Dated: September 6, 2024.

Xavier Becerra,

Secretary.

Accordingly, by the authority vested in me as the Secretary of Health and Human Services, and for the reasons set forth in the preamble, 42 CFR part 121 is proposed to be amended as follows:

PART 121—ORGAN PROCUREMENT AND TRANSPLANTATION NETWORK

■ 1. The authority citation for part 121 continues to read as follows:

Authority: Sections 215, 371–77, and 377E of the PHS Act (42 U.S.C. 216, 273–274d, 274f–5); sections 1102, 1106, 1138 and 1871 of the Social Security Act (42 U.S.C. 1302, 1306, 1320b–8, and 1395hh); section 301 of the National Organ Transplant Act, as amended (42 U.S.C. 274e); and E.O. 13879, 84 FR 33817.

■ 2. In § 121.6, revise paragraph (b) to read as follows:

§ 121.6 Organ procurement.

* * * * *

(b) *HIV.* (1) Organs from donors with human immunodeficiency virus (HIV) may be transplanted only into individuals who—

(i) Are living with HIV before receiving such organ(s); and

(ii)(A) Are participating in clinical research approved by an institutional review board, as defined in 45 CFR part 46, under the research criteria published by the Secretary under subsection (a) of section 377E of the Public Health Service Act, as amended; or

(B) The Secretary has published, through appropriate procedures, a determination under section 377E(c) of the Public Health Service Act, as amended, that participation in such clinical research, as a requirement for transplants of donor organs with HIV, is no longer warranted. The Secretary has determined that participation in such clinical research is no longer warranted for the following categories of transplants:

(*1*) Transplant of a donor kidney with HIV; and

(*2*) Transplant of a donor liver with HIV.

(2) Except as provided in paragraph (b)(3) of this section, the OPTN shall adopt and use standards of quality with respect to donor organs with HIV to the extent the Secretary determines necessary to allow the conduct of research in accordance with the criteria described in paragraph (b)(1)(ii)(A) of this section.

(3) If the Secretary has determined under paragraph (b)(1)(ii)(B) of this section that participation in clinical research is no longer warranted as a requirement for transplants of donor organs with HIV, the OPTN shall adopt and use standards of quality with respect to donor organs with HIV as directed by the Secretary, consistent with 42 U.S.C. 274, and in a way that ensures the changes will not reduce the safety of organ transplantation.

* * * * *

[FR Doc. 2024–20643 Filed 9–11–24; 8:45 am]

BILLING CODE 4150–28–P

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Parts 1 and 64

[GN Docket No. 24–213; MD Docket No. 10–234; FCC 24–85; FR ID 240720]

Improving the Effectiveness of the Robocall Mitigation Database; Amendment of CORES Registration System

AGENCY: Federal Communications Commission.

ACTION: Proposed rule.

SUMMARY: In this document, the Federal Communications Commission (Commission) proposes and seeks comment on procedural measures that would require Robocall Mitigation Database filers to take additional steps to ensure the accuracy of submitted information, potential technical solutions for validating data, accountability measures to ensure and improve the overall quality of submissions in the Robocall Mitigation Database, and generally invites comment on any other procedural steps the Commission could require to increase the effectiveness of the Robocall Mitigation Database as a compliance and consumer protection tool.

DATES: Comments are due on or before October 15, 2024, and reply comments are due on or before November 12, 2024.

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 above. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS). *See Electronic Filing of Documents in Rulemaking Proceedings,* 63 FR 24121 (1998).

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

Accessible Formats. To request materials in accessible formats for people with disabilities (Braille, large print, electronic files, audio format), send an email to *fcc504@fcc.gov* or call the Consumer & Governmental Affairs Bureau at 202–418–0530 (voice).

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

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's *NPRM* in GN Docket No. 24–213, MD Docket No. 10–234, released on August 8, 2024. The complete text of this document is available for download at *https://docs.fcc.gov/public/attachments/FCC-24-85A1.pdf.*

Paperwork Reduction Act: The *NPRM* may contain proposed new and revised information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and the Office of Management and Budget (OMB) to comment on the information collection requirements contained in this document, as required by the Paperwork Reduction Act of 1995, Public Law 104–13. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107–198, see 44 U.S.C. 3506(c)(4),

we seek specific comment on how we might further reduce the information collection burden for small business concerns with fewer than 25 employees.

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

Providing Accountability Through Transparency Act: The Providing Accountability Through Transparency Act, Public Law 118–9, requires each agency, in providing notice of a rulemaking, to post online a brief plain-language summary of the proposed rule. The required summary of the *NPRM* is available at *https://www.fcc.gov/proposed-rulemakings.*

Synopsis

I. Introduction

Illegal robocalls cause billions of dollars in consumer fraud, not to mention the losses suffered by consumers due to lost time and attention, and diminished confidence in the Nation's telephone network. In 2023, the Commission received approximately 96,500 complaints concerning unwanted calls, including illegal robocalls—more than any other issue. Protecting Americans from illegal robocalls remains the Commission's top consumer protection priority. With the NPRM we launch a proceeding to explore new initiatives intended to increase consumer protection, reduce unwanted calls, and increase accountability of non-compliant providers.

This initiative follows a series of Commission actions on multiple fronts to stem the tide of robocalls using every tool at our disposal. One such tool is the Robocall Mitigation Database (RMD or Database), a public database established by the Commission in 2021 to facilitate the implementation of our STIR/SHAKEN and robocall mitigation rules. Consistent with the Commission's efforts to expand both STIR/SHAKEN implementation and robocall mitigation requirements in recent years, *all* providers are now required to file certifications and robocall mitigation plans in the Robocall Mitigation Database, as well as additional information to assist the Commission with evaluating compliance with our rules. This makes the Robocall Mitigation Database an essential consumer protection tool that is not only relied upon by the Commission for our own enforcement activities, but by other Federal and state enforcement bodies, and by downstream providers, which are prohibited from accepting a provider's traffic if it is not listed in the Robocall Mitigation Database. It is, therefore, critical that the information submitted to the Robocall Mitigation Database by providers be complete, accurate, and up-to-date.

Given the importance of the Robocall Mitigation Database, we launch this proceeding to examine ways to ensure and improve the overall quality of submissions based on the collective experience of all stakeholders over the last three years. Specifically, we propose and seek comment on procedural measures that the Commission could adopt to promote the highest level of diligence when providers submit required information to the Robocall Mitigation Database, and technical solutions that the Commission could use to identify data discrepancies in filings—and require them to be corrected—before they are accepted by the system. At this time, we are not proposing or seeking comment on additional content requirements for Robocall Mitigation Database filings. The Commission adopted significant additional content requirements in March 2023 and required all providers to submit Robocall Mitigation Database filings that complied with those additional requirements by February 26, 2024. Those filings are currently under review. We propose and seek comment on measures to increase accountability for providers that submit inaccurate and false information to the Robocall Mitigation Database or fail to update their filings when the information they contain changes, as required by the Commission's rules. Lastly, we generally invite comment on any other procedural steps the Commission could require to increase the effectiveness of the Robocall Mitigation Database as a compliance and consumer protection tool.

II. Background

The Commission created the Robocall Mitigation Database in 2021 to effectuate provisions of the TRACED Act, which directed the Commission to require voice service providers to implement the STIR/SHAKEN caller ID authentication framework on their IP-based voice networks by June 30, 2021, subject to certain extensions due to undue hardship or reliance on non-IP infrastructure. The TRACED Act included two provisions for extension of the June 30, 2021, implementation deadline. First, it permitted the Commission to extend the compliance date for a reasonable period of time ''upon a public finding of undue hardship,'' and second, it directed the Commission to grant an extension to those providers that ''materially rel[y]'' on non-IP infrastructure. First, it permitted the Commission to extend the compliance date for a reasonable period of time ''upon a public finding of undue hardship,'' and second, it directed the Commission to grant an extension to those providers that ''materially rel[y]'' on non-IP infrastructure. Pursuant to these provisions, in 2020 the Commission granted three categorical STIR/SHAKEN implementation extensions on the basis of undue hardship to: (1) small voice service providers with 100,000 or fewer voice subscriber lines; (2) voice service providers unable to obtain the SPC ''token'' necessary to participate in STIR/SHAKEN; and (3) services scheduled for section 214

discontinuance. Further, the Commission granted voice service providers a continuing extension for the portions of their networks that rely on technology that cannot initiate, maintain, or terminate SIP calls. The implementation extensions for services scheduled for section 214 discontinuance ended on June 30, 2022, and the implementation extensions for non-facilities-based and facilities-based small voice service providers ended on June 30, 2022, and June 30, 2023, respectively. In 2023, the Commission granted an indefinite extension of time for small voice providers that are satellite providers originating calls using North American Numbering Plan (NANP) numbers on the basis of the TRACED Act's undue hardship standard. Under the framework established by the TRACED Act, any voice service provider that is granted a STIR/SHAKEN implementation extension pursuant to these provisions must implement ''an appropriate robocall mitigation program to prevent unlawful robocalls from originating on the network of the provider.'' To promote transparency, effective mitigation practices, and diligent enforcement of the Commission's rules, the Commission required voice service providers to submit certifications to the Robocall Mitigation Database concerning their STIR/SHAKEN implementation progress, and if they had not fully implemented STIR/SHAKEN, a description of their robocall mitigation program, including ''[t]he specific reasonable steps the voice service provider has taken to avoid originating illegal robocall traffic.'' Providers filing in the Robocall Mitigation Database were also required to submit additional information, including business names and addresses, and a point of contact for resolving robocall-mitigation related issues. The Commission made the certification data and robocall mitigation plans filed in the Robocall Mitigation Database publicly available on the Commission's website to facilitate inter-provider cooperation and the public's ability to understand providers' robocall mitigation practices.

