## FEDERAL COMMUNICATIONS COMMISSION

### 47 CFR Parts 0 and 64

**[CG Docket No. 17–59, WC Docket No. 17–97; FCC 22–37, FR ID 91946]**

## Advanced Methods To Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor

**AGENCY:** Federal Communications Commission.

**ACTION:** Final rule.

**SUMMARY:** In this document, the Federal Communications Commission (Commission or FCC) takes further steps to stem the tide of foreign-originated illegal robocalls by placing new obligations on the gateway providers that are the entry point or foreign calls into the United States by requiring them to play a more active role in the fight.

**DATES:**

*Effective date:* This rule is effective September 16, 2022.

*Compliance date:* Compliance with the amendments to 47 CFR 64.1200(n)(1) and (o), 64.6303(b), and 64.6305(b), (c)(2), (d), and (e)(2) and (3), are delayed indefinitely. The Federal Communications Commission will publish a document in the **Federal Register** announcing the compliance dates.

**ADDRESSES:** Federal Communications Commission, 45 L Street NE, Washington, DC 20554.

**FOR FURTHER INFORMATION CONTACT:** Jonathan Lechter, Competition Policy Division, Wireline Competition Bureau, at (202) 418–0984, *jonathan.lechter@fcc.gov*; or Jerusha Burnett, Attorney Advisor, Consumer Policy Division, Consumer and Governmental Affairs Bureau, at (202) 418–0526, *jerusha.burnett@fcc.gov*.

**SUPPLEMENTARY INFORMATION:** This is a summary of the Commission's *Sixth Report and Order* in CG Docket No. 17–59 and *Fifth Report and Order* in WC Docket No. 17–97 *Order on Reconsideration* and *Order* in WC Docket No. 17–97 adopted on May 19, 2022 and released on May 20, 2022 (*Gateway Provider Report and Order*). The document is available for download at *https://docs.fcc.gov/public/attachments/FCC-22-37A1.pdf*. Compliance with the amendments to 47 CFR 64.1200(n)(1) and (o), 64.6303(b), and 64.6305(b), (c)(2), and (d), which contain information collection requirements that have not been approved by the Office of Management and Budget (OMB), and the amendments to 47 CFR 64.6305(e)(2) and (3), are delayed indefinitely. The Federal Communications Commission will publish a document in the **Federal Register** announcing the compliance dates.

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), 202–418–0432 (TTY).

### Synopsis

### I. Sixth Report and Order and Fifth Report and Order

1. In this document, the Commission takes steps to protect consumers from foreign-originated illegal robocalls. Gateway providers' networks are the key entry point for foreign-originated robocalls, and the authentication and mitigation requirements the Commission adopts will ensure that American consumers are protected. The Commission defines the term ''gateway provider,'' requires such providers to authenticate all unauthenticated Session Initiation Protocol (SIP) calls in the internet Protocol (IP) portions of their networks, and adopts mitigation requirements specific to such providers, including requirements related to the Robocall Mitigation Database. As explained below, the Commission finds that the benefits of these new requirements, particularly to American consumers deluged by illegal calls originating in other countries, will far outweigh the short-term implementation costs imposed on gateway providers.

*A. Need for Action*

2. *Current Rules Addressing Foreign-Originated Robocalls Are Insufficient to Stop the Deluge of Illegal Robocalls Originating Abroad.* As proposed, the Commission concludes that consumers will benefit from caller ID authentication and illegal robocall mitigation requirements applied to gateway providers to address the problem of foreign-originated illegal robocalls (86 FR 59084, (Oct. 26, 2021)).

3. Commenters overwhelmingly support additional action to stop the flood of foreign-originated illegal calls. For example, Comcast agrees with the Commission that the current rules ''are not sufficient to resolve the problem of foreign-originated illegal robocalls'' and that the robocall landscape ''warrants consideration of further regulatory efforts targeting gateway providers.'' The State attorneys general also support steps to stop the ''continued deluge of illegal foreign-based robocalls that use spoofed, U.S.-based phone numbers.''

4. Foreign robocallers use U.S. North American Numbering Plan (NANP) numbers in myriad ways to reach U.S. end users. In some cases, the foreign robocallers utilize spoofed U.S. numbers, while in other cases they have obtained U.S. NANP numbers from providers who have themselves obtained numbers on the secondary market or directly from the North American Numbering Plan Administrator (NANPA).

5. Commenting parties agree that foreign-originated calls are a significant portion, if not the majority, of illegal robocalls. The latest data from the Industry Traceback Group support the conclusion that many providers facilitating illegal robocalls are gateway providers and the upstream foreign originating and intermediate providers from whom they receive foreign-originating calls. Of the 347 providers identified in the Industry Traceback Group's 2021 report as responsible for transmitting illegal robocalls, 111 were gateway providers that brought the traffic into the U.S. network, and 115 were foreign providers originating illegal robocalls. According to the Industry Traceback Group, 10% of all providers that are not responsive to traceback requests constitute 48% of all non-responsive traceback requests. Of that 10%, over two-thirds are foreign providers. Recent action after the release of the *Gateway Provider Further Notice of Proposed Rulemaking (Gateway Provider FNPRM),* 86 FR 59084, (Oct. 26, 2021), by the Commission's Enforcement Bureau underscores the need for action against foreign-originated robocalls, including cease-and-desist letters the Enforcement Bureau sent to three companies for transmitting illegal robocalls, ''many of which originate overseas.''

