept voice calls from upstream providers that appear in the Database and have not been removed to account for all filings appearing in the database with such indicators? Rather than, or in addition to, including filing status indicators in the Database itself, should the Commission maintain and publish a separate and regularly updated list of all the names of providers whose filings have been removed and/or suspended from the RMD?

Mandatory customer notice. We propose to require providers that are subject to a removal order, suspension (if adopted), or mandatory blocking order to provide notice to their customers. Such notice may reduce consumer disruption by informing lawful customers that their service may be affected and by allowing them to migrate to another provider. We note that, under our existing rules, downstream providers must continue to accept 911 and emergency calls from a provider subject to a removal order. We seek comment on this proposal. Which providers should be required to provide customer notice—only retail providers, or also wholesale providers whose customers may include resellers, call centers, enterprise users, or other service providers? What information should the notice contain, and when should it be sent? Specifically, we seek comment on how the timing of this notice should be sequenced relative to the deadline for downstream providers to comply with any removal or mandatory blocking order so that customers are given sufficient time to find a new provider before their service is interrupted. Below, we propose to specify how quickly providers must stop accepting calls from removed providers. Should compliance with any removal, suspensions, or mandatory blocking order be delayed for some period of time to allow customers time to enter into new service agreements? Additionally, Section 214(a) of the Act provides that a carrier may not discontinue, reduce, or impair a telecommunications service without Commission authorization. Unless otherwise noted, we use the term ''discontinue'' or ''discontinuance'' as a shorthand for the statutory language ''discontinue, reduce, or impair.'' Does RMD removal implicate providers' obligation under Section 214(a) of the Act and our rules to seek Commission authorization before discontinuing, reducing, or impairing service to a community or part of a community? If so, how, if at all, should we revise our RMD rules or discontinuance rules to account for RMD removals? Should the provider be required to certify to the Commission that it has provided the RMD removal notice? Should we require providers seeking reinstatement to submit proof that they provided the RMD removal notice and/or the notice required by our discontinuance rules as a condition of reinstatement? Should the Commission specify a form of notice, such as email, customer portal notice, bill message, direct mail, or contractual notice, or delegate such implementation details to the Bureau? If RMD removal implicates Section 214(a) and our discontinuance rules, should the proposed RMD removal notice be included in the customer notice required by our discontinuance rules, or should it be separate? Are there alternative approaches we should consider for notifying customers that their provider's calls will no longer be accepted by downstream providers?

We further seek comment on whether downstream providers may or should provide direct notice to customers of an upstream provider whose calls will be blocked because of a removal or mandatory blocking order. Downstream providers may have visibility into traffic patterns or customer relationships that could help identify affected entities or individuals. However, such notice may implicate customer proprietary network information and other confidentiality obligations under Section 222 of the Act and the Commission's rules. We seek comment on how Section 222 applies in this context. Would customer notice be permissible either with customer consent, pursuant to an exception for protecting users or the provider's rights and property, or under another legal basis? Should the Commission adopt a rule expressly permitting limited use or disclosure of customer information for the purpose of providing notice required by a Commission removal or blocking order? If so, what safeguards should apply?

4. Keeping Removed Bad Actor Providers Out

We next propose and seek comment on measures to prevent bad actor providers, and the individuals and entities behind them, from reentering the Database after removal. As discussed above, removal from the Database is a significant remedy designed to protect consumers and the voice network from bad actor providers, including those that fail to comply with the Commission's robocall mitigation, caller ID authentication, traceback, and Database filing requirements. But removal may be less effective if the same individuals, related entities, or alter egos can quickly resume participation in the voice ecosystem by filing in the Database under a new business name, affiliate, successor, or other vehicle. We propose and seek comment on measures to address these tactics. We also seek general comment here on whether the processes we discuss are sufficient to prevent bad actor providers from repeatedly ''reinventing'' themselves to evade the consequences of removal, or whether additional tools are needed.

Identifying and acting on unauthorized re-filings. We seek comment on mechanisms to determine when a new filing is unauthorized because it is being made by, on behalf of, or for the benefit of a provider whose filing has been removed from the Database, a provider or person prohibited from filing in the Database pursuant to any debarment process we may adopt (as discussed below), or an alter ego, successor, affiliate, or evasion vehicle of such provider or person. Should any factor, such as common ownership or control, create a rebuttable presumption that the new filing is unauthorized? How should the Commission distinguish between evasion and legitimate business transactions, such as a bona fide arm's length acquisition of assets from a removed provider? Should it be incumbent upon filers to communicate such circumstances to the Commission?

We seek comment on the actions we should take when we determine that a new filing is unauthorized, including for example, rejecting or assigning a ''pending review'' status to prevent publication of such filings and/or removal of filings unauthorized re-filings that are published. Should such actions be performed automatically or manually? Although we believe that such actions may help prevent bad actors from quickly reentering the voice ecosystem, to what extent would they present a risk of false positives that delay or prevent publication of filings by legitimate providers that have common vendors, shared office space, or similar names? Are any such characteristics common for legitimate providers? Should automated rejection, suppression, or removal be limited to filings with high-confidence matches, such as identical OCNs, overlapping FRNs (a given FRN may only be associated with a single RMD filing—however, filers are required to list any additional FRNs in their filing, which may overlap with FRNs associated with other RMD filings, including removed filings), principals, or contact information? When a filing is rejected, suppressed, or removed, should or must we provide notice to the filer with an opportunity to demonstrate that the filing was not made by, on behalf of, or for the benefit of a provider whose filing has been removed from the Database? If so, what showing should we require, and should the filing remain unpublished while the Bureaus review that showing? If, after reviewing the filing and any such showing, the Bureaus determine that a filing is unauthorized, should the filing be rejected, suppressed, or removed? What, if any, additional notice and opportunity to cure is required before an unauthorized filing can be rejected, suppressed, or removed?

Reinstatements. We propose to clarify and codify the circumstances and process under which a removed provider may seek reinstatement to the Database. We propose to require that a removed provider seeking reinstatement must submit a written request to the Enforcement Bureau, demonstrate that it has cured all violations, pay any outstanding regulatory or filing fees owed to the Commission or forfeitures imposed by a court, update all required RMD and CORES information, demonstrate compliance with traceback obligations, and demonstrate it has implemented a robocall mitigation program that complies with Commission rules. We also propose to codify the existing requirement that a provider whose filing has been removed from the Database is not permitted to refile unless and until both the Bureau and Enforcement Bureau consent. Consistent with the publication rule proposed above, even where the Bureaus consent to reinstatement or refiling, the provider's filing would not ''appear'' in the Database for the purposes of § 64.6305(g) unless and until the filing is accepted and published. We further propose to clarify that the Enforcement Bureau, in consultation with the Wireline Bureau, has the discretion to grant, deny, or condition reinstatement based on the provider's cooperation with the Bureau, the provider's showing, the provider's compliance history, and the Enforcement Bureau's risk assessment regarding whether reinstatement would permit the provider's network or services to be used to transmit illegal calls. Reinstatement might also be contingent on the provider agreeing to a consent decree with the Enforcement Bureau. Consistent with current practices, these procedures would create no expectation that a provider whose filing has been removed will be reinstated. We seek comment on these proposals.

Bar on RMD participation. We seek comment on whether to establish an RMD-specific debarment, limited denial of participation, bar on participation, or similar process to prevent bad actor providers and associated natural persons from participating in the Database for a defined period or, in appropriate cases, permanently. For purposes of this inquiry, we use ''participation'' to include filing in the Database, maintaining a filing in the Database, seeking reinstatement after removal, owning or controlling a provider with a filing in the Database, managing or operating such a provider, or submitting a filing on behalf of such a provider. We address below whether RMD misconduct should have broader consequences for other Commission authorizations, licenses, certifications, or applications—here, we focus on whether and how the Commission should limit participation in the Database itself.

In the recent *Suspension and Debarment Order,* 91 FR 18134 (April 9, 2026), the Commission adopted a Limited Denial of Participation (LDP) framework as an FCC-specific alternative to governmentwide suspension and debarment, explaining that an LDP may offer a more flexible remedy for misconduct that warrants limiting participation in FCC programs but may not warrant full suspension or debarment from all government programs. The Commission also adopted rules allowing the LDP to be limited to particular FCC programs, to be extended to other Commission programs depending on the facts and circumstances, to include notice and an opportunity to be heard, and to last initially for up to 12 months, with a possible six-month extension. We seek comment on whether we should establish an RMD-specific framework, modeled off the LDP framework, to address bad actor providers, including those whose filings have been removed from the Database and natural persons

or related entities associated with such providers. As an alternative, should we instead amend the recently adopted LDP rules so that the causes for removal or other enforcement action discussed above may also serve as bases for an LDP, either limited to RMD participation or, where warranted, extended to other Commission programs under the standards and procedures applicable to LDPs?

In particular, we seek comment on whether there should be a process to bar participation by barring from reinstatement a provider whose filing has been removed from the Database for a defined period of time or permanently where the provider was removed for serious or repeated misconduct. We believe that time-limited or permanent bars on RMD reinstatement may be appropriate where the cause for removal was lack of candor, failure to respond to traceback requests or other traceback violations, impersonation, national security or law enforcement concerns, final Commission enforcement actions, or repeat violations by providers that were previously reinstated. We seek comment on this view. Should the Commission codify these or other causes as warranting time-limited or permanent bars on RMD reinstatement? Should the Commission establish a specific period of time for time-limited bars and if so, what duration would be appropriate—one year, three years, five years, or another period? Should different periods apply depending on the nature and severity of the misconduct? Should any particular misconduct warrant a permanent bar, or should permanent bars be reserved for egregious or repeated misconduct after notice and an opportunity to respond?

We also seek comment on the entities and individuals to which an RMD participation bar should apply. Should any RMD-specific debarment, LDP, time-limited or permanent bar on RMD participation, or similar remedy apply only to the removed provider, or also to related entities and natural persons associated with that provider? For example, should the Commission establish a process under which owners, officers, directors, board members, managers, key employees, persons responsible for regulatory compliance, or other associated natural persons may be barred for a period of time or permanently from owning, controlling, managing, operating, or submitting a filing on behalf of a provider that is required to submit a filing in the Database? Should any such rule apply to regulatory consultants, third-party filing agents, or other persons who knowingly submit false, misleading, or inaccurate Database filings on behalf of multiple providers? Should a time-limited or permanent bar on participation extend to affiliates, successors, alter egos, or entities under common ownership or control with the removed provider?