Since 2021, the Commission has worked to expand the scope of providers required to implement STIR/SHAKEN and comply with robocall mitigation requirements, and thus, the providers required to submit certifications and robocall mitigation plans in the Robocall Mitigation Database. Today, all providers carrying or processing voice traffic—voice service providers, gateway providers, and non-gateway intermediate providers—are required to file certifications and robocall mitigation plans in the Robocall Mitigation Database. The consequences for not doing so, or for filing certifications and robocall mitigation plans that do not comply with the Commission's rules, are severe. They may include the imposition of a Commission forfeiture and/or the removal of a deficient filing from the Database. The latter remedy effectively precludes the provider from operating as a provider of voice services in the United States, as the Commission's rules prohibit intermediate and terminating providers from accepting traffic directly from any provider that does not appear in the Database. This prohibition, which denies ''a service provider access to the regulated U.S. voice network if [the Commission] determines that the service provider's . . . robocall mitigation practices are inadequate,'' recognizes the importance of the information submitted to the Robocall Mitigation Database and its role as a tool for enforcement and industry self-regulation.

A. Content Requirements for Robocall Mitigation Database Submissions

To start a filing in the Robocall Mitigation Database, providers must first obtain a business-type FCC Registration Number (FRN) via the FCC's Commission Registration System (CORES) and an FCC username and password. 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. An FRN is a unique 10-digit number assigned to a business or individual registering with the Commission that is used to identify the registrant's business dealings with the agency. Providers establish a CORES account and FRN to submit a new filing or manage existing filings in the Robocall Mitigation Database. Once a provider's FRN is selected in the Database, the entity name and business address associated with that FRN are automatically populated in the Robocall Mitigation Database certification form. These fields of the certification form are ''read only'' and may not be changed without changing the associated data in CORES.

To complete the remainder of the Robocall Mitigation Database certification form, providers must manually enter additional information, including:

- Whether the provider has fully, partially, or not implemented the STIR/SHAKEN authentication framework in the IP portions of its network;
- Confirmation that all of the calls that it originates on its network are subject to a robocall mitigation program consistent with § 64.6305(a), (b), and/or (c);
- Confirmation that any prior Robocall Mitigation Database submission has not been removed by Commission action and that the provider has not been prohibited from filing in the Robocall Mitigation Database by the Commission;
- Any other business name(s) currently in use by the provider;
- All business names previously used by the provider;
- Whether the provider is a foreign voice service 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;
- The provider's role(s) in the call path;
- Whether the provider is eligible for any STIR/SHAKEN implementation extensions or exemptions;
- Information regarding the provider's principals, affiliates, subsidiaries, and parent companies;
- Information on any recent enforcement actions concerning illegal robocalls; and
- The provider's Operating Company Number (OCN), if it has one.

Once the certification is complete, providers must then upload a PDF file containing the written description of their robocall mitigation programs. Providers that wish to designate a portion of their robocall mitigation program filing as confidential may upload both confidential (*i.e.,* unredacted) and non-confidential (*i.e.,* redacted) documents pursuant to the terms of the Protective Order adopted for Robocall Mitigation Database filings. Under the Commission's rules, all providers are required to develop robocall mitigation programs that include reasonable steps to avoid transmitting illegal robocall traffic, and include commitments 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 calls. The Commission's ''reasonable steps'' standard requires that a robocall mitigation program '' 'include[ ] detailed practices that can reasonably be expected to significantly reduce' the carrying or processing (for intermediate providers) or origination (for voice service providers) of illegal robocalls.'' Certain additional

requirements apply based on the role the provider plays in the call path. For instance, voice service providers must describe how they are meeting their existing obligation to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls, and gateway providers and non-gateway intermediate providers must describe their 'know-your-upstream provider' procedures designed to mitigate illegal robocalls. In addition, all providers must describe any call analytics systems they use to identify and block illegal traffic, including whether they use a third-party vendor or vendors and the name of the vendor(s).

The Commission has not otherwise 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.'' At the same time, the Commission directed that providers must comply with the practices specified in their robocall mitigation plans and that their robocall mitigation programs will be deemed deficient if the provider knowingly or through negligence carries or processes calls (for intermediate providers) or originates (for voice service providers) unlawful robocall campaigns. Further, a robocall mitigation plan will be deemed facially deficient if it does not provide any information about the specific reasonable steps that the provider is taking to mitigate illegal robocalls. For example, robocall mitigation plans that only include a generalized statement that a robocall mitigation plan is in place or merely recite the Commission's rules for robocall mitigation will be deemed facially deficient. Providers that submit deficient robocall mitigation plans to the Robocall Mitigation Database and fail to cure those deficiencies are referred to the Commission's Enforcement Bureau for investigation and potential removal from the Database, after which all downstream providers will be prohibited from carrying their traffic.

B. When and How Robocall Mitigation Database Submissions are Filed

Providers are required to submit Robocall Mitigation Database certifications and robocall mitigation plans pursuant to deadlines set and announced by the Commission. Providers are also required to update their submissions within 10 business days of any changes to required content. For instance, if the contact information provided for the individual within the company responsible for robocall mitigation efforts has changed since the provider submitted its certification and robocall mitigation plan to the Robocall Mitigation Database, the provider is required to update its submission to include the current contact information within 10 business days of that change.

All Robocall Mitigation Database submissions are filed via a portal accessible on the Commission's website at *https://www.fcc.gov/robocall-mitigation-database.* After entering all of the required content, the provider's submission must be electronically signed by an officer of the company who certifies, under penalty of perjury, that the information included in the submission is true and correct. The submission is then accepted by the system. Instructions to assist filers with completing their Robocall Mitigation Database submissions are available on the Commission's website, as well as other reference documents providing guidance to providers on what is required to comply with the Commission's rules. Any provider or member of the public may view submissions to the Robocall Mitigation Database via the Commission's website or download a list of them as a .CSV file.

III. Discussion

The Robocall Mitigation Database is a critical tool in the Commission's efforts to ensure compliance with its STIR/SHAKEN and robocall mitigation rules and protect the public from the harms caused by illegal robocalling campaigns. Many stakeholders outside of the Commission also depend on the information in the Robocall Mitigation Database to make important decisions that directly impact consumers. Downstream providers use the information in the Database to determine whether they are permitted to carry traffic on their networks, and other consumer protection and enforcement bodies use the information to pursue their own investigations into suspected illegal robocalling activities under applicable laws. Information submitted to the Robocall Mitigation Database by providers must be accurate and complete, and the Commission's requirements for filing in the Database and related accountability measures must promote accuracy, thoroughness, and continued diligence.

A review of filings in the Robocall Mitigation Database indicates that, among some providers, diligence is lacking. We have identified deficiencies ranging from failures to provide accurate contact information to failing to submit robocall mitigation plans that in any way describe reasonable robocall mitigation practices. While the Commission has acted to support the integrity of Robocall Mitigation Database information by removing deficient filings through enforcement actions and remains committed to doing so, there may be ways that the Commission could incentivize providers to avoid submitting deficient filings to the Database in the first instance through additional procedural steps, accountability measures, and technical validation solutions. In addition to improving the overall quality of submissions to the Robocall Mitigation Database, such measures may also deter bad actors that wish to evade our rules by deliberately submitting false or misleading information to the Database in an effort to ensure the traffic they send is carried by downstream providers.

We initiate this proceeding to propose and seek comment on additional procedural and accountability measures for the Robocall Mitigation Database to make it as effective as possible for the providers and government entities that use it, and thus the consumers it was instituted to protect. Specifically, we:

- Propose to amend the Commission's rules to require providers to update information they have submitted to CORES within 10 business days of any changes to ensure that the business name and address information automatically populated into Robocall Mitigation Database submissions from that system is current;
- Propose to require multi-factor authentication each time a provider accesses the Robocall Mitigation Database;
- Seek comment on requiring providers to obtain a unique Personal Identification Number (PIN) that must be provided before the Robocall Mitigation Database will accept a submission;
- Seek comment on requiring providers to remit a filing fee for submissions to the Robocall Mitigation Database;
- Seek comment on technical solutions that will scan Robocall Mitigation Database submissions, flag data discrepancies, and require providers to resolve such discrepancies before the submission is accepted by the filing system;
- Propose base and maximum forfeiture amounts for submitting inaccurate or false information to the Robocall Mitigation Database, or failing to update information that has changed within 10 business days, as required by the Commission's rules;
- Propose to authorize downstream providers to permissively block traffic from Robocall Mitigation Database filers

that have been given notice of facial deficiencies in their robocall mitigation plans and failed to correct those deficiencies within 48 hours; and

- Seek comment on additional procedural steps the Commission could require to encourage providers to submit accurate and complete information to the Robocall Mitigation Database and CORES and keep that information current.