6. *Role of Gateway Providers.* The Commission concludes that gateway providers serve as a critical choke-point for reducing the number of illegal robocalls received by American consumers, a conclusion confirmed by the record. Gateway providers can stop illegal calls to customers before they reach terminating providers, or, as the Industry Traceback Group data demonstrates, readily allow such calls into the U.S. market. State attorneys general argue that ''in most cases'' robocalling fraud results from ''foreign actors gaining access to the U.S. phone network through international gateway providers.'' State actions against gateway providers following the *Gateway Provider FNPRM* reinforce this conclusion.

*B. Scope of Requirements and Definition*

7. *Definition of Gateway Provider.* The Commission defines a ''gateway provider'' as a U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider, a slightly modified version of the definition the Commission proposed in the *Gateway Provider FNPRM.* By ''U.S.-based,'' the Commission means that the provider has facilities located in the U.S., including a point of presence capable of processing the call. By ''receives a call directly'' from a provider, the Commission means the foreign provider directly upstream of the gateway provider in the call path sent the call to the gateway provider, with no providers in-between. Commenters support the Commission's proposed definition, with some suggesting minor modifications addressed below.

8. In the *Gateway Provider FNPRM,* the Commission initially proposed to define a gateway provider as ''the first U.S.-based intermediate provider in the call path of a foreign-originated call that transmits the call directly to another intermediate provider or a terminating voice service provider in the United States.'' The Commission adds ''receives a call directly from a foreign originating provider or foreign intermediate provider'' and drop ''foreign-originated call'' from its adopted definition for several reasons. First, as commenters note, a gateway provider may not know the identity or location of the entity that originated the call, but it will know the identity of the immediate upstream provider that sent the call to the gateway provider, including whether that provider has registered as a foreign provider in the Robocall Mitigation Database. (As explained below, the Commission clarifies foreign intermediate providers' traffic will be blocked unless they register in the Robocall Mitigation Database.) The Commission's adopted definition ensures that a provider will be considered a gateway provider for any call it receives directly from a foreign provider that the provider does not itself terminate. Second, the Commission's definition ensures that calls sent on a circuitous path out of and then back into the U.S. will be brought within the regime. In that scenario, the U.S.-based provider acts as a gateway provider at the point in the call path when the foreign provider immediately upstream of the gateway provider sends the call to the gateway provider, even for calls originated within the United States. The Commission agrees with commenters that ''U.S.-based facilities'' for the purpose of the Commission's definition means that the provider has facilities in the U.S., including, at a minimum, a U.S.-located point of presence.

9. The Commission clarifies that foreign affiliates of a U.S.-based provider or other U.S.-licensed entities that receive traffic in another country and transmit that traffic to another provider to bring across the boundary of the U.S. network are not gateway providers. As proposed, the Commission does not include in the definition providers that also terminate the call because they are then acting as terminating providers and are subject to the existing rules applicable to such providers. In their capacity as terminating providers, these providers have existing obligations to prevent their own end users from receiving illegal robocalls. (A terminating provider is a voice service provider for purposes of section 4 of the TRACED Act and the Commission's caller ID authentication rules. A voice service provider is required to, among other things, verify caller ID information pursuant to STIR/SHAKEN for traffic it terminates, 47 CFR 64.6301(a)(3), and submit a certification to the Robocall Mitigation Database.)

10. Because the TRACED Act defines ''voice service'' in a manner that excludes intermediate providers, the authentication and Robocall Mitigation Database rules use ''voice service provider'' in this manner. The Commission's call blocking rules, many of which the Commission adopted prior to adoption of the TRACED Act, use a definition of ''voice service provider'' that includes intermediate providers. In that context, use of the TRACED Act definition of ''voice service'' would create inconsistency with the existing rules. To avoid confusion, for purposes of this item, the Commission uses the term ''voice service provider'' consistent with the TRACED Act definition and where discussing caller ID authentication or the Robocall Mitigation Database. In all other instances, the Commission uses ''provider'' and specifies the type of provider as appropriate. Unless otherwise specified, the Commission means any provider, regardless of its position in the call path.

11. *Call-by-Call Basis.* Consistent with the proposal in the *Gateway Provider FNPRM,* the Commission adopts the gateway provider classification on a call-by-call basis. That is, a provider is a gateway provider and subject to the rules for gateway providers the Commission adopts in this document only for those calls for which it acts as a gateway provider unless otherwise noted.

12. As the Commission noted in the *Gateway Provider FNPRM,* the Commission took this approach when classifying intermediate and voice service providers with respect to the Commission's caller ID authentication rules. The Commission adopts the call-by-call classification to ensure that gateway providers, due to their key role in the call path, are subject to the requirements. There is record support for this approach. Concluding that the burdens are overstated, the Commission rejects concerns of commenters that assert that the call-by-call classification would not be administratively feasible, and would potentially impose two different sets of regulations on the same set of providers, causing confusion. As the Commission notes, and a number of commenters agree, a gateway provider will know the identity of the immediate upstream provider from which it receives a call. (As explained below, the Commission clarifies foreign intermediate providers' traffic will be blocked unless they register in the Robocall Mitigation Database.) The gateway provider will also know whether that provider has registered as a foreign provider in the Robocall Mitigation Database. The Commission's approach ensures that a gateway provider is subject to the consumer protection requirements it adopts whenever it receives a call directly from a foreign provider.