We seek comment on the procedures and safeguards that should apply before the Commission imposes an RMD-specific debarment, LDP, time-limited or permanent bar on RMD participation, or similar remedy. Because any such remedy could limit a provider's or natural person's ability to participate in the Database, we seek comment on what process is required before imposing such a remedy for misconduct. What standard of proof should apply? What notice and opportunity to respond should be required? Should such a bar apply automatically upon removal of a provider's filing from the Database, or only after a separate finding that the natural person participated in, directed, knew of, or should have known of the conduct that led to removal? If there exist substantial and material questions of fact regarding whether a provider, related entity, or associated natural person should be barred from RMD participation, should the matter be designated for an evidentiary hearing before the Administrative Law Judge or the Commission? Evidentiary hearings may be conducted by the Administrative Law Judge, by one or more commissioners, or by the Commission, which may appoint a case manager. The Administrative Law Judge may be tasked with finding facts only or with rendering an Initial Decision on the merits, which may be appealed to the Commission. When the Commission hears the matter itself utilizing a case manager, the case manager oversees the daily progress of the case, but the Commission renders the decision on the merits. Evidentiary hearings allow for discovery, including production of documents, taking of depositions and live testimony, subpoenaing of witnesses and documents, and requiring personal appearances by natural persons associated with the provider and by other witnesses. Section 309(e) of the Act, 47 U.S.C. 309(e), provides a model. It requires that when a broadcast application presents a substantial and material question of fact, or when the Commission (or the Media Bureau on delegated authority) is unable to determine upon the record before it whether the application should be granted, that application is to be designated for an evidentiary hearing. Should a hearing before the Administrative Law Judge be available as part of the appeals process for denial of reinstatement or imposition of a time-limited or permanent bar by the Bureaus? The Commission previously has utilized the Administrative Law Judge in the appeals process. To facilitate the upper C-band transition, the Commission established a procedure by which a satellite operator could seek Media Bureau review of the cost clearinghouse's determination of the operator's reimbursable costs. The operator then could seek *de novo* review of the Media Bureau's order. The *de novo* review was effected through an evidentiary hearing before the Administrative Law Judge. This option for *de novo* review, however, did not alter the pre-existing option for the Media Bureau to designate the matter for hearing before the Administrative Law Judge rather than decide the matter based upon the record available to it. The decision of the Administrative Law Judge, whether made after designation for hearing by the Media Bureau or after the operator sought *de novo* review, then could be appealed to the Commission. What appeal rights should apply, and should such appeals be resolved by the Bureaus, the Commission, the Administrative Law Judge, or some combination? Should there be additional procedural safeguards or enhanced processes for permanent bars compared to time-limited bars?

Finally, we seek comment on conditions and collateral requirements that should apply when a provider, related entity, or associated natural person that was barred from participating in the Database is permitted to participate again, such as at the expiration of a time-limited bar. Should the Commission require a compliance plan, independent audit, officer certification, probationary period, periodic reporting, or other conditions as part of any renewed participation? Should such providers be subject to heightened scrutiny or more frequent recertification for a defined period? Should barred individuals or entities be listed publicly, or would publication raise privacy, due process, or law enforcement concerns? Should the Database form require filers to certify that no barred individual or entity owns, controls, manages, operates, or submits filings on behalf of the provider? Would such a certification help prevent bad actors from reentering the Database through new entities, affiliates, successors, or third-party filing agents, or would it impose undue burdens on legitimate providers?

Effect of removal on other Commission business. We further seek comment on whether misconduct in

connection with the RMD should affect a provider's or person's ability to conduct other business with the FCC for a period of time. As a starting point, to what extent are attorneys who submit RMD filings for an entity that is subsequently subject to an RMD enforcement action susceptible to potential censure, suspension, or disbarment from practice before the Commission under § 1.24(a) of the Commission's rules? If remedies under § 1.24(a) already would apply to such attorneys, should the same or similar remedies apply to others who engaged in misconduct in connection with the RMD?

Beyond that, many providers listed in the Database may hold other Commission authorizations, licenses, or certifications, such as domestic and international Section 214 authorizations, authorization for direct access to numbering resources, eligible telecommunications carrier designations, or spectrum licenses. In the *Sixth Caller ID Authentication Order,* the Commission adopted rules permitting revocation of Section 214 authority and other Commission authorizations, licenses, or certifications for continued violations of the robocall mitigation rules, and stated that it would consider, in future application proceedings, whether it is in the public interest for individual company owners, directors, officers, and principals associated with entities subject to revocation to obtain new Commission authorizations, licenses, or certifications. The Commission declined at that time to adopt a broader proposal to ban principals (either individuals or entities) associated with entities subject to any such revocations from serving, either directly or indirectly, as an attributable principal, officer, or director of entities that hold or apply for any FCC license or authorization for the provision of a Title II-regulated service or other voice service, citing the limited record, the complexity of identifying affected providers and applicants, and the risk of harm to providers and customers associated with the targeted principal but not involved in the robocall misconduct, but the Commission stated that it would consider whether to adopt such rules if repeat offenses increased.

Our experience administering the Database and enforcing its requirements has demonstrated an increased risk that bad actor providers, principals, affiliates, successors, or alter egos may evade removal by reentering the voice ecosystem through new filings by related entities. Above, we seek comment on whether to establish an RMD-specific debarment, limited denial of participation, participation bar, or similar process to limit participation in the Database itself. We now seek tailored comment on whether the same types of misconduct that could warrant an RMD participation bar—such as RMD removal, repeated submission of deficient or false RMD filings, evasion through alter egos, repeated failure to respond to traceback requests, or repeated transmission of illegal calls—should also have broader consequences for the provider's or principal's Commission authorizations, licenses, certification, or applications. We note that, in the *Robocall Numbering Policies NPRM,* we sought comment on whether providers' access to numbering resources should be affected when there is indicia of fraud or misuse of numbering resources, such as a high number of tracebacks over a defined period or receipt of a ''Notification of Suspected Illegal Traffic.'' Specifically, should such conduct serve as grounds to initiate proceedings to revoke, suspend, condition, designate for hearing, or otherwise review Commission authorizations, licenses, or certifications held by the provider or principal? Should such conduct affect future applications to the Commission for authorizations, licenses, or certifications by the provider or by principals, affiliates, successors, alter egos, or entities under common ownership or control? If so, should those consequences apply automatically for a defined period, only after a separate Commission finding, or only after application-specific review under the rules and procedures governing the relevant authorization, license, certification, and application? Should we adopt a process to bar, for a period of time or permanently, principals of entities that engage in such misconduct from owning, controlling, managing, or operating, either directly or indirectly, an entity that holds or is applying for an FCC authorization, license, or certification? What additional findings, procedures, and safeguards would be necessary before imposing any such consequences? We note that there might already be procedural requirements governing revocation of certain types of Commission authorizations. For example, Section 312(c) of the Act requires an evidentiary hearing before a broadcast license may be revoked. Potential bases for revoking a broadcast license may arise in relation to the RMD as a result of, for instance, violations of the RMD rules, false or misleading statements in an RMD submission, or abusing the RMD process. Section 73.4280 of the Commission's rules incorporates these character policy statements by reference and thereby makes them part of the Commission's rules. Are there situations in which it would be necessary or appropriate to conduct an evidentiary hearing before the Administrative Law Judge or the Commission, such as when material questions of fact exist or when required by statute or rule governing the relevant authorization, license, or certification? Should the Commission adopt narrower RMD-specific consequences that only affect voice service-related authorizations, licenses, or certifications?

Prohibition on Accepting Voice Calls from Unlisted Providers. We propose to amend § 64.6305(g) to provide greater clarity and specificity regarding downstream providers' obligation to only accept voice calls from providers that appear in the Database, and seek comment on how to do so. Section 64.6305(g) requires intermediate providers and voice service providers to accept voice calls sent directly from domestic or foreign voice service providers and intermediate providers only if the upstream provider's filing appears in the Database and has not been removed. Notwithstanding this requirement, ''(i) [a] provider may not block a voice call under any circumstances if the call is an emergency call placed to 911; and (ii) [a] provider must make all reasonable efforts to ensure that it does not block any calls from public safety answering points and government emergency numbers.'' As an initial matter, should we amend our rules to affirmatively prohibit providers from accepting voice calls from a provider that is not published in the Database, rather than the current wording that requires providers to only accept calls from a provider whose filing appears in the Database and has not been removed? If we adopt our proposal that providers have a temporary exemption while they seek to obtain an SPC token, should we specify that providers are not permitted to accept calls from upstream providers unless they appear in the Database and have obtained an SPC token?

We propose to specify the minimum frequency with which providers must check the Database to ensure compliance with this obligation and seek comment on that frequency. Should providers be required to check the Database before entering into a new interconnection, service, or traffic-exchange arrangement; at regular intervals; and/or upon notice from the Commission that a provider has been removed? Should the Commission

establish a minimum frequency, such as daily, weekly, monthly, or before accepting calls from any upstream provider? Should the obligation vary based on a provider's size, role in the call path, traffic volume, or risk profile? What costs would providers, particularly small and rural providers, face in complying with such procedures? If the Commission were to adopt any such procedures, how long would providers need to implement any changes to their networks or operations to comply with new rules? We also seek comment on providers' current practices for complying with their obligations under § 64.6305(g), including whether they rely on the Database's API, downloadable .CSV file, or another data source, and whether they employ any technical validation tools or rely on manual checks.