We estimate that the gains—including reduced fraud, avoided aggravation, and enhanced consumer confidence—should far exceed any added compliance burdens. We seek comment on the costs and benefits of our proposals outlined below.

A. Measures To Improve the Quality of Robocall Mitigation Database Submissions

In this section, we seek comment on procedural and technical measures to improve the overall quality of Robocall Mitigation Database submissions in order to make the Database more effective for all stakeholders who use it. First, we seek comment on any additional steps filers should be required to affirmatively take to ensure the accuracy of information submitted to the Robocall Mitigation Database, and to ensure that such information remains accurate and up-to-date over time. Second, we seek comment on any technical solutions that the Commission could deploy to validate data in submissions and flag discrepancies before they are accepted by the Robocall Mitigation Database.

1. Procedural Steps To Improve the Accuracy of Robocall Mitigation Database Filings

We seek comment on whether the Commission should adopt additional procedural steps for Robocall Mitigation Database filings to improve and ensure the accuracy of information contained in the Robocall Mitigation Database. We believe that there is ample information in the Commission's rules, orders, public notices, filing instructions, and other materials to advise providers on *what* they must file in the Robocall Mitigation Database to comply with our rules. We now turn to explore ways to improve diligent adherence to those requirements by filers. We, therefore, seek comment on measures that will prompt providers to affirmatively verify that the information they submit is responsive to the Commission's legal requirements and factually accurate, and to incentivize compliance with the on-going requirement to keep information in the Robocall Mitigation Database current. In addition to the specific measures discussed below, we invite general comment on procedures that we could adopt that would achieve these goals.

Requiring Filers to Update Information in CORES. We first propose adopting a rule to require providers to update any information submitted to CORES within 10 business days of any changes to that information. As noted above, a CORES account and FRN are required to file in the database. A user's FRN is uniquely associated with each Robocall Mitigation Database filing, and the entity name and address associated with this FRN in CORES are imported directly into the Database along with a user's FRN. This contact information, along with a taxpayer identification number (TIN), such as a Social Security Number (SSN) for individuals, or an Employer Identification Number (EIN) for businesses is entered by users when they create a CORES account and complete an FRN registration form. Currently, § 1.8002 of the Commission's rules, which governs obtaining an FRN, requires that information submitted by registrants, including the entity's name and address, ''be kept current.'' It does not, however, establish a deadline for submitting updates after a change in information occurs. Thus, information in CORES may be out of date at the time a provider submits a certification and robocall mitigation plan to the Robocall Mitigation Database, resulting in inaccurate information being imported into the Database.

We therefore propose to require all entities and individuals that register in CORES to update any information required by the system within 10 business days of any changes, as is currently required for filings in the Robocall Mitigation Database. We seek comment on the benefits and burdens of this proposal. We believe a requirement to update contact information promptly would not impose any significant costs on CORES users, which are already obligated to keep their information current under § 1.8002, and that any incidental burdens are easily outweighed by the significant interests of the Commission and other stakeholders in obtaining accurate identifying information from the Commission's databases. This is particularly true given that other Commission databases beyond the Robocall Mitigation Database similarly make use of contact information imported directly from CORES. We seek comment on this view. Are there nevertheless any countervailing burdens that the Commission should consider in weighing this proposal? How should the Commission enforce such a requirement, if it were adopted? Should this proposed deadline apply to all entities registering for an FRN, or only those that must file in the Robocall Mitigation Database? Since Robocall Mitigation Database filers must obtain a business-type FRN in order to submit a certification, should we apply this requirement only to business-type FRNs, rather than individual FRNs? Are there reasons a longer duration of time may be necessary for individual FRN holders? Are there alternative proposals the Commission should consider to ensure the accuracy of information submitted to CORES, and by extension, other FCC databases that make use of information imported from CORES?

Multi-Factor Authentication. We seek comment on whether to deploy multi-factor authentication functionality for the Robocall Mitigation Database and whether to require providers to use such technology in order to submit a filing to the Database. Multi-factor authentication, which requires use of multiple authentication protocols in order to grant access to an account—for example, a password and a one-time verification code—is more secure than authentication with a username and password alone. We note that the Commission's Office of Managing Director recently required all CORES users to undergo two-factor authentication each time a user logs into CORES. Under this system users are ''prompted to request a six-digit secondary verification code, which will be sent to the email address(es) associated with each username.'' The code must then be entered into CORES by the user before accessing their account. Would a more robust authentication system of this kind be beneficial for the Robocall Mitigation Database? Why or why not? If the Commission were to require multi-factor authentication for the Database, what type of authentication protocol should the Commission employ? For example, in addition to a password, should the Commission require use of a one-time verification code provided by an authentication app or physical security key? We tentatively conclude that, under applicable OMB policy, if the Commission adopts multi-factor authentication for the Robocall Mitigation Database, we also will have to afford users the option to use ''phishing-resistant authentication'' methods. We seek comment on this understanding and on users' expectations regarding authentication methods. We also seek comment on the benefits and burdens associated with

different means of deploying such functionality.

Requiring Filers to Obtain a PIN to File in the Robocall Mitigation Database. In addition, or as an alternative to the multi-factor authentication methods discussed above, we seek comment on increasing accountability for the accuracy of information submitted to the Robocall Mitigation Database by requiring an officer, owner, or other principal of a provider (collectively, ''officer'') to obtain a PIN that must be entered before an Robocall Mitigation Database submission is accepted by the filing system. Currently, an officer is required to electronically sign a provider's Robocall Mitigation Database certification. By doing so, the officer declares that ''under penalty of perjury'' the information provided in the Robocall Mitigation Database submission is true and correct. As noted above, the provider's business name and address is imported from CORES, and contact information for an employee of the company responsible for robocall mitigation must be provided. An officer is not, however, required to provide their own direct contact information or to make more specific certifications with respect to their role in ensuring that the provider submits and maintains accurate information in the Robocall Mitigation Database. We are concerned that this may lead to consultants and provider employees completing Robocall Mitigation Database submissions without sufficient diligence, and that an additional verification step by the responsible officer may be necessary to ensure that Robocall Mitigation Database certifications and robocall mitigation plans are submitted and kept up-to-date in accordance with our rules.

We therefore seek comment on whether we should require the signing officer to submit additional information and certifications to obtain a PIN that must be used to submit an Robocall Mitigation Database certification. Specifically, we seek comment on requiring the officer to complete a form, separate from the filing in the Robocall Mitigation Database and prior to certification thereto can be submitted, that collects: (1) A non-P.O. box street address and telephone number for the location of the office where the officer does business, and a direct business email address for the officer; (2) a business address, telephone number, and email address for the provider's registered agent for service of process in the District of Columbia (or a certification that such an agent is not required by § 1.47(h) of the Commission's rules); and (3) certifications, under penalty of perjury pursuant to § 1.16 of the Commission's rules, that the officer:

- Is authorized to submit the PIN form, Robocall Mitigation Database certification, and robocall mitigation plan on behalf of the provider;
- Has personally reviewed the provider's Robocall Mitigation Database certification and robocall mitigation plan and verifies that the information provided in both is true and accurate;
- Verifies that the information in the PIN form is true and accurate;
- Understands that the provider is required to update the information submitted to the Robocall Mitigation Database within 10 business days of any changes, and that failure to do so could result in the provider's filing being removed from the Robocall Mitigation Database and additional penalties permitted under law, including a forfeiture as discussed in section B.1 below; and
- Understands that any false statements on the PIN form and in the Robocall Mitigation Database submissions can be punished by fine or forfeiture under the Communications Act, 47 U.S.C. 502, 503(b), and removal of the provider's filing from the Robocall Mitigation Database.

By direct business email address, we mean a business email address associated with the officer individually and used by them to conduct business in their official capacity, rather than a general email inbox, such as ''*robocall.mitigation@provider.com,*'' which is not tied to any specific individual(s).