13. Moreover, a call-by-call approach will have a limited practical burden for several reasons. As an initial matter, several of the obligations the Commission adopts do not require a gateway provider or providers downstream from the gateway provider to determine, in real time, whether or not the relevant provider is acting as a gateway provider for a particular call. First, the 24-hour traceback requirement and know-your-upstream provider requirements do not involve any real-time action on the part of a gateway provider when it receives the call. Second, the obligation to block traffic upon notification by the Commission applies only to those entities identified by the Commission, so that providers need not identify relevant traffic in real-time in the first instance. Third, if a provider acts as a gateway provider for *any* calls, it must submit a robocall mitigation plan to the Robocall Mitigation Database describing how it mitigates calls in its role as a gateway provider *generally.* Fourth, where a downstream provider needs to block

traffic from an upstream provider that has not filed in the Robocall Mitigation Database, it is required to do so if it has reason to believe it is a gateway or voice service provider for *any* calls. Additionally, while gateway providers must undertake call blocking on a call-by-call basis at the time of the call for numbers on a Do Not Originate (DNO) list, all domestic providers in the call path are already permitted to engage in such blocking and can therefore elect to apply such blocking to all calls, rather than simply the calls for which they act as a gateway provider. Similarly, while gateway providers must take ''reasonable steps'' to mitigate calls received as a gateway provider on a call-by-call basis, the burden of identifying the relevant calls is likely low; gateway providers should know those calls they receive from foreign providers and send downstream to another domestic provider and can apply the appropriate mitigation procedures to those calls. Indeed, several stated that they already do so. At a minimum, to the extent a provider receives a call directly from a provider listed as ''foreign'' in the Robocall Mitigation Database, it is acting as a gateway provider for that call.

14. The Commission notes that many providers already operate under multiple sets of obligations—for example, as intermediate providers and voice service providers under the Commission's caller ID authentication rules—and no party has indicated why a call-by-call approach for gateway providers would be more burdensome. Moreover, no commenter proposed an alternative approach for imposing unique obligations on gateway providers. (Many commenters assert that the Commission should not impose unique obligations on gateway providers. The Commission addresses that argument in Section I.E.4 *infra*.) The Commission thus concludes that the burden on gateway providers to identify the appropriate regulatory regime applicable to a particular call will be limited.

15. *U.S. NANP Numbers.* Consistent with its proposal, the Commission limits the scope of the requirements for gateway providers to those calls that are carrying a U.S. number in the caller ID field. By a ''U.S. number,'' the Commission means NANP resources that pertain to the United States. The Commission excludes from the scope of its rules those calls that carry a U.S. number in the ANI field but display a foreign number in the caller ID field. Commenters uniformly support this approach, which is consistent with the scope of the prohibition on receiving calls carrying U.S. NANP numbers from foreign voice service providers not listed in the Robocall Mitigation Database. Foreign-originated robocalls are successful to the extent that end users believe they are calls from U.S. customers or businesses, and the Commission therefore concludes it is appropriate to focus its efforts on such calls. (For this reason, the Commission concludes that including ''in the caller ID field'' within its definition and elsewhere in its newly adopted rules will not encourage a deluge of illegal robocalls using non-US numbers as ZipDX argues.)

16. *No Traffic Carve-Outs.* Finally, the Commission declines to exclude certain types of traffic from the consumer protections it adopts. The Commission therefore rejects iBasis's contention that the Commission should exempt from the rules cellular roaming calls sent from U.S. customers abroad. The Commission also declines, at this time, to draw a distinction between ''conversational'' and ''non-conversational traffic'' and to require it to be segregated at the gateway and subject to different levels of regulatory scrutiny. (The Commission notes that it seeks comment on some of these ideas in the accompanying *FNPRM* published elsewhere in this this issue of the **Federal Register**.) The record does not reflect sufficient evidence to justify the utility of these carve-outs, or explain how they could be implemented in an administrable way and in a manner that avoids robocallers gaming whatever call-length definitions the Commission adopts. For example, the Commission is concerned that, if it sets a threshold for conversational traffic at a particular call length, robocallers would find a way to avoid crossing it while continuing to send robocalls. The Commission finds, at this time, that analytics providers, who can and do take call-length patterns into account in determining whether a call is likely to be an illegal robocall, are in the best position to make these sorts of determinations. These entities have the incentive and ability to react quickly to robocallers' shifting tactics and can do so without disclosing to bad actors the specific thresholds on which they rely.

### *C. Robocall Mitigation Database*

17. The Commission adopts its proposal to require gateway providers to submit a certification and mitigation plan to the Robocall Mitigation Database. As explained below, the Commission requires gateway providers to take ''reasonable steps'' to mitigate robocall traffic regardless of whether they have fully implemented STIR/SHAKEN. Gateway providers' robocall mitigation plans must describe their robocall mitigation practices and state that they are adhering to those practices, regardless of whether they have fully implemented STIR/SHAKEN. The Commission also adopts a modified version of its proposal for downstream domestic providers receiving traffic from gateway providers to block traffic from such a provider if the gateway provider has not submitted a certification in the Robocall Mitigation Database or if the gateway provider has been de-listed from the Robocall Mitigation Database pursuant to enforcement action. The vast majority of commenters supported these proposals.