We propose to specify how quickly downstream providers must stop accepting calls after a provider's filing is removed from the Database and seek comment on when this should occur. In the *Sixth Caller ID Authentication Report and Order,* the Commission concluded that the existing Enforcement Bureau process, whereby providers are given two business days to block calls following Commission notice of removal from the Database, is sufficient, as it appropriately balances the public's interest in blocking unwanted robocalls against the need to allow providers sufficient time to take the necessary steps to block calls. However, since that *Order* was adopted, the Enforcement Bureau has issued orders removing substantial numbers of filings from the Database, including two orders in August 2025 that removed 1,203 and 185 filings, respectively. In light of this substantial uptick in enforcement, we now seek further comment on whether the current two-day compliance timeline is reasonable, and on the burdens and costs to providers in complying, and on the impact on customers of the deficient filer. Should we establish a default or minimum timeline that would apply to compliance with § 64.6305(g) with respect to removal orders generally, but delegate to the Enforcement Bureau the discretion to establish a longer compliance timeline in a particular removal order, such as based on the number of filings being removed? Should a default minimum timeline require downstream providers to cease accepting calls immediately upon release of the removal order, within the current two business days, or some other length of time? Should the Enforcement Bureau consider other factors for extending the compliance timeline, and if so, what factors? What operational steps must downstream providers take to stop accepting calls, and how much time is reasonably necessary? How should we balance the need to protect consumers from illegal calls against the risk of disrupting lawful calls?

We also seek comment on harmonizing the Database removal process with the Commission's call blocking rules. Under § 64.1200(n), a provider that receives a Notification of Suspected Illegal Traffic from the Enforcement Bureau must, within a minimum of 14 days, investigate the identified traffic, report the results of its investigation within the timeframe specified in the notice, and, if its investigation determines that it served as the gateway or originating provider for the identified traffic, block or cease accepting the identified traffic and substantially similar traffic on an ongoing basis within the timeframe specified in the notice. If the provider fails to respond, provides an insufficient response, continues to originate or transmit substantially similar traffic, or the Enforcement Bureau determines that the traffic is illegal despite the provider's assertions, the Enforcement Bureau may issue an Initial Determination Order and, after a minimum of 14 additional days to respond, a Final Determination Order finding that the provider is not in compliance with § 64.1200(n)(2). Section 64.1200(n)(3), in turn, requires any provider immediately downstream from the upstream provider identified in the Final Determination Order to block all traffic received directly from that upstream provider beginning 30 days after release of the Final Determination Order.

Thus, the Commission's blocking obligations under § 64.1200(n) operate using different processes and timelines than used for § 64.6305(g), described above. We seek comment on whether and how these processes and timelines should be harmonized. Should the Commission align the two-day time period for downstream providers to cease accepting traffic from a provider removed from the Database with the 30-day period that applies to immediately downstream providers after release of a Final Determination Order? Should we instead align the 30-day period with the two-day period, or otherwise set different periods for these timelines before harmonizing them? How much time do voice service providers need to implement mandatory blocking under § 64.1200(n)(3) or cease accepting traffic under § 64.6305(g)? Are the obligations sufficiently distinct that different timeframes remain warranted? Should a mandatory blocking order under § 64.1200(n)(3) automatically trigger the RMD removal process for the provider that received the Final Determination Order as well as for the provider(s) that originated the illegal traffic identified in the order, or should Database removal and mandatory blocking orders remain separate actions? Should the Commission align terminology across the two rules, such as ''refuse traffic,'' ''block traffic,'' ''cease accepting traffic,'' and ''identified and substantially similar traffic'' to reduce confusion about providers' obligations? We also seek comment on whether providers should be permitted to satisfy both rule frameworks through a single compliance process, such as unified investigation, mitigation, blocking, and reporting workflow and how such a process could operate effectively. Would such harmonization reduce burdens on providers and improve enforcement, or would it risk conflating distinct obligations that address different types of provider misconduct? We seek comment on these questions.

We seek comment on how downstream providers can identify whether a provider whose filing has been removed from the Database is the same entity as, or affiliated with, a provider from which they accept calls. Should the Commission include OCNs (when available), FRNs, known business names, prior business names, affiliates, principals, or other identifiers in removal orders to assist downstream providers? Should the Database include a downloadable list of removed providers and associated identifiers? Should downstream providers be entitled to rely on the Database as the authoritative source, or should they also be required to conduct independent due diligence when they have reason to believe an upstream provider is an alter ego of a removed provider? How would such obligations interact with KYUP obligations proposed in the *KYUP FNPRM*?

We propose to clarify that providers' call refusal obligations apply to all voice calls, including calls that originate outside of the United States using non-NANP resources, and not just calls using NANP resources, to ensure bad actors cannot attempt to evade robocall mitigation rules by using non-NANP numbers, invalid numbers, or other caller ID information. The Commission's existing rule requiring providers to accept calls from a foreign voice service provider only if it is listed in the Database refers to calls using NANP resources that pertain to the United

States in the caller ID field. We believe that expanding this requirement to require refusal of all voice calls will better prevent bad actors' evasive tactics. This would not change providers' obligation to not block emergency voice calls placed to 911 and to ''make all reasonable efforts to ensure that it does not block any calls from public safety answering points and government emergency numbers.'' In the *Gateway Order,* 87 FR 42916 (July 18, 2022), the Commission stated that ''[f]oreign-originated robocalls are successful to the extent that end users believe they are calls from U.S. customers or businesses, and we therefore conclude it is appropriate to focus our efforts on such calls.'' However, as we and providers increase efforts to combat illegal calls that use U.S. NANP resources, we are concerned that bad actors may increase the volume of illegal calls using non-U.S. NANP resources and seek to close that loophole here. We seek comment on this proposal, including on the extent to which this changes providers' current practices, on any operational challenges to this requirement, and on any unintended effects for lawful international traffic. Similarly, while our existing rules place a general requirement on originating, terminating, and non-gateway providers to adopt a robocall mitigation program, gateway providers must only adopt a program to address robocalls using U.S. NANP resources in the caller ID field. In the *KYUP FNPRM,* we proposed to modify the robocall mitigation program obligation for gateway providers to require that their programs apply to all calls they carry and process, and not just calls using U.S. NANP resources in the caller ID filed.

We also seek comment on whether providers should be required or permitted to block text traffic from providers that are not listed in or have been removed from the Database. The RMD is designed for voice service provider robocall mitigation obligations, but illegal text messages present related consumer protection concerns, and some providers participate in both the voice and text ecosystems. We believe providers that pose threats to consumers and the integrity of the voice ecosystem are also likely to pose threats to consumers and the integrity of the text ecosystem. We seek comment on this view. What authority would support such action? What technical, operational, and consumer-impact issues would arise?

Finally, we seek comment on whether we should specify additional consequences that should follow from Database removal, such as notification to the Governance Authority for potential SPC token suspension or revocation, notification to the NANPA for potential review of access to numbering resources, notification to other Commission bureaus or offices regarding licenses or authorizations held by the provider, and notice to state and federal law enforcement partners. Should any of these consequences be automatic, or should they require separate review under the rules governing the relevant authorization or credential? We also seek comment on how to coordinate these processes while preserving appropriate procedural protections.

5. Audits

The Commission recently asked if it should consider requiring independent audits of provider compliance with both its KYC rules and KYUP rules. Should the Commission use audits to assess companies' compliance with requirements designed to target illegal calls, including its RMD requirements? If so, should the Commission, either itself or through a third party, conduct random audits of Database filings, targeted audits of high-risk providers, audits of providers seeking reinstatement, or a combination? Should providers be required to retain records supporting their Database filings, robocall mitigation plans, KYC and KYUP practices, STIR/SHAKEN implementation certifications, traceback responses, and customer or upstream-provider due diligence? If so, for how long? Should failure to cooperate with and provide fulsome responses to audits constitute a cause for removal and/or other penalties? We seek comment on the burdens audits would impose, particularly on small providers, and on the benefits of audits in deterring bad actor providers and improving the reliability of the Database. We also seek comment on amending § 52.15(k) of the Commission's rules subjecting telecommunications service providers to ''for cause'' and random audits to ''verify carrier compliance with Commission regulations and applicable industry guidelines relating to numbering administration'' to expand the scope of audits that may be conducted under that rule to include compliance with the Commission's RMD requirements and whether such a change would be necessary. Or, should the Commission consider proposing new audit requirements for purposes of testing provider compliance with all Commission requirements aimed at preventing unlawful calls and robocalls, including the RMD requirements?

6. Resources for Administration

The RMD currently contains over 11,000 filings and continues to grow as new providers enter the voice ecosystem. In addition, existing filings are continuously updated when providers comply with the requirement to update their filings within 10 business days of any change to the information they must provide. Each RMD submission must be processed and reviewed by Commission staff to determine if it complies with the requirements of the Commission's caller ID authentication and robocall mitigation rules, as well as to verify that all existing filers have timely complied with the requirement to recertify their filings annually by March 1. As the Commission has recognized, this compliance review process requires significant staff resources, including analysts to review each filing, attorneys to perform compliance assessments, and a supervisory attorney to oversee the process and coordinate the referral of any non-compliance and fraudulent filings to the Enforcement Bureau. Enforcement actions also require significant staff resources.

The Commission has adopted several measures to support the continued administration and integrity of the Database. Specifically, the Commission established a $100 application processing fee for initial Database filings and annual recertifications and applied the Commission's red-light rule to RMD filings. As noted in the *RMD Order,* filing fees assessed pursuant to our Section 8 authority are deposited in the general fund of the U.S. Treasury and are not available for use by the agency absent an appropriation made by law. We note that the requirement to submit an application fee as required by the amendment to 47 CFR 1.1105 adopted in the *RMD Order,* is not yet effective. The Commission stated in the *RMD Order,* that the rules it adopted would become effective 30 days after publication in the **Federal Register**, except for § 1.1105, ''which requires notice to Congress pursuant to Section 9A(b)(2) of the Communications Act, 47 U.S.C. 159A(b)(2), and also requires certain updates to the FCC's information technology systems and internal procedures . . . .'' The Commission will publish a notice in the **Federal Register** announcing when it has completed these steps and when the application fee requirement will become effective. The Commission has also implemented multi-factor authentication for accessing the Database, has established a dedicated email address that stakeholders can use

to report deficient RMD filings to the Commission, and has released guidance and filer education in the form of a ''Frequently Asked Questions'' document to assist filers with their RMD compliance obligations. At the Commission's direction and pursuant to its delegated authority, Bureau staff coordinates the development, testing, implementation, and maintenance of various technical and administrative aspects of the RMD system and submission portal. Staff also monitors the email inboxes established for general questions, outreach and compliance, and reports of deficient filings, and responds as appropriate to inquiries from users and stakeholders.