We tentatively conclude that we have authority to adopt this information collection under the provisions of the Communications Act cited herein. We seek comment on this tentative conclusion and on whether requiring the submission of this information to obtain a PIN to file in the Robocall Mitigation Database will improve the accuracy of the information in the Database. In particular, we seek comment on whether such a system would dissuade inaccurate or inadequately reviewed filings, or filings by bad actors by: (1) increasing direct accountability by an officer for reviewing, understanding, and verifying the contents of a provider's filing; and (2) providing additional direct contact information that can be used in enforcement actions if the business information imported from CORES or robocall mitigation contact information submitted to the Robocall Mitigation Database is inaccurate or becomes out of date. We seek comment on the scope of this information collection and whether it is sufficient to achieve these objectives. Should we collect additional or different information and certifications, and if so, what? To the extent necessary, the Commission will make necessary changes to the applicable System of Records under the Privacy Act. Is there information that we could also collect to verify that the person completing the form is, in fact, an officer of a legitimate provider? Should we require that all filers, even those not required to under § 1.47(h) of the Commission's rules, have a registered agent in the District of Columbia and report that information via this separate PIN form? We believe that doing so would aid in Commission investigations into bad actors that should be removed from the Database and for purposes of service of process. We seek comment on whether and how such a requirement would facilitate these or other goals.

We seek comment on the benefits and burdens of such an information collection, and on any alternative approaches. What are the burdens and potential consequences of collecting this information? How could we mitigate these burdens? Are there, for example, confidentiality or privacy issues with collection of this information? Because the information that we propose to collect is about individuals in their official or business capacities, we expect that this information is low sensitivity, reducing the privacy risk associated with this proposed collection. We also anticipate that, relative to other Commission programs that collect personally identifiable information (PII) and/or Privacy Act records, fewer individuals, who generally are not members of vulnerable populations, will be required to submit this low-sensitivity information to the database, further reducing the privacy risk. We seek comment on this analysis. We also note that our proposed requirement, discussed above, that filers update their information in CORES will help ensure the accuracy, relevance, timeliness, and completeness of the PII and/or records that we are proposing to collect. Additionally, under the Federal Information Security Modernization Act of 2014 (FISMA), any information system that we would use to collect information and provide PINs would need to have applicable privacy and security controls to ensure the confidentiality, integrity, and availability of such information. We therefore tentatively conclude that the overall privacy risk associated with this collection of information would be low.

We seek comment on this tentative conclusion and the reasons for it. We also seek comment on whether the collection of this information would cause any undue delays for providers in submitting their filings.

We seek comment on the method by which the Commission could collect this information and generate the PIN for use by the officer when submitting an Robocall Mitigation Database filing. We expect that this information collection would require the use of a platform accessed via the Commission's website that would allow the officer to complete a digital form and then generate the PIN. We seek comment on any such platforms or other PIN-generating solutions that are currently in use, including any that are currently employed by other Federal agencies. Are there other procedural issues we should consider? For example, should a provider be required to submit a new PIN form within 10 business days if the officer leaves the company or any information on the form changes? Should we require providers to obtain a PIN each time they revise their filing (*i.e.,* a unique PIN for each submission) or just once (*i.e.,* a unique PIN for each filer)? In keeping with the two-factor authentication protocol deployed recently for CORES, we believe that requiring a PIN for each submission would provide greater security benefits. We seek comment on this view.

We also seek comment on whether to require all providers that have already filed in the Robocall Mitigation Database to submit the separate form we propose above as a prerequisite to obtaining a PIN, so that the Commission has the same information on file for all providers in the Database. We also seek comment on any procedural steps that would guard against bad actors submitting false information to obtain a PIN. Finally, we seek comment on delegating authority to the Wireline Competition Bureau, in consultation with the Office of the Managing Director, to take the steps necessary to implement any system for collecting the information required to generate and provide Robocall Mitigation Database filers with a PIN, to publish instructions for providers on how to use the system, and to establish additional filing requirements needed to achieve the objectives of the system.

Requiring Providers to Remit a Filing Fee. We next seek comment on requiring providers to pay a fee when submitting filings to the Robocall Mitigation Database. Section 8(a) of Communications Act states that ''[t]he Commission shall assess and collect application fees at such rates as the Commission shall establish in a schedule of application fees to recover the costs of the Commission to process applications.'' In 2018, as part of the RAY BAUM'S Act of 2018, Congress revised the Commission's application fee authority by amending section 8 and adding section 9A to the Communications Act. Prior to the RAY BAUM'S Act, the Commission had limited authority to amend the application fee schedule, which was set out by Congress. The Commission was required to simply adjust these fees every two years to reflect changes in the Consumer Price Index; the Commission did not have the authority to make other changes to application fees or to add or delete fee categories. Pursuant to the requirements of the RAY BAUM's Act, the Commission has adopted a schedule of fees based on the cost of processing applications, with cost determined based on direct labor costs. The Commission uses time and staff compensation estimates to establish the direct labor costs of application fees, which are in turn based on applications processed by Commission staff found to be typical in terms of the amount of time spent on processing each type of application. In applying our statutory authority, we adhere to the goal of ensuring that our fees are fair, administrable, and sustainable. This is the same overarching set of goals we employ in the context of our regulatory fee collections. The application of our overarching program goals, however, must work within the language of the statute. Moreover, in administering the application fee authority, we are also mindful of other general limits of fee authority. While the Independent Offices Appropriation Act of 1952 (IOAA) no longer applies to the Commission, we are nevertheless cognizant of broader legal issues raised by user fee and/or regulatory fee precedent.

We tentatively conclude that submissions to the Robocall Mitigation Database are ''applications'' within the meaning of the RAY BAUM's Act. The Commission has broadly construed the term ''applications'' to apply to a wide range of submissions for which filing fees are required, including tariff filings containing the rates, terms, and conditions of certain services provided by telecommunications providers. Following a period of public notice, a tariff filing is deemed accepted unless the Commission takes action, which can include suspension or rejection of the tariff filing by staff. We believe this process is analogous to Robocall Mitigation Database filings, which are accepted upon submission but may be subject to further action by the Commission, including removal from the Robocall Mitigation Database for failure to cure any identified deficiencies. Additionally, the application fee proposed here in some ways mirrors the fee charged for filing formal complaints and pole attachment complaints. In calculating the fee for such complaints, the Commission noted that staff must still review the complaint after its receipt ''for general conformance with the Commission's complaint rules to determine if it is accepted for adjudication.'' In response to a commenter's argument that the fee for formal complaints should be lower, the Commission explained that the fee being assessed also covers ''the costs of adjudicating such complaints.'' Thus, even after a complaint is filed and ''a letter to the parties [is sent] indicating that the filing has been accepted or rejected,'' Commission staff—like here—must still engage in a lengthy review process thereafter that involves ''significant work'' in order to adjudicate, *i.e.,* process, the complaint. We thus believe that Robocall Mitigation Database filings may be deemed applications for the purposes of requiring a filing fee, and seek comment on this view. We note that in the *2020 Application Fee Report and Order* (86 FR 15026, March 19, 2021), the Commission recognized that, as a result of the changes it made then and ''those made previously to implement the RAY BAUM's Act . . . with respect to regulatory fees,'' further revisions to the part 1, subpart G, Schedule of Statutory Charges and Procedures for Payment, may be required. Since the creation of the Robocall Mitigation Database, which occurred after the adoption of the *Application Fee NPRM* (85 FR 65566, October 15, 2020), the Commission has gained a fuller understanding of the costs involved in processing submissions thereto, and now proposes a filing fee consistent with those costs.

Further, the Commission's review of Robocall Mitigation Database submissions requires a significant investment of labor hours that continues to increase. The original requirement for voice service providers to file certifications and robocall mitigation plans in the Robocall Mitigation Database resulted in more than 2,600 submissions. As noted above, the Commission has since expanded the scope of providers required to file in the Database and the information that must be filed. As a result, there are currently approximately 9,000 filings in the Robocall Mitigation Database, each

comprising not only a certification form, but also a robocall mitigation plan that details the specific steps the provider is taking to mitigate illegal robocall traffic.