18. *Gateway Provider Robocall Mitigation Database Filing Obligations.* The Commission concludes that requiring gateway providers to submit a certification to the Robocall Mitigation Database describing their robocall mitigation practices and stating that they are adhering to those practices, in conjunction with the new robocall mitigation obligations the Commission adopt elsewhere in this document, is an appropriate extension of similar obligations that currently apply to other providers. The Commission further concludes that requiring gateway provider certification will encourage compliance and facilitate enforcement efforts and industry cooperation. The record reflects significant support for this action. For example, iBasis, a gateway provider, ''believes that it is appropriate to require such a submission'' along with a mitigation plan. While INCOMPAS and T-Mobile argue that gateway providers that have implemented STIR/SHAKEN should not have to submit a mitigation plan, the Commission disagrees because of the importance of gateway providers in the call path and its conclusion that STIR/SHAKEN, on its own, will not eliminate illegal robocalls, particularly traffic originating from outside the United States.

19. These rules the Commission adopts require gateway providers to submit the same information to the Robocall Mitigation Database that voice service providers must submit under existing Commission rules, except for the limited areas described below. Specifically, gateway providers must certify to the status of STIR/SHAKEN implementation and robocall mitigation on their networks; submit contact information for a person responsible for addressing robocall mitigation-related issues; and describe in detail their robocall mitigation practices. Gateway providers may make confidential submissions consistent with the

Commission's existing confidentiality rules. (As USTelecom notes, providers may only redact filings to the extent appropriate under the Commission's confidentiality rules.) Gateway providers must also certify that they will comply with traceback requests within 24 hours, unlike the current ''reasonable period of time'' applicable for voice service providers, or that it has received a waiver of that rule.

20. Consistent with voice service providers' current obligations, the Commission does not require gateway providers to describe their mitigation program in a particular manner, with the exception of clearly explaining how they are complying with the know-your-upstream-provider obligation adopted in this document. The Commission concludes that it and the public will benefit from understanding how each provider chooses to comply with the know-your-upstream provider duty, both because compliance is critical to stopping the illegal carrying or processing of robocalls and because providers may choose to comply with this duty in different ways. (In several legal settlements with gateway providers, the gateway providers were required to comply with extremely detailed, and public, know-your-customer obligations.) As USTelecom argues, ''providers' robocall mitigation programs should reflect at least a basic level of vetting of the providers from whom they directly accept traffic—beyond ensuring that they are registered in the [Robocall Mitigation Database].''

21. The Commission also clarifies that, consistent with existing Commission filing requirements in other contexts, all mitigation plans must be submitted in English or with a certified English translation. To remove any ambiguity, the Commission also codifies that requirement with respect to its STIR/SHAKEN rules. Plans that were not submitted in English or with a certified English translation must be updated no later than 10 business days following the effective date of this document, consistent with the Commission's existing requirement for updating information in the Robocall Mitigation Database.

22. The Commission delegates to the Wireline Competition Bureau the authority to specify the form and format of any submissions, and it directs the Wireline Competition Bureau to comply with any requirements under the Paperwork Reduction Act attendant upon such action. This includes whether gateway providers that are also voice service providers may either submit a separate certification and plan as a gateway provider or amend their current certification and any plan. A gateway provider that is also a voice service provider should explain the mitigation steps it undertakes as a gateway provider and the mitigation steps it undertakes as a voice service provider, to the extent those mitigation steps are different for each role. And as with voice service providers, and consistent with the Commission's proposal, the Commission requires gateway providers to update their certifications within ten business days of ''any change in the information'' submitted, ensuring that the information is kept up to date.

23. The Commission also notes that it may take the same enforcement actions against a gateway provider whose certification is deficient or who fails to meet the standards of its certifications as is the case for voice service providers. This includes, but is not limited to, delisting the gateway provider from the Robocall Mitigation Database. In the *Second Caller ID Authentication Report and Order,* 85 FR 73360 (Nov. 17, 2020), the Commission set forth consequences for providers that file a deficient robocall mitigation plan or that ''knowingly or negligently'' originate illegal robocall campaigns, including removal from the Robocall Mitigation Database. To promote regulatory symmetry and close any loopholes in the Commission's regime, gateway providers will be subject to similar consequences. Specifically, if the Commission find that a certification is deficient, such as if the certification describes an ineffective program, or it determines that a provider knowingly or negligently carries or processes illegal robocalls, it will take appropriate enforcement action. These actions may include, among others, removing a certification from the database after providing notice to the gateway provider and an opportunity to cure the filing, requiring the gateway provider to submit to more specific robocall mitigation requirements, and/or the imposition of a forfeiture. Should the Commission remove a gateway provider from the Robocall Mitigation Database, downstream providers must block that gateway provider's traffic as described below.