The proposals and inquiries in this Further Notice may require additional technical tools, staff review, coordination among Commission bureaus and offices, information-sharing mechanisms, and provider outreach. We seek comment on measures the Commission can implement to effectively administer the RMD, including resources and mechanisms that may support the costs and requirements of such administration. To the extent we determine that changes in procedures proposed herein result in increases or decreases in the cost of processing such that the application fee schedule may require an amendment pursuant to Section 8(c) of the Communications Act, 47 U.S.C. 158(c), the Commission will initiate a rulemaking to seek comment on any proposed amendment(s) to the application fee schedule. In a recent *NPRM,* 91 FR 21761 (Apr. 23, 2026), that aimed to take the profit out of unlawful calls originating from outside of the United States, the Commission sought comment on bond- or fee-based approaches to deter bad actors, and referenced the House version of the Foreign Robocall Elimination Act bill which would require certain providers to post a bond or fee to file in the RMD. Should the Commission adopt a bond-based or similar approach, we seek comment on whether the Commission has statutory authority to retain such monies, and how collected fees or bonds could best be expended on the Commission's robocalls-related administrative functions, including resources for administering the RMD. We also seek comment on whether we have authority to establish or designate an RMD Administrator, either within the FCC or externally, to perform certain administrative functions under Commission oversight, and on the virtues and shortcomings of doing so.

C. Other Considerations

1. Further Streamline and Clarify the RMD Rules

In this section, we propose and seek comment on additional amendments to streamline and clarify the Commission's RMD rules. In the *KYUP FNPRM,* we proposed a comprehensive review of our caller ID authentication rules to remove unnecessary redundancy, ensure consistency, and increase clarity for providers. The proposed changes would already result in significant streamlining of the RMD rules, and as stated above, those proposed streamlined rules were the starting point for our proposed rule revisions here. We propose to further revise our RMD rules without changing providers' existing obligations (except as proposed above) to ensure that § 64.6305 uses consistent terminology, accurately reflects the full scope of the information providers must submit and maintain in the Database, and aligns with related robocall mitigation, KYC, and KYUP obligations in § 64.1200. We also propose the following specific revisions.

First, we propose to revise § 64.6305 to use the term ''filing,'' as in ''Robocall Mitigation Database filing'' or ''Database filing,'' when referring to the full submission a provider must make and maintain in the Database, including its certifications, robocall mitigation information, business identifying information, provider type and service information, and robocall mitigation plan. The current rules often use ''certification'' to refer to the broader Database submission, even though the required filing includes information and documents beyond the provider's certifications. We believe using ''filing'' to refer to the overall submission and ''certification'' only when referring to a specific certification will make the rules easier to understand and administer. We seek comment on this proposal. Would this terminology better reflect how providers interact with the Database? Are there provisions where retaining the term ''certification'' would avoid confusion? Should we instead use ''submission'' or another term?

Second, we propose to amend the terminology in § 64.6305 to refer to ''illegal calls'' rather than only ''illegal robocalls'' or ''illegal robocall traffic.'' Above, we propose to amend the rule obligating providers to implement a mitigation program to require that such programs are designed to mitigate all illegal calls, and not just robocalls. For the detailed reasons we provided there, we believe all our RMD rules should be targeted toward all illegal calls, and therefore propose to change all references to ''robocalls'' to ''calls,'' except when referring to the Robocall Mitigation Database, robocall mitigation program, and robocall mitigation plan, where the word ''robocall'' would take on the colloquial use. Relatedly, we propose to amend the term ''illegal robocall traffic'' to ''illegal calls,'' to align with other rules and proposals that focus on the illegality of each call. Should we define the term ''illegal calls,'' and if so, how?

Third, we propose to codify the existing requirement that providers with a STIR/SHAKEN implementation obligation are prohibited from certifying to complete or partial implementation in the RMD unless they have obtained an SPC token and digital certificate and sign calls with their certificate, either themselves or when working with a third party to perform the technological act of signing calls. The Commission established this prohibition in the *Eighth Caller ID Authentication Order,* but it did not codify the requirement in § 64.6305. We believe that codifying this requirement is necessary to clarify and ensure compliance with providers' filing obligations.

Finally, we seek comment on any additional conforming, clarifying, or streamlining amendments to § 64.6305 that would improve readability and administrability without altering providers' substantive obligations, except as otherwise proposed in above.

2. Effective Date

We propose that the proposed rules become effective as follows:

- The proposed rules in Section III.A.1 would become effective the later of 6 months after **Federal Register** publication of a Report and Order adopting the rules or 30 days after publication in the **Federal Register** of notice of approval by the Office of Management and Budget (OMB) for rules that contain new or modified information collections subject to review under the Paperwork Reduction Act (PRA);
- The proposed rules in Sections III.A.2 and III.A.3 would become effective under the following conditions: (1) a Report and Order adopting the rules is published in the **Federal Register***;* (2) publication in the **Federal Register** of notice of approval by OMB of rules that contain new or modified information collections subject to review under the PRA; (3) the FCC's information technology systems and internal procedures have been updated to implement the rules; and (4) the Bureau publishes notice(s) in the **Federal Register** announcing that providers must comply with the rules

when completing the next annual recertification; and

- The proposed rules in Sections III.B and III.C would become effective the later of 30 days after **Federal Register** publication of a Report and Order adopting the rules or 30 days after publication in the **Federal Register** of notice of approval by OMB for rules that contain new or modified information collections subject to review under the PRA.

We seek comment on these proposals.

D. Legal Authority

We propose to adopt the foregoing proposals pursuant to the same sources of authority we have relied upon in our previous RMD, caller ID authentication, and call blocking orders. Specifically, we propose to rely on Sections 201(b) and 202(a), which provide the Commission broad authority to adopt rules governing the just and reasonable practices of common carriers, as the basis for our proposed requirements with respect to common carriers. We believe that Section 251(e)(1) of the Act, which grants us ''exclusive jurisdiction over those portions of the North American Numbering Plan that pertain to the United States,'' also provides us with authority to adopt additional RMD requirements to prevent the fraudulent abuse of NANP resources. The Commission has found that our Section 251(e) authority provided the basis for permissive blocking of invalid, unallocated, or unused numbers to protect users from spoofing. Similarly, the Commission has found that ''the Truth in Caller ID Act grants us authority to prescribe rules to make unlawful the spoofing of caller ID information with the intent to defraud, cause harm, or wrongfully obtain something of value.'' Section 251(e) and the Truth in Caller ID Act, taken together, grant us authority to prescribe rules to prevent the unlawful spoofing of caller ID and abuse of NANP resources by all voice service providers, and the proposed RMD requirements would take a further positive step toward stopping such illegal calling. In addition, the Commission has relied on Section 251(e) and the Truth in Caller ID Act to prohibit certain providers from accepting traffic from entities that are not listed in the RMD. The TRACED Act's authentication framework provisions also grant us authority over non-IP networks, including to require robocall mitigation programs. The Commission has also relied on Section 4 of the TRACED Act in adopting robocall mitigation duties for voice services providers, and we intend to also rely on that authority. We also believe that our proposed RMD mitigation and certification requirements will help protect consumers from unwanted calls and invite comment on our authority under Section 7 of the TRACED Act, which directed the Commission to ''initiate a rule-making to help protect a subscriber from receiving unwanted calls or text messages from a caller using an unauthenticated number.'' We seek comment on these proposals and on additional sources of legal authority for any new or amended rules discussed above.

We propose to rely on Sections 201(b) and 202(a), the Truth in Caller ID Act, and the TRACED Act for ensuring that our proposed robocall mitigation rules apply to all illegal calls, including calls originating outside of the United States using non-NANP resources, and not just calls using NANP resources. Sections 201(b) and 202(a) apply to all common carriers and are not limited to calls using NANP resources. We believe the Truth in Caller ID Act would apply to any calls that involve misleading or inaccurate caller identification information, and not just such caller identification information using NANP resources because the statute, as amended, applies not just to ''any person within the United States'' but also to ''any person outside the United States if the recipient is within the United States.'' We seek comment on this proposal. We also seek comment on whether Section 4 of the TRACED Act may provide authority to impose requirements on providers to address all illegal calls. In particular, we seek comment on whether the definition of ''voice service'' in the TRACED Act, which specifies that it is a service that uses NANP resources, is jurisdictional, limiting the providers to which we may apply requirements to only those that provide services using NANP resources but not limiting the requirements we may impose to only calls that use NANP resources in the caller ID field.

Ancillary authority. We propose to rely on our ancillary authority under Section 4(i) of the Act to the extent necessary to support our RMD-related proposals, particularly as they apply to voice service providers that have not been classified as common carriers. Although we believe our direct statutory authorities provide substantial support of the rules we propose, we have, in prior rulemakings addressing illegal calls, also relied on Section 4(i) as an independent basis for adopting requirements applicable to all voice service providers. We seek comment on this approach. The Commission has previously relied on Section 4(i) to extend KYC, KYUP, call-blocking, and mitigation related obligations to non-common-carrier providers, explaining that applying these requirements uniformly is essential to the effectiveness of our robocall mitigation framework. We likewise believe that the RMD-related obligations proposed here are ''reasonably ancillary to the Commission's effective performance of its . . . responsibilities.'' The Commission may exercise ancillary authority when two conditions are met: (1) the subject of regulation falls with the Commission's general jurisdictional grant under Title I, and (2) the regulations are reasonably ancillary to the Commission's statutorily mandated responsibilities. We tentatively conclude that the first prong is satisfied because voice service providers are interconnected with the public switched telephone network, and the exchange of IP-based voice traffic constitutes ''communication by wire or radio'' under Section 2(a) of the Act.