Each of those submissions must be reviewed by Commission staff to determine if they comply with the requirements of the Commission's caller ID authentication and robocall mitigation rules. 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 deficient filings to the Enforcement Bureau. We estimate that this process involves $100 per filing in costs. The Bureau estimates that each filing will require 40 minutes of analyst review at the GS–12 level; 20 minutes of attorney review at the GS–14 level; and 15 minutes of attorney supervisory review at the GS–15 level. The estimated total labor costs (including 20% overhead) for the analyst review (GS–12, step 5) of each filing is $43 (0.66 hours * $64.64 = $43). The estimated labor costs (including 20% overhead) for the attorney review (GS–14, step 5) for each filing is $32.95 (0.33 hours * $98.84 = $32.95). The estimated total labor costs (including 20% overhead) for the attorney supervisory review (GS–15, step 5) for each filing is $26.71 (0.25 hours * $106.85 = $26.71). The total labor costs per filing review is $102.66 ($43 + $32.95 + $26.71). Salary data is sourced from the Office of Personnel Management and include overhead costs based on 2,087 annual hours. Based on these hourly rates and the estimated time for processing each filing, the Bureau proposes that the filing fee is $100 per filing, and we seek comment on this determination. We therefore propose to add ''Robocall Mitigation Database Certification'' as a service requiring an application fee in § 1.1105 of the Commission's rules, and to set that application fee based on this cost estimate. We seek comment on whether it is appropriate for the Commission to assess an application fee for Robocall Mitigation Database submissions based on these costs, and if not, the scope of costs that should serve as the basis for the fee, if any. In so doing, we remind commenters that our section 8 authority is distinct from the Commission's authority with respect to other collections. In particular, the Commission is required by Congress to assess and collect as an offsetting collection regulatory fees each year in an amount that can reasonably be expected to equal the amount of the Commission's Salaries and Expenses (S&E) annual appropriation. The Commission is also directed by Congress to recover, as an offsetting collection, against auction proceeds costs incurred, subject to an annual cap, in developing and implementing our section 309(j) spectrum auctions program. Both such collections are deposited with the U.S. Treasury and credited to the Commission's account. For more information about the Commission's collections and budgetary authority, the Commission's annual financial statement and budget estimates for Congress provide helpful material. Application fees collected by the Commission are deposited in the general fund of the U.S. Treasury. Thus, while the determination of the fee amount will be based on cost, the collected fees are not used to fund Commission activities. In crafting comments, we ask that commenters explain whether their proposals are supported by the statute.

In addition, although not a basis for proposing a fee for Robocall Mitigation Database filings, we believe that requiring providers to submit a fee may have collateral public interest benefits, including (1) discouraging filings by bad actors by requiring them to use a traceable payment method; and (2) incentivizing better filings by requiring entities to incur a nominal expense upon filing or refiling, should they be removed from the Database for noncompliance. We seek comment on these beliefs.

We seek comment on when the Commission should collect the fee. Should they be collected only with initial filings or also when filings are updated, given that Commission staff will need to re-review the updated filings? We note that currently, there is no requirement that providers refile in the Database, outside of a change in the underlying information contained in the filing, or a change in the Commission's Robocall Mitigation Database filing requirements necessitating providers to resubmit their filings. Should the fee be collected from existing filers, and if so, under what circumstances—*e.g.,* when a provider refiles to update their information? Should the fee be collected if a provider refiles after being removed from the Robocall Mitigation Database pursuant to an enforcement action? Would assessing a refiling fee deter providers, particularly smaller providers, from updating their policies and procedures? We seek comment on these and any other procedural matters relevant to the collection of a filing fee for the Robocall Mitigation Database.

Red-Light Rule. Finally, we seek comment on whether to apply the Commission's ''red-light'' rule to Robocall Mitigation Database filings. Under the red-light rule, the Commission will not process applications and other requests for benefits by parties that owe non-tax debt to the Commission. In the context of our rules implementing the Debt Collection Improvement Act, the Commission has noted some filings with the Commission go into effect immediately ''thus precluding a check to determine if the filer is a delinquent debtor before the request goes into effect.'' In such situations, the Commission has the ability to take appropriate action after the fact for noncompliance with any of the Commission's rules. In the context of filings to the Commission's Intermediate Provider Registry, which similarly ''make[s] registrations immediately effective upon receipt,'' the Commission determined that ''any applicable red-light check will be conducted after intermediate provider registration; appropriate action, if any, will be taken against intermediate providers who are later discovered to be delinquent debtors, including de-registration.'' We seek comment on whether to apply such an approach to Robocall Mitigation Database filings, and on any alternative approaches to conducting a red-light check for Database filers.

2. Availability and Use of Data Validation Tools

We seek comment on technological and marketplace innovations that the Commission could employ to validate data entered into Robocall Mitigation Database filings and require filers to take a more proactive role in ensuring that accurate and complete information is submitted to the Database in the first instance. Specifically, we seek comment on software and other technical solutions that would cross-reference addresses and other contact details submitted by filers against other data sources and flag actual or potential discrepancies for filers to resolve. What tools could be used to cross-reference data entered into Robocall Mitigation Database certifications against reliable external sources and flag discrepancies, such as confirming the validity of address information submitted to the RMD against a United States Postal Service (USPS) database? For example, the USPS offers several web-based tools including an API for ''Address Validation/Standardization.'' How do the tools work and how have they been integrated into systems to prompt users to confirm the validity of the

information being entered into the system and correct any errors? What are the costs of integrating such tools into a system, and what are the technical and legal requirements for doing so? For example, we note that establishing a ''matching program'' with another Federal or non-Federal entity requires entering into a written matching agreement under the computer matching provisions of the Privacy Act of 1974. However, we tentatively conclude that the validation of filers to the Robocall Mitigation Database would not qualify as a matching program since the purpose of such validation does not relate to Federal benefits programs. We seek comment on this tentative conclusion. Would integrating such tools into the Robocall Mitigation Database raise any legal, privacy, or policy concerns? We note, for instance, that the applicable system of records notice permits disclosures, as a routine use, to non-Federal personnel, including contractors and other vendors, and specifically ''identity verification service[ ]'' providers. While information submitted by providers to the Robocall Mitigation Database is generally public, providers may request confidential treatment of information included in their robocall mitigation plans. Would allowing a data validation tool to cross-reference data from Robocall Mitigation Database filings against an external data source raise concerns about protecting confidential or proprietary information? Are there ways to mitigate any such concerns?

We seek comment on whether the Commission should prevent a filing from being submitted to the Robocall Mitigation Database if any technical validation tools employed flag a data discrepancy and the filer fails to resolve that discrepancy. For example, if the Commission were to employ a technical solution for verifying all or part of an address, and the provider does not or cannot submit an address that can be validated by the solution, should the filing be provisionally rejected until the provider finds a way to resolve the discrepancy? Or, should the filing be accepted by the system but flagged as an internal warning to the Commission that the filing should be prioritized for compliance review and enforcement? Is there a middle ground that would allow the system to hold the filing containing the unvalidated address while the provider seeks to resolve the discrepancy through other means with Commission staff, *e.g.,* through the manual submission of documents that corroborate the submitted address? We seek comment on the benefits and burdens of employing a technical approach to Robocall Mitigation Database data validation, and on how the Commission should seek to integrate such tools into its review of Robocall Mitigation Database filings.

B. Increased Consequences for Submitting False or Inaccurate Information to the Robocall Mitigation Database

1. Establishing Forfeiture for Submitting Inaccurate or False Certification Data

We propose to establish a separate base forfeiture amount for submitting false or inaccurate information to the Robocall Mitigation Database. In the *Sixth Caller ID Authentication Report and Order* (88 FR 40096, June 21, 2023), the Commission found that Robocall Mitigation Database filings are Commission authorizations. The Commission may impose a forfeiture against any person found to have willfully or repeatedly failed to comply substantially with the terms and conditions of any authorization issued by the Commission. In the *Fifth Caller ID Authentication Further Notice of Proposed Rulemaking (FNPRM)* (87 FR 42670, July 18, 2022), the Commission proposed to ''impose the highest available forfeiture for failures to appropriately certify in the Robocall Mitigation Database.'' We now propose a base forfeiture of $10,000 for each violation for filers that submit false or inaccurate information to the Robocall Mitigation Database. The Commission has set the base forfeiture for failure to file required forms or information at $3,000. We tentatively conclude that submitting false or inaccurate information to the RMD warrants a significantly higher penalty, and seek comment on this tentative conclusion. What are the benefits to this approach? Would a higher or lower base forfeiture amount be more appropriate? Alternatively, we propose to impose the statutory maximum forfeiture amount allowable under section 503 of the Communications Act for submitting false or inaccurate information to the Robocall Mitigation Database. The Commission has set the statutory maximum as the base forfeiture for violations of § 1.17 of our rules related to misrepresentation and lack of candor in investigatory or adjudicatory matters. Is submitting false or inaccurate information to the RMD similar to the Commission's misrepresentation and lack of candor rules to justify the highest possible penalty? What are the benefits and drawbacks to this alternative approach? We seek comment on these proposals.

For either proposal, should we consider each instance of false or inaccurate information a single violation or a continuing violation for each day the false information remains in the Robocall Mitigation Database? Are there particular aggravating or mitigating factors we should take into consideration when determining the amount of a forfeiture penalty? Or are the aggravating and mitigating factors set forth in our rules sufficient? Should we use the same maximum forfeiture regardless of whether the violator is a common carrier or not? Currently, common carriers may be assessed a maximum forfeiture of $2,449,575 for a continuing violation, while entities not explicitly mentioned in section 503 of the Communications Act may only be assessed a maximum forfeiture of $183,718 for a continuing violation. In the *Sixth Caller ID Authentication Report and Order,* the Commission found it should not impose a higher maximum penalty on common carriers for violations of the mandatory blocking rules. Should we take a similar approach here? Are there any practical or legal considerations? We seek comment on these proposals.