24. Gateway providers must submit a certification to the Robocall Mitigation Database by 30 days following publication in the **Federal Register** of notice of approval by OMB of any associated Paperwork Reduction Act (PRA) obligations. (In the *Gateway Provider FNPRM,* the Commission proposed a filing deadline of 30 days after the publication of this document, but that did not account for OMB approval of PRA obligations.) The Commission concludes that the deadline will give providers sufficient time to prepare their submission following notification of OMB approval. If a gateway provider has not fully implemented STIR/SHAKEN by the filing deadline, it must so indicate in its filing. (Below, the Commission requires gateway providers to authenticate unauthenticated SIP traffic pursuant to STIR/SHAKEN by June 30, 2023.) It must then later update the filing within 10 business days of STIR/SHAKEN implementation. (Given the importance of tracking gateway providers' mitigation efforts, the Commission concludes that the benefit of an earlier filing deadline outweighs the burden for some providers to subsequently update their filing with their STIR/SHAKEN compliance status.)

25. The Commission does not at this time adopt a requirement for gateway providers to inform the Commission through an update to the Robocall Mitigation Database filing if the gateway provider is subject to a Commission, law enforcement, or regulatory agency action, investigation, or inquiry due to its robocall mitigation plan being deemed insufficient or problematic, or due to suspected unlawful robocalling or spoofing. Similarly, the Commission does not at this time require all or a subset of Robocall Mitigation Database filers to include additional identifying information. While the Commission concludes that taking these steps may have merit, it finds the record is insufficient to support taking action at this time. Instead, the Commission seeks comment in the accompanying *FNPRM* on imposing these obligations on all domestic providers in the call path.

26. The Commission also does not at this time extend this certification obligation to domestic intermediate providers other than gateway providers or require voice service providers that have already implemented STIR/SHAKEN to meet the ''reasonable steps'' standard and submit a robocall mitigation plan. However, the Commission seeks comment on doing so in the accompanying *FNPRM.*

27. *Gateway Provider Call Blocking.* The Commission also extends the prohibition on accepting traffic from unlisted voice service providers to gateway providers as proposed. This proposal received significant record support and will close a loophole in the Commission's regime. Under this rule, downstream providers will be prohibited from accepting any traffic from a gateway provider not listed in the Robocall Mitigation Database, either because the provider did not file or their

certification was removed from the Robocall Mitigation Database as part of an enforcement action. The Commission concludes that a gateway provider Robocall Mitigation Database filing requirement and an associated prohibition against accepting traffic from gateway providers not in the Robocall Mitigation Database will ensure regulatory symmetry between voice service providers and gateway providers and underscore the key role gateway providers play in stemming foreign-originated illegal robocalls. Consistent with the Commission's proposal, and the parallel requirement adopted for voice service providers in the *Second Caller ID Authentication Report and Order,* this prohibition will go into effect 90 days following the deadline for gateway providers to submit a certification to the Robocall Mitigation Database.

28. As a result of gateway providers' affirmative obligation to submit a certification in the Robocall Mitigation Database, the Commission concludes that downstream providers will no longer be able to rely upon any gateway provider database registration imported from the intermediate provider registry when making blocking determinations. (Previously, all intermediate providers were imported into the Robocall Mitigation Database from the rural call completion database's Intermediate Provider Registry so that all intermediate providers would be represented therein, giving voice service providers ''confidence that any provider not listed in the Robocall Mitigation Database'' was not in compliance with the Commission's rules.) In the *Second Caller ID Authentication Report and Order,* the Commission imported intermediate providers into the Robocall Mitigation Database from the intermediate provider registry to ensure that downstream providers did not inadvertently block traffic sent from the intermediate providers' networks. At that time, no intermediate providers were subject to a Robocall Mitigation Database filing or mitigation requirement. To the extent a gateway provider was imported into the Robocall Mitigation Database via the intermediate provider registry, that Robocall Mitigation Database entry is not sufficient to meet the gateway provider's Robocall Mitigation Database filing obligation or to prevent downstream providers from blocking traffic upon the effective date of the obligation for downstream providers to block traffic from gateway providers. Therefore, gateway providers must submit a certification to the Robocall Mitigation Database by 30 days following **Federal Register** publication of OMB approval of the relevant information collection requirements, and the downstream provider must begin blocking traffic within 90 days of that certification deadline if the gateway provider has not submitted a certification to the Robocall Mitigation Database. The Commission delegates to the Wireline Competition Bureau to make the necessary changes to the Robocall Mitigation Database to indicate whether a gateway provider has made an affirmative filing (as opposed to being imported as an intermediate provider) and whether any provider's filing has been de-listed as part of an enforcement action. The Bureau may, pursuant to an enforcement action, remove the record of a providers' filing or clearly mark it in a way so that downstream providers may not rely on it.