We further believe that the proposed RMD requirements are reasonably ancillary to the effective performance of our statutory responsibilities under Sections 201(b), 202(a), 251(e), the Truth in Caller ID Act, and the TRACED Act. More specifically, we believe the proposed requirements are reasonably ancillary to our exercise of authority under Sections 201(b) and 202(a), as we do not believe we could ensure that voice service providers that are classified as common carriers comply with obligations to address illegal calls if the same rules do not apply to voice service providers that are not classified as common carriers, and the inability of common carriers to comply with obligations could create a gap that bad actor providers could exploit to undermine the effectiveness of illegal-call mitigation and impede our ability to carry out our statutory responsibilities. Additionally, we believe the proposals are reasonably ancillary to our authority in Section 251(e) and the Truth in Caller ID Act to adopt rules to prevent the unlawful spoofing of caller ID and abuse of NANP resources by all voice service providers, and our authority in the TRACED Act to ensure mitigation to prevent unlawful robocalls. We also believe our proposal to apply robocall mitigation requirements is reasonably ancillary to the authority in these provisions to prevent the transmission of illegal calls. We seek comment on this analysis and on the extent to which Section 4(i) provides additional or independent support for our proposed RMD requirements.

Indirect effect on foreign voice service providers. We propose to conclude that

any effect our proposed rules may have on foreign voice service providers would be indirect and therefore consistent with the scope of the Commission's authority. In the *Second Caller ID Authentication Order,* the Commission recognized that its rules would ''have an indirect effect on foreign voice service providers by incentivizing them to certify to be listed in the database,'' but found such effects permissible under longstanding Commission and court precedent. This precedent includes the Commission's authority under Section 201 to require a domestic carrier to modify its contractual arrangements with a foreign provider concerning ''foreign communication'' to ensure that related charges and practices remain ''just and reasonable.'' Consistent with this approach, we tentatively conclude that the rules proposed here do not assert or entail any direct exercise of jurisdiction over foreign providers. We seek comment on this tentative conclusion and on whether any of our proposals may extend beyond the limits of our authority over foreign communications entering the United States. We also seek comment on whether any proposed rule would conflict with U.S. treaty obligations or with other applicable international laws or norms, or would create the risk of retaliatory measures by foreign governments.

E. Cost-Benefit Analysis

Robocalls and related scams result in substantial harms to consumers, and the proposed rule revisions are intended to help reduce the volume of illegal robocalls reaching U.S. consumers. We believe these proposals may yield substantial benefits, including improved transparency, enhanced data accuracy, and more reliable compliance information from providers. At the same time, we recognize that the proposals may impose incremental costs on RMD filers, such as expanded information-submission requirements and strengthened accountability obligations. We seek comment on how to quantify the expected reduction in illegal robocalls and the associated benefits, including the degree to which improved data quality, enhanced screening of bad actor providers, and more effective mitigation program requirements may contribute to observable reductions in illegal call activity. We also seek comment on appropriate methods to isolate the effects of these proposed rule changes from other recent efforts to combat illegal calls.

We believe our proposals to strengthen RMD filing obligations will improve predictability and administrative efficiency for providers and Commission staff alike. Clearer obligations regarding which entities must file, what information must be submitted, and how such information should be organized may reduce confusion and enhance the quality of RMD filings. To the extent codifications and clarifications ease providers' ability to comply with our requirements, we seek comment on the anticipated time and cost savings. We also seek comment on the costs associated with any new or expanded filing requirements. For instance, the proposed rules would codify the existing requirement that parents, affiliates, and subsidiary companies must submit separate RMD filings when they independently meet the definition of voice service provider, and we seek comment on how many entities will be newly aware of their obligation to file and on the associated incremental costs. Our preliminary view is that good-faith providers should already maintain much of the newly required information in the normal course of business and therefore would not require significantly more time to submit this information to the RMD. We seek comment on the accuracy of these assumptions and on the incremental costs providers may incur in preparing and submitting the expanded RMD filings.

We believe our proposals to strengthen our ability to identify, deter, and remove non-compliant or bad actor providers are likely to generate significant benefits by improving the integrity of the RMD and reducing opportunities for illegal calls to reach consumers. Enhanced information sharing, improved traceback responsiveness, clearer removal and reinstatement procedures, and stronger safeguards against evasion may increase the efficiency of enforcement and further deter unlawful activity. We also acknowledge that these proposals may impose new obligations on some providers, including increased responsiveness to inquiries, additional documentation obligations, and the potential for more frequent compliance reviews. The proposed rules would also codify, clarify, or expand our processes for removing non-compliant and fraudulent filings from the RMD and the conditions under which a provider may refile in the RMD. We seek comment on the expected costs associated with these new obligations, on the benefits of any streamlined removal or reinstatement procedures, and on the burdens such processes may impose on affected filers. We further seek comment on the expected benefits of strengthening providers' traceback commitments and cooperation obligations, including whether faster or more automated traceback could materially improve the identification of bad actors, as well as on how increased information sharing and coordination between the Commission and the Governance Authority may affect providers.

II. Initial Regulatory Flexibility Analysis

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

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

In the *FNPRM,* the Commission proposes additional steps to strengthen the effectiveness of the Robocall Mitigation Database (RMD or Database) as a central tool in our broader efforts to combat illegal robocalls and restore trust in voice communications. The RMD supports provider transparency, accountability, and compliance with robocall mitigation and caller ID authentication obligations, but as its importance has grown, the Commission must ensure its RMD rules and existing functionality stays ahead of bad actors' increasingly sophisticated tactics to gain access to the U.S. voice network.

The *FNPRM* therefore aims to improve the reliability and usefulness of RMD filings and establish clearer and more enforceable obligations for all providers in the call path. Specifically, we seek comment on whether additional clarity is needed regarding which entities must file in the RMD, including which entities meet the broad definition of ''voice service provider.'' We also propose and seek comment on enhancements to the information required in RMD submissions, including certifications and commitments filers must make; information about the STIR/SHAKEN implementation exemptions

prior enforcement actions, and use of third-party vendors as part of the robocall mitigation information providers must supply; the type of business identifying information providers must submit; provider type and other service related information; and the level of detail for robocall mitigation plans. These measures aim to ensure that RMD filings give the Commission and other stakeholders a more complete and accurate picture of provider operations and compliance, thereby supporting compliance review and enforcement functions.

The *FNPRM* also seeks to ensure that only legitimate providers with compliant filings appear in the Database. Specifically, we propose and seek comment on measures to prevent bad actors and deficient filings from entering the Database in the first instance, including clarifying the Bureau's authority to develop and implement technical and operational measures to screen filings, identify indicia of deficient or evasive filings, and prevent such filings from being accepted into the Database. We also propose to codify that a filing does not ''appear'' in the Database for purposes of § 64.6305(g) unless and until it has been accepted and published, and that the Bureau may reject, withhold publication of, or place into pending status filings that appear deficient, evasive, unauthorized, or otherwise subject to a cause for removal, and on the appropriate process for such filings, including notice, opportunity to cure, and timing for Commission action. We also seek comment on whether letters of credit or similar requirements could help deter bad actors from filing in the RMD.

We also propose and seek comment on measures and tools to enhance our ability to identify and remove bad actors that are in the Database. These include proposals to develop enhanced technical screening mechanisms and require domestic voice service providers with RMD filings to submit Foreign Adversary Control attestations and seeking comment on expediting the traceback process and improving information sharing with the STIR/SHAKEN Governance Authority. We propose to adopt new causes for removal and to codify three-step and two-step removal procedures to address deficiencies ranging from incomplete filings to facially deficient filings and other serious causes for removal. We also seek comment on whether additional streamlining, including a potential one-step removal process for egregious conduct or circumstances requiring immediate action, would be appropriate. We seek comment codifying the scope of causes for removal. We also seek comment on establishing a grace period for annual recertifications, on potential suspension mechanisms for providers that fail to complete an annual recertification or pay required fees or that otherwise present serious compliance concerns, and on whether and how to use filing status indicators. Additionally, we propose to require providers that are subject to a removal order, suspension, or mandatory blocking order to provide notice to their customers.

We further seek comment on measures to keep removed bad actor providers out of the Database and to clarify the obligations of providers that rely on the Database. We seek comment on criteria for determining when a filing is unauthorized or made on behalf of a removed or prohibited provider and whether similar filings should be held for review or automatically removed, as well as proposing procedures and standards for reinstatement. We seek comment on whether to establish an RMD-specific debarment-style framework or apply participation bars to removed providers and natural persons associated with removed providers. We also ask whether misconduct related to RMD filings should affect a provider's ability to obtain or maintain other Commission authorizations, licenses, and certifications and how to ensure appropriate due process protections. We seek comment on downstream provider obligations, including how often providers should check the RMD, how quickly providers must cease accepting traffic from providers whose filings do not appear or are removed from the Database, how providers can identify alter egos or affiliates of removed providers, whether and how to harmonize Database-related refusal obligations with call blocking obligations under § 64.1200(n), and whether RMD-based refusal or blocking obligations should apply to all voice traffic, including calls using non-U.S. NANP resources. We seek comment on whether providers should be required or permitted to block text traffic from providers that are not listed in or have been removed from the Database, and on whether additional consequences should follow from Database removal, such as notice to the Governance Authority, the NANPA, other Commission bureaus or offices, or state and federal law enforcement partners.

We seek comment on administrative and operational considerations for filers and entities that rely on the accuracy of RMD filings, including on whether certain RMD information should remain non-public, whether recertification or update intervals should be adjusted, and whether audits should be used to verify compliance. Finally, we request comment on what resources and system improvements may be necessary to support expanded screening and enforcement functions, propose additional conforming and clarifying rule changes, and seek comment on the effective date for rules adopted in this proceeding.

B. Legal Basis

The proposed action is authorized pursuant to sections 4(i), 4(j), 201, 202, 217, 227, 227b, 251(e), 303(r), 403, 501, 502, and 503 of the Communications Act of 1934, as amended, 47 U.S.C. 154(i), 154(j), 201, 202, 217, 227, 227b, 251(e), 303(r), 403, 501, 502, and 503 and Sections 4 and 7 of the TRACED Act, 47 U.S.C. 227b.

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

The RFA directs agencies to provide a description of and, where feasible, an estimate of the number of small entities that may be affected by the proposed rules, if adopted. The RFA generally defines the term ''small entity'' as having the same meaning as the terms ''small business,'' ''small organization,'' and ''small governmental jurisdiction.'' In addition, the term ''small business'' has the same meaning as the term ''small business concern'' under the Small Business Act. A ''small business concern'' is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA. 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.

Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe three broad groups of small entities that could be directly affected by our actions. In general, a small business is an independent business having fewer than 500 employees. These types of small businesses represent 99.9% of all businesses in the United States, which translates to 34.75 million businesses. Next, ''small organizations'' are not-for-profit enterprises that are independently owned and operated and not dominant in their field. While we do not have data regarding the number of

non-profits that meet that criteria, over 99 percent of nonprofits have fewer than 500 employees. Finally, ''small governmental jurisdictions'' are defined as cities, counties, towns, townships, villages, school districts, or special districts with populations of less than fifty thousand. Based on the 2022 U.S. Census of Governments data, we estimate that at least 48,724 out of 90,835 local government jurisdictions have a population of less than 50,000.

The rules proposed in the *FNPRM* will apply to small entities in the industries identified in the chart below by their six-digit North American Industry Classification System (NAICS) codes and corresponding SBA size standard. Where available, we also provide additional information regarding the number of potentially affected entities in the industries identified below.

TABLE 1—2022 U.S. CENSUS BUREAU DATA BY NAICS CODE

Regulated industry (footnotes specify potentially affected entities within a regulated industry where applicable)	NAICS code	SBA size standard	Total firms	Total small firms	% Small firms
Wired Telecommunications Carriers	517111	1,500 employees	3,403	3,027	88.95
Wireless Telecommunications Carriers (except Satellite)	517112	1,500 employees	1,184	1,081	91.30
Telecommunications Resellers	517121	1,500 employees	955	847	88.69
Satellite Telecommunications	517410	$44 million	332	195	58.73
All Other Telecommunications	517810	$40 million	1,673	1,007	60.19

TABLE 2—TELECOMMUNICATIONS SERVICE PROVIDER DATA

2025 Universal service monitoring report telecommunications service provider data (data as of December 2024)	SBA size standard (1,500 employees)		
Affected entity	Total number FCC form 499A filers	Small firms	% Small entities
Competitive Local Exchange Carriers (CLECs)	4,049	3,853	95.16
Incumbent Local Exchange Carriers (Incumbent LECs)	1,175	920	78.30
Interexchange Carriers (IXCs)	112	92	82.14
Local Exchange Carriers (LECs)	5,224	4,773	91.37
Local Resellers	253	242	95.65
Other Toll Carriers	72	69	95.83
Prepaid Card Providers	47	45	95.74
Telecommunications Resellers	655	630	96.18
Toll Resellers	402	388	96.52
Wired Telecommunications Carriers	4,971	4,531	91.15
Wireless Telecommunications Carriers (except Satellite)	608	522	85.86
Wireless Telephony	336	262	77.98

TABLE 3—CABLE ENTITIES DATA

Cable entities	Size standard	Total firms	Small firms	% Small firms in industry
Cable System Operators (Telecom Act Standard), Small Cable Operator.	Serves fewer than 498,000 subscribers, either directly or through affiliates.	530	524	98.87

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

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

In the *FNPRM,* the Commission proposes and seeks comment on rules that, if adopted, would affect all voice service providers seeking to obtain or maintain a filing in the RMD, including those that may be small entities. Specifically, we seek comment on whether we need to further clarify which entities qualify as voice service providers and therefore must file in the RMD. We propose and seek comment on enhancements to the information required in RMD filings, including additional certifications, more detailed ownership and affiliate disclosures, documentation regarding third-party service arrangements, enhanced robocall mitigation plan content, and more granular information about provider operations, numbering access, and STIR/SHAKEN implementation status. We seek comment on audit procedures and related burdens specific to small entities, expanding filing update requirements, potential participation bars, and new obligations related to traceback, data verification, and call acceptance by downstream providers. If adopted, these proposals could require small entities to devote additional resources to compliance, including the possible need to engage legal, technical, or compliance professionals, invest in new systems, or modify existing operational processes. However, good-faith providers likely already maintain much of the newly-required information in the normal course of business, and therefore we do not expect that the proposed rules, if adopted, would

require small entities to spend significantly more time submitting this information to the RMD. Additionally, several proposals—such as simplified filing formats, clearer definitions, and consolidation of certain disclosures—may reduce burdens by increasing predictability and reducing confusion for small entities. We anticipate that the comments we receive will assist the Commission in identifying and evaluating the extent of these potential burdens on small entities, including compliance costs such as whether small entities will have to hire professionals, and other burdens that may result from the inquiries we make in the *FNPRM.*

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

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

In the *FNPRM,* the Commission seeks to advance its objective of improving the effectiveness of the RMD while also minimizing unnecessary burdens on small entities. We seek comment on a range of proposals and possible alternatives that may impact small entities, including approaches specifically intended to achieve our goals to mitigate disruption to end users and consumers. For example, we seek comment on the use of third parties to submit RMD filings to reduce administrative costs for small providers that may lack significant in-house regulatory staff. We propose to specify the frequency with which providers must check the RMD to ensure compliance with new obligations and seek comment on whether that frequency should vary based on if the provider is a small or rural provider, and the associated costs for compliance. We also seek comment on whether any proposed enhancements to filing requirements could be tailored or streamlined for smaller providers, or whether certain information should be collected only when necessary for risk-based review. We also carefully consider the economic impact of these and other proposals on small entities and invite comment on potential approaches that would minimize burdens while still protecting consumers and the integrity of the U.S. voice network.

As we evaluate these proposals, the Commission will fully consider the economic impact on small entities, including costs and benefits identified in the record, and we expect that comments will provide additional insight into the potential compliance challenges these entities may face. We recognize that small providers may face unique challenges in meeting enhanced robocall mitigation, authentication, reporting, and filing obligations, and therefore we seek comment on the costs that could result from the proposed requirements and on alternative approaches that would achieve similar benefits at lower costs. The Commission's evaluation of the comments filed in this proceeding will shape the final conclusions it reaches, the final alternatives it considers, and the actions it ultimately takes to minimize any significant economic impact that may occur on small entities from the final rules.

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

None.

III. Ordering Clauses

Accordingly, pursuant to sections 4(i), 4(j), 201, 202, 217, 227, 251(e), 303(r), 403, 501, 502, and 503 of the Communications Act of 1934, as amended, 47 U.S.C. 154(i), 154(j), 201, 202, 217, 227, 251(e), 303(r), 403, 501, 502, and 503, and Sections 4 and 7 of the TRACED Act, 47 U.S.C. 227b, this Further Notice of Proposed Rulemaking *is adopted.*

It is further ordered that the Commission's Office of the Secretary *shall send* a copy of this Further Notice of Proposed Rulemaking, including the Initial Regulatory Flexibility Analysis, to the Chief Counsel for the Small Business Administration (SBA) Office of Advocacy.

List of Subjects in 47 CFR Parts 0, 1, and 64

Administrative practice and procedure, Communications, Communications common carriers, Communications equipment, Penalties, Reporting and recordkeeping requirements, Security measures, Telecommunications, Telephone, Waivers.

Federal Communications Commission.

Marlene Dortch,

Secretary.

Proposed Rules

For the reasons discussed in the preamble, the Federal Communications Commission proposes to amend 47 parts 0, 1, and 64 as follows:

PART 0—COMMISSION ORGANIZATION

■ 1. The authority citation for part 0 continues to read as follows:

Authority: 47 U.S.C. 151, 154(i), 154(j), 155, 225, 409, and 1754, unless otherwise noted.

■ 2. Amend § 0.91 by adding paragraph (s) to read as follows:

§ 0.91 Functions of the Bureau.

* * * * *

(s) Administer the Robocall Mitigation Database established under § 64.6305 of this chapter, in consultation with the Office of Managing Director, the Office of Economics and Analytics, and the Enforcement Bureau, as appropriate, including by:

(1) Establishing the form and format of filings;

(2) Making technical and operational changes to the Robocall Mitigation Database portal and submission interface;

(3) Developing and implementing technical data validation and screening measures;

(4) Developing measures for accepting and publishing a new or updated filing, including implementing policies and procedures for placing a filing into a pending status, withholding publication of a filing, rejecting publication of a filing, or removing a filing when the filing appears non-compliant, appears to have been submitted in evasion of Commission rules or orders, appears to have been submitted by, on behalf of, or for the benefit of a voice service provider whose filing was previously removed from the Robocall Mitigation Database absent any consent required under § 64.6305(n), or otherwise requires further analysis before it can be accepted and published because it appears to present a cause for removal or other enforcement action under § 64.6305(j); and

(5) Acting jointly with the Enforcement Bureau in determining whether filings are unauthorized under § 64.6305(m) and on requests for reinstatement under § 64.6305(n).

* * * * *

■ 3. Amend § 0.111 by revising paragraph (a)(28) to read as follows:

§ 0.111 Functions of the Bureau.

(a) * * *

(28) Take enforcement action, including removal from the Robocall Mitigation Database, against any voice service provider for any of the causes under § 64.6305(j) of this chapter, and act jointly with the Wireline Competition Bureau in determining whether filings are unauthorized under § 64.6305(m) and on requests for reinstatement under § 64.6305(n).

* * * * *

PART 1—Practice and Procedure

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

Authority: 47 U.S.C. chs. 2, 5, 9, 13; 28 U.S.C. 2461 note; 47 U.S.C. 1754, unless otherwise noted.

■ 5. Amend § 1.80002 by revising Table 1 to paragraph (a) to read as follows:

§ 1.80002 Schedules of Covered Authorizations subject to Foreign Adversary Control rules.