Finally, we propose to find that we can impose a forfeiture on filers that fail to update information that has changed in the Robocall Mitigation Database within 10 business days. All filers in the Robocall Mitigation Database are required to update their filings within 10 business days if any information they are required to submit has changed. We propose a base forfeiture of $1,000 for failure to update information within 10 business days. We propose treating it as a continuing violation for every day the inaccurate information remains in the Robocall Mitigation Database, with a maximum forfeiture of $24,496 for each day of the continuing violation up to the statutory maximum of $183,718. We seek comment on these proposals. Should we establish separate base and maximum forfeiture amounts for failing to update a filing within 10 business days? Should the violation be a single violation or a continuing violation for each day the non-updated information remains in the Robocall Mitigation Database? If it is a continuing violation, what should the maximum forfeiture for the continuing violation be?

2. Authorizing Permissive Blocking for Facially Deficient Filings

We next propose to authorize downstream providers to permissively block traffic by Robocall Mitigation Database filers that have been given notice that their robocall mitigation plans are facially deficient and that fail

to correct those deficiencies within 48 hours. We seek comment on this proposal.

The Commission's rules currently require downstream providers to refuse traffic from providers that are not in the Robocall Mitigation Database. This means that when a provider is removed from the Database, it is effectively precluded from operating as a provider of voice services in the United States. For this reason, the Commission has recognized that removal of Robocall Mitigation Database submissions has severe consequences and is arguably equivalent to revoking a license, and thus has adopted notice and opportunity to cure procedures before removal of filings from the Robocall Mitigation Database consistent with the Administrative Procedure Act (APA). For most filing deficiencies, the Commission follows a three-step process for removal, whereby:

(1) the Wireline Competition Bureau contacts the provider, notifying it that its filing is deficient, explaining the nature of the deficiency, and providing 14 days for the provider to cure the deficiency; (2) if the provider fails to rectify the deficiency, the Enforcement Bureau releases an order concluding that a provider's filing is deficient based on the available evidence and directing the provider to explain, within 14 days, 'why the Enforcement Bureau should not remove the Company's certification from the Robocall Mitigation Database' and giving the provider a further opportunity to cure the deficiencies in its filing; and (3) if the provider fails to rectify the deficiency or provide a sufficient explanation why its filing is not deficient within that 14-day period, the Enforcement Bureau releases an order removing the provider from the Robocall Mitigation Database.

In the *Sixth Caller ID Authentication Report and Order,* however, the Commission recognized that the failure to submit a robocall mitigation plan within the meaning of our rules constitutes a facial deficiency that warrants an expedited removal process. A robocall mitigation plan is facially deficient if it fails to submit any information regarding the ''specific reasonable steps'' the provider is taking to mitigate illegal robocalls. In such cases, the Commission found that providers have ''willfully'' violated its Robocall Mitigation Database filing rules and an expedited removal process is therefore warranted. Under this two-step expedited procedure for removing a facially deficient certification, the Enforcement Bureau will: (1) issue a notice to the provider explaining the basis for its conclusion that the certification is facially deficient and providing an opportunity for the provider to cure the deficiency or explain why its certification is not deficient within 10 days; and (2) if the deficiency is not cured or the provider fails to establish that there is no deficiency within that 10-day period, issue an order removing the provider from the Database.

We seek comment on whether the Commission should adopt additional measures to protect consumers where submissions to the Robocall Mitigation Database demonstrate willful violations of the Commission's rules. Specifically, we propose to allow downstream providers to permissively block traffic from providers that have submitted facially deficient robocall mitigation plans beginning 48 hours after the agency issues the notice of facial deficiency and continuing until either the deficiency is cured or the provider's certification is removed from the Robocall Mitigation Database, which would trigger the mandatory blocking requirement. We propose to do so through a three step process: (1) a notice would be issued to the provider that its robocall mitigation plan is facially deficient because it fails to describe the specific reasonable steps that the provider is taking to avoid carrying and transmitting illegal robocalls; (2) the provider would be allowed 48 hours to cure this facial deficiency by uploading a robocall mitigation plan that sufficiently describes its mitigation practices; and (3) if it fails to do so, the Wireline Competition Bureau would apply a flag to the facially deficient filing in the Robocall Mitigation Database to inform other providers that they may permissively block traffic from that provider after providing notice to the Commission that they intend to do so.

We view this process to be similar to that authorized when the Commission sends cease-and-desist letters pursuant to § 64.1200(k)(4) of our rules, which states that a provider may, without liability, block voice calls or traffic from an originating or intermediate provider that has been notified by the Commission but fails to take steps to mitigate or prevent its network from being used to originate illegal calls. Under this rule, a provider must, prior to initiating blocking, provide the Commission with notice and a brief summary of the basis for its determination that the originating or intermediate provider has met one of these two conditions for blocking.

In the context of the Robocall Mitigation Database, the flag applied to the filing would constitute notice that the provider has failed to remedy a facial deficiency in its filing within 48 hours and that downstream providers may block traffic from that provider if they submit a notice to the Commission that they intend to do so for the reason stated in the notice. We believe that there are equivalencies between the context in which the Commission issues cease-and-desist letters pursuant to § 64.1200(k)(4) of the Commission's rules and a willful failure to submit the required description of a provider's robocall mitigation practices in the Robocall Mitigation Plan. We seek comment on this belief. In the former, the Enforcement Bureau has found evidence that the provider has originated or transmitted illegal robocalls (*e.g.,* traceback data). The willful violation of the Commission's rules requiring providers to describe the steps they are taking to avoid carrying and transmitting illegal robocalls supports a presumption that no such steps are being taken and that the provider is doing nothing to stop illegal traffic as required by our rules.

We seek comment on this view and whether applying the three-step process for permissive blocking proposed above in the context of facially deficient Robocall Mitigation Database filings is warranted. Are there considerations that apply when the Commission issues cease-and-desist letters pursuant to § 64.1200(k)(4) of the Commission's rules that do not apply in the context of the Robocall Mitigation Database? For instance, is it significant that in the context of § 64.1200(k)(4) cease-and-desist letters, the Enforcement Bureau has evidence that illegal robocalls have actually been transmitted, whereas here, the evidence would be that the provider has willfully failed to describe the reasonable steps it is taking to mitigate illegal traffic? If commenters argue that is not a sufficient showing to authorize permissive blocking from a provider that has willfully violated the Commission's robocall mitigation rules, what showing would be sufficient to authorize permissive blocking, if any?

Is 48 hours an appropriate amount of time to allow a provider with a facially deficient plan to cure the deficiency to avoid permissive blocking, or should more or less time be allowed prior to opening the window for permissive blocking? Should the new rule include a safe harbor from liability under the Communications Act or the Commission's rules for providers that engage in permissive blocking under this new rule if they notify the Commission that they intend to do so, as under § 64.1200(k)(4)? What information should be included in a notice to the Commission that a provider intends to permissively block traffic from another provider? Should

they simply state that they intend to block traffic from the provider that has been flagged by the Commission due to its facially deficient robocall mitigation plan, or should additional information be required? Should the new rule also address situations where the facial deficiency is cured after the Wireline Competition Bureau applies a flag? In such situations, we propose that the Wireline Competition Bureau would take down the flag applied to the Robocall Mitigation Database filing and notify any providers that have commenced permissive blocking to cease such blocking. We seek comment on this approach and whether our rules should require providers to cease permissive blocking within a specified period of time. If so, what is an appropriate timeframe?

What are the risks to legitimate providers, and their customers, of authorizing permissive blocking in the context of facially deficient robocall mitigation plans submitted to the Robocall Mitigation Database, and do those risks outweigh the public interest benefits of enabling providers to decline traffic from providers that have demonstrated a willful disregard for their duty to mitigate illegal robocalls without penalty under our rules? What are the costs of authorizing permissive blocking in this context, and do the public interest benefits outweigh those costs? To the extent commenters argue that the risks and costs of the proposed permissive blocking process are high, is there a way to modify the process to minimize those risks and costs, or to otherwise improve it in a manner that appropriately balances the public interest objective of protecting consumers from illegal traffic against potential burdens to legitimate providers? We invite comment on these or any other points the Commission should consider when assessing the merits of our permissive blocking proposal.

Scope of Facial Deficiencies. As stated above, we propose to limit any permissive blocking measure to circumstances where the robocall mitigation plan submitted to the Robocall Mitigation Database is facially deficient, versus circumstances that require the Commission to make a qualitative judgment about the sufficiency of the measures described in the plan. In the *Sixth Caller ID Authentication Report and Order,* the Commission found it was ''not practical to provide an exhaustive list of reasons why a filing would be considered 'facially deficient,' '' but provided several examples, including ''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 [FRN] 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.'' We seek comment on whether there are additional examples of robocall mitigation plan deficiencies that would rise to the level of willful violations of the Commission's robocall mitigation rules within the meaning of section 9(b) of the APA. While the Commission has not set a particular format or minimum requirements for robocall mitigation plans, understanding the value of allowing providers flexibility to develop robocall mitigation programs that are specific to their networks, are there factors short of a complete failure to describe a provider's specific robocall mitigation practices that could render a mitigation plan facially deficient? For instance, are there any omissions that should universally render any robocall mitigation plan filed by any provider deficient, such that the Commission should adopt a standard that a failure to address that subject constitutes a willful violation of our rules? Is there a level of brevity that clearly falls below the requirement to describe *specific* reasonable steps being taken by the provider? While we do not intend to define a specific standard for facial deficiency, we do seek comment on whether there are any other bright line circumstances to which the standard should be applied generally and for the purposes of the permissive blocking process proposed above.