29. For the purpose of the downstream providers' call blocking duty, the Commission does not require the downstream provider to determine if a specific call was sent from a provider acting as a voice service provider or gateway provider for that call. Nevertheless, the Commission recognizes that it may not always be possible for the downstream provider to know whether the upstream provider is (1) a voice service provider or gateway provider whose traffic must be blocked if the provider did not make an affirmative certification in the Robocall Mitigation Database and has not been de-listed; or (2) an intermediate provider that is not a gateway provider, whose traffic should not be blocked. The Commission therefore only requires the downstream provider to block calls if they have a reasonable basis to believe that the upstream provider acts, *for some calls,* as a voice service provider or gateway provider and that the provider did not affirmatively file or in the Robocall Mitigation Database or has been de-listed. The Commission notes it is proposing in the *FNPRM* to expand the obligation to submit an affirmative certification to the Robocall Mitigation Database to all domestic intermediate providers. Adoption of that proposal should eliminate any of these implementation concerns. In that case, the downstream provider would simply check to see if the upstream provider affirmatively filed in the Robocall Mitigation Database and has not been de-listed and would block the call if appropriate. Nevertheless, the Commission concludes it must act now with respect to gateway providers to stem the tide of foreign-originated calls.

30. *Bureau Guidance.* The Commission directs the Wireline Competition Bureau to make the necessary changes to the Robocall Mitigation Database portal and provide appropriate filing instructions and training materials consistent with this document. The Commission also directs the Wireline Competition Bureau to release a public notice upon OMB approval of the information collection requirements for filing a certification, setting the deadlines for filing a certification, and for the downstream provider to block traffic from a gateway provider that has not filed a certification in the database. Either in that same or a separate public notice, the Wireline Competition Bureau shall also state when gateway providers may begin filing certifications in the Robocall Mitigation Database.

31. Commenters disagreed whether intermediate providers' imported data should be deleted from the database. Consistent with the Commission's direction to the Wireline Competition Bureau to make the necessary changes to the portal to effectuate the rules, the Commission directs the Bureau to determine how to manage the imported data of gateway providers and to announce its determination as part of its guidance described in the paragraph above.

32. *Public Safety Calls.* In the *Gateway Provider FNPRM,* the Commission clarified that: (1) even if a provider is not listed in the Robocall Mitigation Database, other voice service providers and intermediate providers in the call path must make all reasonable efforts to avoid blocking calls from public safety answering points (PSAPs) and Government outbound emergency numbers; and (2) emergency calls to 911 from originating providers not in the Robocall Mitigation database must not be blocked ''under any circumstances.'' (These clarifications reflect the Commission's existing requirements.) The Commission now codifies these requirements and applies them as well to the new blocking obligations it adopts in this document. Codifying these clarifications with respect to providers not listed in the Robocall Mitigation Database are consistent with the Commission's action to similarly codify these safeguards in its other blocking rules and will ensure completion of emergency calls is subject to the same safeguards regardless of the rule under which the call would otherwise be blocked. There was record support for this approach. The Commission disagrees with ZipDX that its clarification in the *Gateway Provider FNPRM* and its expansion to gateway providers would not be administratively feasible. Providers have had to comply

with the Commission's public safety exception to blocking for other purposes for several years, and ZipDX does not adequately explain why applying this exception to traffic sent from providers not in the Robocall Mitigation Database now would be different. Additionally, in balancing any implementation concerns against the critical importance of completing emergency calls, the Commission concludes that adopting and expanding the public safety exception is in the public interest.

33. The Commission also sought comment in the *Gateway Provider FNPRM* on whether it should expand these clarifications, including whether it should further define what constitutes ''reasonable efforts'' to prevent blocking of emergency calls. In light of the limited comments in the record and the uncertain benefits to be gained, the Commission does not take any further action at this time.

*D. Authentication*

34. To combat foreign-originated robocalls, and to further the long-standing Commission goal and benefits of ubiquitous STIR/SHAKEN authentication, the Commission requires gateway providers, consistent with its proposal, to implement STIR/SHAKEN to authenticate SIP calls that are carrying a U.S. number in the caller ID field. The Commission concludes based on the record that authentication, as well as the additional data sent to downstream providers along with the authentication, will reduce the incentive and ability of foreign providers to send illegal robocalls into the U.S. market, as well as provide downstream intermediate and terminating providers and their call analytics partners with additional data to protect their customers, and therefore will provide a significant benefit. Attestation information will facilitate analytics and promote traceback and enforcement efforts. Speeding traceback efforts is also consistent with the underlying goal of the Commission's 24-hour traceback requirement. The Commission finds those benefits outweigh the implementation costs. Additionally, certain commenters support requiring gateway providers to authenticate calls.

35. As the Commission has previously explained, application of caller ID authentication by intermediate—including gateway—providers ''will provide significant benefits in facilitating analytics, blocking, and traceback by offering all parties in the call ecosystem more information.'' At the time the Commission reached this conclusion, given the concerns that an authentication requirement on all intermediate providers ''was unduly burdensome in some cases,'' the Commission determined that intermediate providers could, instead of authenticating unauthenticated calls, ''register and participate with the industry traceback consortium as an alternative means of complying with our rules.'' Since that time, the Commission imposed on all domestic providers the requirement to respond to all traceback requests from the Commission, law enforcement, or the industry traceback consortium, fully and in a timely manner. Because evidence shows that foreign-originated robocalls are a significant and increasing problem and that the benefits of a gateway authentication requirement outweigh the burdens, the Commission thus adopts a gateway provider authentication obligation to address this problem. The Commission believes gateway provider authentication will address a significant risk to American consumers and enhance their trust in this country's telecommunications network.