(a) *Schedule A Covered Authorizations.*

TABLE 1 TO PARAGRAPH (a)

Legal authority citation	Covered authorization type	Qualification(s)
47 CFR parts 22, 24, 27, 30, 90, 96, and 101	Broadband-capable, geographic-area wireless licenses in the following services: • AWS–4 (2000–2020 MHz and 2180–2200 MHz). • AWS–H Block (at 1915–1920 MHz and 1995–2000 MHz). • AWS–3 (1695–1710 MHz, 1755–1780 MHz, and 2155–2180 MHz). • AWS (1710–1755 MHz and 2110–2155 MHz). • 1670–1675 MHz Band, Market Area. • Broadband Radio Service. • 900 MHz Broadband Service. • Commercial Aviation Air-Ground Radiotelephone (800 MHz band). • Cellular. • PCS Broadband. • 1910–1915/1990–1995 MHz Bands, Market Area. • Educational Broadband Service. • 3.45 GHz Service. • 3.5 GHz Band Priority Access License. • 3.7 GHz Service. • Upper Microwave Flexible Use Service. • Wireless Communications Service. • 600 MHz Band. • 700 MHz Upper Band (Block C). • 700 MHz Lower Band (Blocks A, B & E). • 700 MHz Lower Band (Blocks C, D).	
47 CFR parts 26, 87, 90, 95, and 96	Frequency coordinator certifications.	
47 U.S.C. 310(b); 47 CFR part 1	Section 310(b) declaratory rulings.	
47 CFR part 25	Space and earth station authorizations.	
47 CFR parts 73, 74, 76, and 78	• Broadcast licenses (AM, FM, LPFM, FM translator, FM Booster, Full Power TV, Class A TV, LPTV, TV translator). • Cable television relay service station (CARS) licenses.	The holder of which has 6 or more full-time employees or, in the case of a holder of a broadcast license, receives an affirmative response under the Commission's foreign sponsorship identification rules from a lessee that is a foreign adversary.
47 CFR part 73	International broadcast station licenses	The holder of which has 6 or more full-time employees or receives an affirmative response under the Commission's foreign sponsorship identification rules from a lessee that is a foreign adversary.
47 U.S.C. 325(c); 47 CFR part 73	Section 325(c) authorizations	The holder of which has 6 or more full-time employees or receives an affirmative response under the Commission's foreign sponsorship identification rules from a lessee that is a foreign adversary.
Cable Landing License Act of 1921; Executive Order 10530 of 1954; 47 CFR part 1.	Submarine cable landing licenses.	
47 U.S.C. 214(a); 47 CFR part 63	Domestic section 214(a) authorizations.	
47 U.S.C. 214(e), 47 CFR part 54, subpart C	Eligible telecommunications carrier designations.	
47 U.S.C. 214; 47 CFR part 63	International section 214 authorizations.	
47 CFR part 52	Interconnected Voice over Internet Protocol direct access to numbering resources authorizations.	
47 CFR part 2, subpart J	Equipment certifications.	
47 CFR part 1; ITU–T Recommendation X.121.	Data network identification codes.	
47 CFR part 1; ITU–T Recommendation Q.708.	International signaling point codes.	
47 CFR part 1; 47 CFR part 63; Constitution and Convention of the International Telecommunication Union.	Recognized operating agencies.	
47 U.S.C. 225; 47 CFR part 64, subpart F	Internet-based telecommunications relay services certifications.	
47 CFR part 64, subpart HH	Robocall Mitigation Database filings	The filer is a domestic voice service provider and the filing has been accepted and published in the Robocall Mitigation Database pursuant to § 64.6305.

* * * * *

PART 64—MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

■ 6. 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.

■ 7. Amend § 64.6304 by redesignating paragraphs (c) through (f), as (d) through (g), and adding new paragraph (c) to read as follows:

§ 64.6304 Extension of implementation deadline.

* * * * *

(c) *Temporary SPC Token Extension.* A voice service provider that is in the process of obtaining an SPC token is exempt from the requirements of §§ 64.6301 and 64.6302.

* * * * *

■ 8. Revise § 64.6305 to read as follows:

§ 64.6305 Robocall mitigation.

(a) *Robocall mitigation program requirement.* Each voice service provider shall implement a robocall mitigation program that includes affirmative, effective measures to prevent its network or services from being used to transmit illegal calls.

(b) *Robocall Mitigation Database filing.*

(1) Each voice service provider, including each parent, affiliate, and subsidiary of a voice service provider that independently meets the definition of a voice service provider, shall submit a filing in the Robocall Mitigation Database that includes in English or with a certified English translation the information described in paragraphs (c) through (g) of this section.

(2) A voice service provider's Robocall Mitigation Database filing shall be signed by an officer of the voice service provider in conformity with § 1.16 of this chapter.

(3) A voice service provider's robocall mitigation plan required under paragraph (g) of this section shall be submitted as a PDF in machine-readable format.

(4) A filing does not appear in the Robocall Mitigation Database for purposes of this section unless and until the filing has been accepted and published in the Robocall Mitigation Database by the Wireline Competition Bureau under the measures developed pursuant to § 0.91(s)(4).

(c) *Certifications.*

(1) A voice service provider shall certify that:

(i) All of the calls its network or services transmit are subject to a robocall mitigation program consistent with paragraph (a) of this section;

(ii) It is not presently prohibited from filing in the Robocall Mitigation Database by the Commission;

(iii) It will respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium in accordance with § 64.1200(n)(1) of this chapter;

(iv) It will cooperate with the Commission, law enforcement, and the industry traceback consortium in investigating and stopping any person or entity from using the voice service provider's network or services to transmit illegal calls;

(v) It has not submitted false, misleading, or inaccurate information to the Commission, the Governance Authority, the Policy Administrator, any Certification Authority, or any agent or other third party designated by the Commission or acting on behalf of the Commission pursuant to Commission rules or direction; and

(vi) It is in compliance with all applicable Commission rules pertaining to robocalls and other illegals calls, including all rules in subparts L, P, and HH of this part and in part 52 of this chapter.

(2) A facilities-based voice service provider shall certify to one of the following:

(i) It has fully implemented the STIR/SHAKEN authentication framework across its entire network and services and all calls it transmits are compliant with the Commission's caller ID authentication rules;

(ii) It has implemented the STIR/SHAKEN authentication framework on a portion of its network and services and all calls it transmits on that portion of its network are compliant with the Commission's caller ID authentication requirements; or

(iii) It has not implemented the STIR/SHAKEN authentication framework on any portion of its network.

(3) A facilities-based voice service provider shall not certify to full or partial implementation of the STIR/SHAKEN authentication framework pursuant to paragraphs (c)(2)(i) or (c)(2)(ii) of this section unless it has obtained an SPC token and Secure Telephone Identity certificate and signs all calls using its certificate in accordance with §§ 64.6301 and 64.6302.

(4) A voice service provider that serves end users directly shall certify that it makes attestation level decisions and applies attestation levels consistent with the STIR/SHAKEN authentication framework for each of its end users' calls it transmits on its network or services.

(d) *Robocall mitigation information.*

(1) A voice service provider that has certified to partial or no implementation of the STIR/SHAKEN authentication framework pursuant to paragraphs (c)(2)(ii) or (c)(2)(iii) of this section shall identify the exemption(s) or extension(s) the voice service provider received under § 64.6304 by citing the rule(s) permitting the exemption(s) or extension(s) for those portions of its network and explaining in detail why the exemption(s) or extension(s) applies, including the facts specific to its network and services that are within the scope of the exemption(s) or extension(s) and any steps it has taken to confirm that it cannot implement STIR/SHAKEN, or indicate that it is a foreign voice service provider not subject to a STIR/SHAKEN implementation obligation;

(2) A voice service provider shall state whether, at any time in the prior two years, the filing entity (and/or any entity for which the filing entity shares common ownership, management, directors, or control) has been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal calls or spoofing, or a non-compliant Robocall Mitigation Database filing, and, if so, shall describe any such action or investigation, except to the extent and only for the period during which an action or investigation has been designated as non-public or confidential by a law enforcement agency, regulatory agency, court, or other government entity that is involved, by providing:

(i) All law enforcement or regulatory agencies involved;

(ii) The date any findings of actual or suspected wrongdoing were issued;

(iii) One or more identifier for the action or investigation, such as a file number, case number, or document number; and

(iv) A URL to access a publicly available document that describes the findings of wrongdoing made in connection with the action or investigation, or if no such document is publicly available, a copy of such document, or if not memorialized in a document, an accurate summary of the specific findings of wrongdoing made in connection with the action or

investigation, including whether the findings constitute an actual determination of wrongdoing or a suspected determination of wrongdoing.

(3) A voice service provider shall identify whether or not it uses third parties for the following purposes, and supply the email, phone number, and, if available, website for such third parties.

(i) To perform call analytics in connection with its obligation to describe its call analytics system in its robocall mitigation plan under paragraph (g)(2) of this section.

(ii) To perform the technological act of signing calls to satisfy STIR/SHAKEN obligations as permitted under §§ 64.6301(b) and 64.6302(f).

(iii) To fulfill its obligation to know its customers and/or know its upstream providers, as applicable, pursuant to § 64.1200(n)(4)–(5).

(iv) To submit Robocall Mitigation Database filings as required by paragraph (b) of this section.

(e) *Business identifying information.* All filings submitted in the Robocall Mitigation Database pursuant to paragraph (b) of this section shall include the following information:

(1) The voice service provider's business name(s) and primary address;

(2) Other business names in use by the voice service provider;

(3) All business names previously used by the voice service provider;

(4) The name, title, department, business address, telephone number, and email address of one person within the company responsible for addressing robocall mitigation-related issues;

(5) The name, title, telephone number, email address, physical address, country of residence, and citizenship for each human principal (which must be no less than one individual);

(6) The Robocall Mitigation Database number for each non-human principal, affiliate, subsidiary, and parent company that has a filing in the Robocall Mitigation Database or the name and business address for each non-human principal, affiliate, subsidiary, and parent company that does not have a filing in the Robocall Mitigation Database; and

(7) The name, United States mailing address, telephone number, and email address for a United States registered agent that is authorized to accept service on behalf of the voice service provider.

(f) *Provider type and service information.* All filings submitted in the Robocall Mitigation Database pursuant to paragraph (b) of this section shall include the following information:

(1) Whether the voice service provider is a foreign voice service provider;

(2) Whether the voice service provider:

(i) Is a facilities-based provider that:

(A) Is an originating or terminating voice service provider directly serving end users;

(B) Is an originating or terminating provider acting as a wholesale voice service provider that is originating or terminating calls for end users it does not directly serve on behalf of any other voice service provider(s);

(C) Is a gateway provider; and/or

(D) Is a non-gateway intermediate provider; and/or

(ii) Is a non-facilities-based provider that:

(A) Is directly serving end users; and/or

(B) Is a wholesale voice service provider to any other voice service provider(s) that does not directly serve end users.

(3) The voice service provider's OCN if the voice service provider:

(i) has claimed the temporary SPC token extension pursuant to § 64.6304(c);

(ii) has certified to full or partial STIR/SHAKEN implementation pursuant to paragraph (c)(2) of this section; or

(iii) if the voice service provider otherwise has an OCN.