Delegation of Authority. Should the Commission authorize permissive blocking when a provider submits a facially deficient robocall mitigation plan to the Robocall Mitigation Database, we propose to delegate authority to the Wireline Competition Bureau to design the permissive blocking system, including the process for issuing notifications to providers that their robocall mitigation plan is facially deficient, the contents of that notice, the procedures for allowing the providers to remedy the deficiency by uploading a robocall mitigation plan that describes their robocall mitigation practices, the mechanism for applying a flag to the Robocall Mitigation Database filing of any provider that fails to do so within 48 hours, the process for collecting notifications from downstream providers that they intend to block traffic from the flagged provider, the content requirements for such notifications, and the process for removing a flag and notifying blocking providers in the event that a provider cures its facially deficient filing after a flag has been applied. We propose to delegate authority to the Wireline Competition Bureau to make any necessary changes to the Robocall Mitigation Database to implement these processes and direct the Bureau to release a public notice providing updated instructions and training materials regarding any relevant changes to the Database. We seek comment on this approach.

IV. Legal Authority

We propose to adopt the foregoing obligations in part pursuant to the legal authority relied upon by the Commission in prior caller ID authentication and call blocking orders. We propose to rely upon sections 201(b), 202(a), and 251(e) of the Act, the Truth in Caller ID Act, and section 4 of the TRACED Act to authorize downstream providers to permissively block traffic by facially deficient Robocall Mitigation Database filers that have failed to correct those deficiencies within 48 hours after notice, and to require corporate officers to obtain a PIN before filing in the Robocall Mitigation Database.

We propose to rely on sections 501, 502, and 503 of the Act to establish forfeiture amounts for submitting inaccurate or false certification data to the Robocall Mitigation Database. We propose to rely on our authority under section 8 of the Act to add Robocall Mitigation Database filings to the Commission's Schedule of Application Fees. We believe the Commission has ample authority to adopt the foregoing obligations related to the Robocall Mitigation Database, as well as any related administrative enhancements pertaining to CORES. We seek comment on this view and whether there are any alternative sources of authority that we should consider.

Digital Equity and Inclusion. The Commission, as part of its continuing effort to advance digital equity for all, including people of color and others who have been historically underserved, marginalized, and adversely affected by persistent poverty and inequality, invites comment on any equity-related considerations and benefits (if any) that may be associated with the proposals and issues discussed herein. We define the term ''equity'' consistent with

Executive Order 13985 as the consistent and systematic fair, just, and impartial treatment of all individuals, including individuals who belong to underserved communities that have been denied such treatment, such as Black, Latino, and Indigenous and Native American persons, Asian Americans and Pacific Islanders and other persons of color; members of religious minorities; lesbian, gay, bisexual, transgender, and queer (LGBTQ+) persons; persons with disabilities; persons who live in rural areas; and persons otherwise adversely affected by persistent poverty or inequality. Specifically, we seek comment on how our proposals may promote or inhibit advances in diversity, equity, inclusion, and accessibility.

V. Procedural Matters

Regulatory Flexibility Act. The Regulatory Flexibility Act of 1980, as amended (RFA), requires that an agency prepare a regulatory flexibility analysis for notice and comment rulemakings, unless the agency certifies that ''the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities.'' Accordingly, the Commission has prepared an Initial Regulatory Flexibility Analysis (IRFA) concerning the possible/potential impact of the rule and policy changes contained in the *NPRM.* The IRFA is set forth in this document.

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 possible significant economic impact on a substantial number of small entities from the policies and rules proposed in the *NPRM.* Written public comments are requested on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments provided on the first page of the *NPRM.* The Commission will send a copy of the *NPRM,* including the IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA). In addition, the *NPRM* and IRFA (or summaries thereof) will be published in the **Federal Register**.

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

In order to continue the Commission's work of protecting American consumers from illegal calls, the *NPRM* seeks comment on ways to ensure and improve the overall quality of submissions to the Robocall Mitigation Database (RMD). In its review of filings by providers in the RMD, the Commission staff noted a lack of information ranging from a failure to provide accurate contact information for employees responsible for completing certifications of robocall mitigation practices, to failing to submit robocall mitigation plans with sufficient detail. The *NPRM* proposes and seeks comment on measures to increase accountability for providers that submit inaccurate and false information to the RMD and fail to update their filings when the information they contain changes, as required by the Commission's rules. The *NPRM* also invites comment on any other procedural steps the Commission could require to increase the RMD's effectiveness as a compliance and consumer protection tool.

B. Legal Basis

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

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

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

Small Businesses, Small Organizations, Small Governmental Jurisdictions. Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe, at the outset, three broad groups of small entities that could be directly affected herein. First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, according to data from the SBA's Office of Advocacy, in general a small business is an independent business having fewer than 500 employees. These types of small businesses represent 99.9% of all businesses in the United States, which translates to 33.2 million businesses.

Next, the type of small entity described as a ''small organization'' is generally ''any not-for-profit enterprise which is independently owned and operated and is not dominant in its field.'' The Internal Revenue Service (IRS) uses a revenue benchmark of $50,000 or less to delineate its annual electronic filing requirements for small exempt organizations. Nationwide, for tax year 2022, there were approximately 530,109 small exempt organizations in the U.S. reporting revenues of $50,000 or less according to the registration and tax data for exempt organizations available from the IRS.

Finally, the small entity described as a ''small governmental jurisdiction'' is defined generally as ''governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of less than fifty thousand.'' U.S. Census Bureau data from the 2022 Census of Governments indicate there were 90,837 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States. Of this number, there were 36,845 general purpose governments (county, municipal, and town or township) with populations of less than 50,000 and 11,879 special purpose governments (independent school districts) with enrollment populations of less than 50,000. Accordingly, based on the 2022 U.S. Census of Governments data, we estimate that at least 48,724 entities fall into the category of ''small governmental jurisdictions.''

Wired Telecommunications Carriers. The U.S. Census Bureau defines this industry as establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including voice over internet protocol (VoIP) services, wired (cable) audio and video programming distribution, and wired broadband internet services. By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry. Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.

The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 4,590 providers that reported they were engaged in the provision of fixed local services. Of these providers, the Commission estimates that 4,146 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

Local Exchange Carriers (LECs). Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. Providers of these services include both incumbent and competitive local exchange service providers. Wired Telecommunications Carriers is the closest industry with an SBA small business size standard. Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 4,590 providers that reported they were fixed local exchange service providers. Of these providers, the Commission estimates that 4,146 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

Incumbent Local Exchange Carriers (Incumbent LECs). Neither the Commission nor the SBA have developed a small business size standard specifically for incumbent local exchange carriers. Wired Telecommunications Carriers is the closest industry with an SBA small business size standard. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms in this industry that operated for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 1,212 providers that reported they were incumbent local exchange service providers. Of these providers, the Commission estimates that 916 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, the Commission estimates that the majority of incumbent local exchange carriers can be considered small entities.

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

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

Cable System Operators (Telecom Act Standard). The Communications Act of 1934, as amended, contains a size standard for a ''small cable operator,'' which is ''a cable operator that, directly or through an affiliate, serves in the aggregate fewer than one percent of all subscribers in the United States and is not affiliated with any entity or entities whose gross annual revenues in the aggregate exceed $250,000,000.'' For purposes of the Telecom Act Standard, the Commission determined that a cable system operator that serves fewer than 498,000 subscribers, either directly or through affiliates, will meet the definition of a small cable operator. Based on industry data, only six cable system operators have more than 498,000 subscribers. Accordingly, the Commission estimates that the majority of cable system operators are small under this size standard. We note however, that the Commission neither requests nor collects information on whether cable system operators are affiliated with entities whose gross annual revenues exceed $250 million. Therefore, we are unable at this time to estimate with greater precision the number of cable system operators that would qualify as small cable operators under the definition in the Communications Act.