36. *Requirement.* To comply with the requirement to authenticate calls, consistent with the Commission's proposal, a gateway provider must authenticate caller ID information for all SIP calls it receives for which the caller ID information has not been authenticated and which it will exchange with another provider as a SIP call. (As noted, the call blocking rules have mooted this choice—all domestic providers now must cooperate with traceback efforts.) A gateway provider can satisfy its authentication requirement if it adheres to the three Alliance for Telecommunications Industry Solutions (ATIS) standards that are the foundation of STIR/SHAKEN—ATIS–1000074, ATIS–1000080, and ATIS–1000084—and all documents referenced therein. Compliance with the most current versions of these standards as of the compliance deadline, including any errata to the standards as of that date or earlier, represents the minimum requirement to satisfy the Commission's rules. (No commenters addressed this proposal.) ATIS and the SIP Forum conceptualized ATIS–1000074 as ''provid[ing] a baseline that can evolve over time, incorporating more comprehensive functionality and a broader scope in a backward compatible and forward looking manner.'' The Commission intends for its rules to provide this same room for innovation, while maintaining an effective caller ID authentication ecosystem. Gateway providers may incorporate any improvements to these standards or additional standards into their respective STIR/SHAKEN authentication frameworks, so long as any changes or additions maintain the baseline call authentication functionality exemplified by ATIS–1000074, ATIS–1000080, and ATIS–1000084.

37. In addition, in line with the rule applicable to intermediate providers generally and the Commission's proposal, gateway providers have the flexibility in implementing call authentication to assign the level of attestation appropriate to the call based on the call information available to the gateway provider. Gateway providers are not limited to assigning ''gateway'' (C-level) attestation, and one commenter notes that there are significant benefits to be gained from gateway providers appropriately applying higher attestation levels consistent with the standard. Stakeholders support this approach.

38. *Benefits Outweigh Burdens.* The Commission concludes that the benefits of a gateway provider authentication obligation outweigh the burdens. Record evidence demonstrates that the benefits of gateway provider authentication are significant and are likely to grow over time as more providers are brought within the STIR/SHAKEN regime. Illegal robocalls cost Americans billions of dollars each year. Even minimal deterrence arising from authenticating unauthenticated foreign-originated calls is likely to be highly beneficial. To the extent ''gateway providers already exchange traffic in SIP and therefore likely are ready to implement STIR/SHAKEN,'' the requirement will have a real, near-term benefit.

39. Those commenters asserting such a requirement will cost significant time and resources to implement do not provide detailed support for their claims. Indeed, to the extent a gateway provider also serves as a voice service provider, it will have already implemented STIR/SHAKEN in at least some portion of its network, likely lowering its compliance costs to meet the requirement the Commission adopts. Given the real and significant benefits to providers and American consumers in the form of billions in savings and increased trust in the voice network that will flow from the reduction in foreign-originated illegal robocalls, the Commission concludes that requiring authentication is in the public interest even if it credits those arguing that there are substantial implementation costs.

40. While gateway providers are likely to authenticate most calls with only C-level attestation at least initially, the

Commission disagrees with those commenters who argue that the benefits of lower attestation levels, along with other information sent along with the attestation, are not worth the asserted cost. While ''C-level attestation is not as good as higher-level attestation . . . it is far more valuable, particularly in the case of foreign-originated illegal robocalls, than NO signature.'' Terminating providers and their end users directly benefit from gateway provider authentication. As T-Mobile notes, ''[r]eceiving *any* level of attestation can help carriers trace where unwanted or illegal calls enter the country so they can follow up and prevent additional traffic from the offending source. The information passed along with the attestation can be valuable for analytics engines, enabling calls to be appropriately labeled or sent to voice mail'' before reaching end users. Indeed, the North American Numbering Council (NANC) recently recognized the value of this information. Even if not all analytics providers currently use this information, more could readily do so in the future. And, while the Commission agrees with commenters that gateway provider authentication is not a ''silver bullet,'' it ''will have a significant impact on curtailing illegal robocalls which is critical to restoring trust in the voice network.'' It also will make the traceback process more efficient and rapid, consistent with the underlying goal of the Commission's newly adopted 24-hour traceback requirement. Even if foreign-originated calls carrying U.S. numbers constitute a small portion of gateway providers' overall traffic, such traffic represents a disproportionate share of illegal robocall traffic received by such providers, underscoring the importance of authentication. The Commission agrees with USTelecom that the Commission's authentication regime would be harmed if gateway providers improperly sign calls with A-level attestations, but that is not a problem unique to gateway provider authentication—all domestic providers authenticating calls are obligated to provide the appropriate attestation level. Similarly, the Commission disagrees with Verizon that because some gateway providers still have some time division multiplex (TDM) facilities, which fall ''out of the scope'' of the attestation mandate, the Commission should not require gateway providers to authenticate SIP calls. The Commission continuously has required voice service providers to implement authentication on the IP portions of their networks, as it does for gateway providers here, despite the presence of TDM facilities on their networks subject to a continuing extension.