(4) A general description of the nature of its voice service, including the types of services offered and the types of customers it serves or intends to serve.

(g) *Robocall mitigation plan.* A voice service provider shall describe in detail the affirmative, effective measures the voice service provider uses to prevent its network or services from being used to transmit illegal calls, as part of its robocall mitigation program required by paragraph (a) of this section, including:

(1) a description of how it complies with its obligation to know its customers and/or know its upstream providers, as applicable, pursuant to § 64.1200(n)(4)–(5);

(2) a description of the specific call analytics measures it uses to identify and block illegal calls and whether or not each measure is performed by the voice service provider or by a third party; and

(3) a description of any contractual provisions with end-users or upstream providers addressing robocall mitigation.

(h) *Requirement to keep filing updated.* A voice service provider shall update its filing within ten (10) business days of any change to the information it must provide pursuant to paragraph (b) of this section, except that:

(1) A voice service provider that has been aggrieved by a Governance Authority decision to revoke that voice service provider's SPC token need not update its filing on the basis of that revocation until the sixty (60)-day period to request Commission review pursuant to § 64.6308(b)(1) following completion of the Governance Authority's formal review process expires or, if the aggrieved voice service provider files an appeal, until ten (10) business days after the Wireline Competition Bureau releases a final decision pursuant to § 64.6308(d)(1).

(2) If a voice service provider elects not to file a formal appeal of the Governance Authority decision to revoke that voice service provider's SPC token, the voice service provider need not update its filing on the basis of that revocation until the thirty (30) day period to file a formal appeal with the Governance Authority Board expires.

(i) *Annual recertification requirement.* In accordance with this section and § 1.16, all voice service providers shall certify annually, on or before March 1, that any information submitted to the Robocall Mitigation Database is true and correct.

(j) *Causes for removal.* A filing may be removed from the Robocall Mitigation Database for the following reasons:

(1) *deficient filing* because it contains information that is incomplete or insufficient, but not substantially or materially so;

(2) *facially deficient filing* because it lacks required information or certifications or the information it contains is invalid, non-responsive, or illegible;

(3) *materially deficient RMD filing* because it contains information that is substantially and materially incomplete or insufficient, contains material internal inconsistencies, or contains information that is materially inconsistent with information the provider has reported elsewhere or with reliable external sources, including CORES, the Governance Authority, the Policy Administrator, and Certification Authority, or the North American Numbering Plan Administrator;

(4) *lack of candor,* including submission of false, misleading, or inaccurate information to the Commission, the Governance Authority, the Policy Administrator, a Certification Authority, or any agent or other third party designated by the Commission or acting on behalf of the Commission pursuant to Commission rules or direction, including the North American Numbering Plan Administrator and the industry traceback consortium;

(5) *annual recertification violations,* including failure to complete the recertification, failure to complete the recertification on time, and failure to

pay the required annual recertification fee;

(6) *accepting calls from a prohibited voice service provider,* including a voice service provider that does not have a filing that appears in the Robocall Mitigation Database, whose filing has been removed from the Robocall Mitigation Database, or that is subject to a mandatory blocking order under § 64.1200(n);

(7) *traceback violations,* including failure to respond to traceback requests, repeated appearance in tracebacks, or submission of incomplete or inaccurate information in traceback responses;

(8) *enabling transmission of illegal calls,* including knowingly or negligently initiating, originating, carrying, processing, or terminating illegal calls;

(9) *inadequate robocall mitigation measures,* including failure to implement a robocall mitigation program that complies with § 64.6305(a) or failure to comply with the robocall mitigation practices described in the voice service provider's robocall mitigation plan;

(10) *failure to cooperate with a Commission investigation,* including failure to respond to a subpoena, letter of inquiry, cease-and-desist letter, or notice of suspected illegal traffic;

(11) *impersonation,* including the unauthorized use of another person's or entity's identifying information in a Robocall Mitigation Database filing;

(12) *STIR/SHAKEN implementation violations,* including failure to implement STIR/SHAKEN in accordance with §§ 64.6301 and/or 64.6302, as applicable, improper attestations, and unauthorized authentication practices;

(13) *national security and law enforcement concerns,* including when a voice service provider, or the voice service provider's subsidiary or affiliate, is identified on the Covered List, is identified as having foreign adversary control through the Foreign Adversary Control System, is subject to a Commission action revoking or terminating a license or authorization on national security or law enforcement grounds, is otherwise subject to a final Commission determination that its continued participation in the United States communications ecosystem poses unacceptable risks, or is owned or controlled by, under common ownership or control with, or acting on behalf of an entity that is subject to any such determination;

(14) *final Commission enforcement actions* with accompanying findings of actual wrongdoing related to facilitating illegal calls or spoofing, including a final determination order under section 64.1200(n)(3), a forfeiture order involving illegal calls or spoofing (if the forfeiture is paid or ordered to be paid by a court), revocation of a Commission authorization, or a final order finding that the provider has failed to comply with any rule in subparts L, P, and HH of this part and in part 52 of this chapter; and

(15) *repeat violations for reinstated voice service providers,* including when the voice service provider is removed for one basis and, after reinstatement, commits a violation under the same or another basis.

(k) *Removal procedures.* A voice service provider's filing may be removed from the Robocall Mitigation Database under the following procedures:

(1) *Three-Step Removal Process.* For removals under paragraph (j)(1) of this section, or for any other cause for removal for which the Wireline Competition Bureau or Enforcement Bureau determines that the Three-Step Removal Process is appropriate:

(i) the Wireline Competition Bureau or the Enforcement Bureau will notify the voice service provider of the violation under paragraph (j) of this section and direct the voice service provider to, within 14 days, cure the violation and notify the Wireline Competition Bureau or the Enforcement Bureau that the violation has been cured or accurately explain why the violation is not applicable;

(ii) if the voice service provider fails to cure the violation or accurately explain why the violation is inapplicable, the Enforcement Bureau will issue an order finding that the voice service provider's filing qualifies for removal under the violation identified and directing the voice service provider to, within 14 days, cure the violation and notify the Enforcement Bureau that the violation has been cured or explain why its filing should not be removed; and

(iii) if the voice service provider fails to cure or provide a sufficient explanation within the 14-day period, the Enforcement Bureau will issue an order removing the filing from the Robocall Mitigation Database.

(2) *Two-Step Removal Process.* For removals under paragraph (j)(2) through (14) of this section, unless the Wireline Competition Bureau or the Enforcement Bureau determines that the Three-Step Removal Process is appropriate:

(i) the Enforcement Bureau will issue an order finding that the voice service provider's filing qualifies for removal due to a violation under paragraph (j) of this section based on the available evidence and directing the voice service provider to, within 5 days, cure the violation and notify the Enforcement Bureau that the violation has been cured or explain why its filing should not be removed; and

(ii) if the voice service provider fails to cure or provide a sufficient explanation within the 5-day period, the Enforcement Bureau will issue an order removing the filing from the Robocall Mitigation Database.

(l) *Customer notice.* A voice service provider whose filing has been removed from the Robocall Mitigation Database, or that is subject to a Commission mandatory blocking order under § 64.1200(n)(3), shall provide notice to its customers in the manner and within the timeframe specified by the Commission, Wireline Competition Bureau, or Enforcement Bureau.

(m) *Unauthorized Filings and Evasion.*

(1) A voice service provider whose filing has been removed from the Robocall Mitigation Database may not re-file in, or otherwise have a filing accepted and published in, the Robocall Mitigation Database unless and until the Enforcement Bureau and the Wireline Competition Bureau consent to reinstatement pursuant to paragraph (n) of this section.

(2) The Wireline Competition Bureau or Enforcement Bureau may, absent the consent required under paragraph (n) of this section, place into pending status, reject, suspend, or remove a filing that is made by, on behalf of, or for the benefit of a voice service provider whose filing has been removed from the Robocall Mitigation Database, that is prohibited from filing in the Robocall Mitigation Database, or that is an alter ego, successor, affiliate, or evasion vehicle of such voice service provider, person, or entity.

(n) *Reinstatement.* A voice service provider whose filing has been removed from the Robocall Mitigation Database may request reinstatement from the Enforcement Bureau and the Wireline Competition Bureau.

(1) A request for reinstatement must be made in writing and must demonstrate that the voice service provider has cured all violations under paragraph (j) of this section, paid any outstanding regulatory or filing fees owed to the Commission and forfeitures imposed by a court, updated all required Robocall Mitigation Database and CORES information, demonstrated compliance with traceback obligations, and implemented a robocall mitigation program consistent with paragraph (a)(1) of this section.

(2) The Enforcement Bureau, in consultation with the Wireline Competition Bureau, may grant, deny, or condition reinstatement based on the voice service provider's showing, the voice service provider's cooperation with the Bureaus, the voice service provider's compliance history, and the risk that reinstatement would permit the voice service provider's network or services to be used to transmit illegal calls.

(3) A filing submitted pursuant to a grant of reinstatement does not appear in the Robocall Mitigation Database for purposes of this section unless and until the filing has been accepted and published in accordance with paragraph (b)(4) of this section.

(o) *Voice traffic acceptance obligations.*

(1) *Accepting calls from domestic voice service providers.* A voice service provider shall not accept calls directly from a domestic voice service provider unless that domestic voice service provider's filing appears in the Robocall Mitigation Database in accordance with paragraph (b)(4) of this section and has not been removed pursuant to Commission action.

(2) *Accepting calls from foreign voice service providers.* A voice service provider shall not accept calls directly from a foreign voice service provider unless that foreign voice service provider's filing appears in the Robocall Mitigation Database in accordance with paragraph (b)(4) of this section and has not been removed pursuant to Commission action.

(3) *Public safety safeguards.* Notwithstanding paragraphs (o)(1) and (2) of this section:

(i) A voice service provider may not block a voice call under any circumstances if the call is an emergency call placed to 911; and

(ii) A voice service provider must make all reasonable efforts to ensure that it does not block any calls from public safety answering points and government emergency numbers.

[FR Doc. 2026–18366 Filed 9–8–26; 8:45 am]

BILLING CODE 6712–01–P