Other Toll Carriers. Neither the Commission nor the SBA has developed a definition for small businesses specifically applicable to Other Toll Carriers. This category includes toll carriers that do not fall within the categories of interexchange carriers, operator service providers, prepaid calling card providers, satellite service carriers, or toll resellers. Wired Telecommunications Carriers is the closest industry with an SBA small business size standard. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small. U.S. Census Bureau data for 2017 show that there were 3,054 firms in this industry that operated for the entire year. Of this number, 2,964 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 90 providers that reported they were

engaged in the provision of other toll services. Of these providers, the Commission estimates that 87 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

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

Satellite Telecommunications. This industry comprises firms ''primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications.'' Satellite telecommunications service providers include satellite and earth station operators. The SBA small business size standard for this industry classifies a business with $38.5 million or less in annual receipts as small. U.S. Census Bureau data for 2017 show that 275 firms in this industry operated for the entire year. Of this number, 242 firms had revenue of less than $25 million. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 65 providers that reported they were engaged in the provision of satellite telecommunications services. Of these providers, the Commission estimates that approximately 42 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, a little more than half of these providers can be considered small entities.

Local Resellers. Neither the Commission nor the SBA have developed a small business size standard specifically for Local Resellers. Telecommunications Resellers is the closest industry with an SBA small business size standard. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. Mobile virtual network operators (MVNOs) are included in this industry. The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year. Of that number, 1,375 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 207 providers that reported they were engaged in the provision of local resale services. Of these providers, the Commission estimates that 202 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

Toll Resellers. Neither the Commission nor the SBA have developed a small business size standard specifically for Toll Resellers. Telecommunications Resellers is the closest industry with an SBA small business size standard. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. MVNOs are included in this industry. The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year. Of that number, 1,375 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 457 providers that reported they were engaged in the provision of toll services. Of these providers, the Commission estimates that 438 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

Prepaid Calling Card Providers. Neither the Commission nor the SBA has developed a small business size standard specifically for prepaid calling card providers. Telecommunications Resellers is the closest industry with an SBA small business size standard. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. MVNOs are included in this industry. The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year. Of that number, 1,375 firms operated with fewer than 250 employees. Additionally, based on Commission data in the 2022 Universal Service Monitoring Report, as of December 31, 2021, there were 62 providers that reported they were engaged in the provision of prepaid card services. Of these providers, the Commission estimates that 61 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

All Other Telecommunications. This industry is comprised of establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation. This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving

telecommunications from, satellite systems. Providers of internet services (*e.g.,* dial-up ISPs) or VoIP services, via client-supplied telecommunications connections are also included in this industry. The SBA small business size standard for this industry classifies firms with annual receipts of $35 million or less as small. U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year. Of those firms, 1,039 had revenue of less than $25 million. Based on this data, the Commission estimates that the majority of ''All Other Telecommunications'' firms can be considered small.

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

In the *NPRM,* the Commission proposes and seeks comment on imposing several reporting, recordkeeping, and compliance obligations on various providers, many of whom may be small entities. Specifically, the *NPRM* proposes to require all entities and individuals that file in the Commission Registration System (CORES) to update any information required by the system within 10 business days of any changes.

With respect to the RMD, the *NPRM* seeks comment on whether to deploy multi-factor authentication functionality and whether to require providers to use such technology in order to submit a filing to the Database. In addition, or as an alternative to multi-factor authentication, the *NPRM* seeks comment on requiring an officer, owner, or other principal of a provider to obtain a PIN that must be entered before an RMD submission is accepted by the filing system. In particular, we seek comment on whether the Commission should require the signing officer to submit additional information to obtain a PIN that must be used to submit an RMD certification, including: (1) a non-P.O. box street address and telephone number for the location of the office where the officer does business, and a direct business email address for the officer; (2) a business address, telephone number, and email address for the provider's registered agent for service of process (or a certification that such an agent does not exist); and (3) certifications, under penalty of perjury pursuant to 47 CFR 1.16 of the Commission's rules. The *NPRM* also seeks comment on the method by which the Commission could collect this information and generate the PIN for use by the officer when submitting an RMD filing. The *NPRM* seeks comment on whether to require providers to pay a fee when submitting filings to the RMD, and seeks comment on when the Commission should collect the fee. In addition, the *NPRM* seeks comment on technological innovations that the Commission could employ to validate data entered into RMD filings, specifically, on software and other technical solutions that would cross-reference addresses and other contact details submitted by filers against other data sources, and flag actual or potential discrepancies for filers to resolve before the filing is submitted to the Commission.

With regard to our enforcement of these proposed rules, the *NPRM* seeks comment on whether to establish a base and/or maximum forfeiture for submitting inaccurate or false information to the RMD, and failing to update information that has changed in the within 10 business days. The *NPRM* also seeks comment on what an appropriate forfeiture would be when a provider submits inaccurate or false information to the RMD, and in what circumstances this forfeiture would apply. Specifically, we propose to use the current statutory maximum of $24,496 listed in section 503(b)(2)(D) of the Act as the base forfeiture amount regardless of the type of service provided by the filer for submitting false or inaccurate information to the Robocall Mitigation Database. Additionally, the *NPRM* proposes a base forfeiture of $5,000 for failure to update information within 10 days, and further proposes treating this as a continuing violation for every day the inaccurate information remains in the RMD, up to the statutory maximum of $183,718.

The *NPRM* proposes to authorize downstream providers to permissively block traffic by RMD filers that have been given notice that their robocall mitigation plans are facially deficient and that fail to correct those deficiencies within 48 hours. The proposed blocking would occur through a three step process: (1) a notice issued to the provider through the RMD that their robocall mitigation plan is facially deficient because it fails to describe the specific reasonable steps that the provider is taking to avoid carrying and transmitting illegal robocalls; (2) allowing the provider 48-hours to cure this facial deficiency by uploading a robocall mitigation plan that sufficiently describes its mitigation practices; and (3) if it fails to do so, having a flag applied to the facially deficient filing in the RMD advising other providers that they may permissively block traffic from that provider upon providing notice to the Commission that they intend to do so. The *NPRM* seeks comment on whether there are additional examples of robocall mitigation plan deficiencies that would rise to the level of willful violations of the Commission's robocall mitigation rules.

We anticipate the information we receive in comments including where requested, cost and benefit analyses, will help the Commission identify and evaluate relevant compliance matters for small entities, including compliance costs and other burdens that may result from the proposals and inquiries we make in the *NPRM.* With respect to costs for filing fees, we seek comment on a fee schedule based on the cost of processing applications, with cost determined by the Commission's direct labor costs. We also believe that some proposals, such as the requirement that providers update any information submitted to CORES within 10 business days of any changes to that information, may not impose significant costs on small entities because Commission databases beyond the RMD similarly make use of contact information imported directly from CORES. We seek comment from small and other entities on that perspective.

E. Steps Taken To Minimize the Significant Economic Impact on Small Entities, and Significant Alternatives Considered

The RFA requires an agency to describe any significant alternatives that could minimize impacts to small entities that it has considered in reaching its proposed approach, which may include the following four alternatives (among others): (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 rules for such small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof, for such small entities.

The *NPRM* seeks comment on proposals and alternatives that may have a significant impact on small entities. In particular, it seeks comment on the benefits and burdens of requiring all entities and individuals that file in CORES, including small entities, to update any information required by the system within 10 business days of any changes. The *NPRM* seeks comment on the benefits and burdens associated with various procedural and technical solutions to improve the quality of RMD filings, including: (1) deploying multi-factor authentication functionality for

the RMD; (2) requiring an officer to obtain a PIN in order to submit an RMD filing; and (3) employing a technical approach to RMD data validation, and any alternatives that might mitigate those burdens for RMD filers, including small entities. The *NPRM* also seeks comment on fees for future RMD filings, and seeks comment on whether these fees should be collected from existing filers.

In proposing to establish the statutory maximum as the base forfeiture amount for submitting false or inaccurate information to the RMD, the *NPRM* seeks comment on whether a lower base forfeiture amount would be more appropriate. Further, it also seeks comment on whether there are particular mitigating factors the Commission should take into consideration when determining the amount of the forfeiture penalty, and proposes to find that the Commission should not impose a higher penalty on common carriers, including those that are small entities. In proposing to find that the Commission can impose a forfeiture on filers that fail to update information that has changed in the RMD within 10 days, the *NPRM* seeks comment on whether to establish a base or maximum forfeiture, and whether the violation should be a single violation or continuing violation for each day the non-updated information remains in the RMD, which may have a particular impact on small entities. It also seeks comment on what the maximum forfeiture for a continuing violation should be.

In proposing to allow downstream providers to permissively block traffic from providers that have submitted facially deficient robocall mitigation plans, instead of instances where the Commission must make a qualitative judgement, the *NPRM* seeks comment on the risks and costs to legitimate providers, including small entities, of authorizing permissive blocking, and whether those risks and costs outweigh the public interest benefits. The *NPRM* also seeks comment on any alternative that may modify the process to minimize those risks and costs to legitimate providers, including small entities. The Commission expects to more fully consider the economic impact and alternatives for small entities following the review of comments filed in response to the *NPRM.*

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

None.

Federal Communications Commission.

Marlene Dortch,

Secretary.

[FR Doc. 2024–20176 Filed 9–11–24; 8:45 am]

BILLING CODE 6712–01–P