41. Expanding the scope of providers subject to the STIR/SHAKEN regime will increase the overall benefits of the standard and its future reach. As many parties and the NANC note, STIR/SHAKEN has beneficial network effects, and the more steps the Commission takes to increase its use, the greater the overall benefit for those providers that have already implemented the standard and those providers' customers. (For the same reasons, the Commission does not adopt USTelecom's alternative proposal to only impose a gateway provider authentication obligation on smaller, non-facilities-based providers.) Indeed, the Commission's expansion of the STIR/SHAKEN regime may spur other countries and regulators to also develop and adopt STIR/SHAKEN, further increasing the standards' benefit. (While the i3forum opposes an attestation obligation, it notes that cross-border adoption of STIR/SHAKEN and voluntary agreements can lead to ''situations in which [the gateway provider] has access to information that would enable it to provide an A-level or B-level attestation.'') In the interim, gateway provider authentication is the only way to ensure that all foreign-originated calls with U.S. numbers in the caller ID field are authenticated. The Commission acknowledges that at least some of the benefits that will flow from gateway provider authentication are based on its reasoned predictions arising from disputed record evidence. Nevertheless, in adopting its rule, the Commission is persuaded by the available evidence that the benefits will be significant, and the sooner the Commission acts, the sooner the public will obtain these benefits. For these reasons, the Commission disagrees with CTIA-The Wireless Association that it would be ''premature'' for the Commission to require gateway authentication while foreign regulators consider mandating STIR/SHAKEN or that the Commission should wait for the recommendations of outside third parties, or possible future rule changes, before acting.

42. *Compliance Deadline.* The Commission requires that gateway providers authenticate unauthenticated foreign-originated SIP calls carrying U.S. NANP numbers by June 30, 2023, a longer period than the Commission proposed in the *Gateway Provider FNPRM*. One commenter supported a December 2023 deadline, while others supported either a longer or shorter deadline. The Commission conclude that this deadline appropriately balances the relevant burdens and benefits of implementation; it will give gateway providers less time than the 18 months voice service providers had to implement STIR/SHAKEN, but more time than the shorter deadline of the effective date of the order proposed by the 51 State attorneys general. This deadline also coincides with the extension for STIR/SHAKEN implementation for facilities-based small voice service providers.

43. The Commission also believes that a June 30, 2023, deadline is reasonable because the industry has much more experience with implementation than when the Commission originally required voice service providers to implement STIR/SHAKEN, there is evidence that STIR/SHAKEN implementation costs have dropped since it first adopted the requirement for voice service providers and because the authentication requirement applies only to the IP portions of the gateway providers' networks. Finally, to facilitate uniformity, simplify compliance, and consistent with comments in the record, the Commission does not adopt an earlier deadline for those providers that have, in their role as voice service providers, already implemented STIR/SHAKEN, nor do it adopt a longer deadline for certain providers or classes of provider, or a specific process for the grant of extensions or exemptions from this requirement, with the exception of two extensions regarding token access and non-IP networks described below. (Parties are, of course, free to file a request for waiver. The Commission may grant such requests where the particular facts at issue make strict compliance with the rule at issue inconsistent with the public interest. In considering whether to grant a waiver, the Commission may take into account factors such as hardship, equity, or more effective implementation of overall policy. This extension will be similar to the one already in place for voice service providers.) As noted above, once a gateway provider has fully implemented STIR/SHAKEN, it must update its filing in the Robocall Mitigation Database.

44. *Token Access.* The Commission sought comment on whether the Secure Telephone Identity Governance Authority's (STI–GA) token access policy serves as a barrier for all or a subset of gateway providers from obtaining a token and, if so, what if any actions it should take to address that barrier, but it received limited response. (USTelecom and iconnectiv assert that the policy should not be changed. iBasis argues that the operating company

number (OCN) criteria should be eliminated.) The Commission concludes that the current token access policy will likely not present a material barrier to gateway providers meeting their authentication obligation, and it anticipates that the STI–GA can address any concerns before gateway providers are required to authenticate calls by June 30, 2023. Nevertheless, to ensure that gateway providers are not unfairly penalized, the Commission provides a STIR/SHAKEN extension to gateway providers that are unable to obtain a token due to the STI–GA token access policy. The extension will run until the gateway provider is able to obtain a token as long as the gateway provider ''diligently pursues'' doing so.

45. *Non-IP Networks and Authentication.* The Commission concludes that gateway providers should have the same duty as voice service providers to either upgrade their non-IP networks to IP and implement STIR/SHAKEN or work with a working group, standards group, or consortium to develop a non-IP caller ID authentication solution. Such an obligation is appropriate in light of gateway providers' key role in serving as the entry point for foreign-originated voice traffic into the U.S. marketplace and the limited burden gateway providers would experience in working with a standards group. No party commented on this issue, and this approach is consistent with those commenters arguing that all domestic providers in the call path should have similar obligations. As with voice service providers, gateway providers that choose to work with a working group are subject to an extension to implement STIR/SHAKEN in the non-IP portions of their networks.

46. The Commission asked in the *Gateway Provider FNPRM* whether it should require gateway providers to adopt a non-IP caller ID authentication solution, an obligation that voice service providers currently do not have. A number of commenters filed specific proposals in the record for authentication on IP and non-IP networks for gateway providers as well as voice service providers. The Commission does not adopt these proposals, in part because many are outside of the scope of the *Gateway Provider FNPRM.* However, the Commission seeks comment on some of these alternatives in the accompanying *FNPRM,* as well as their applicability to all domestic providers in the call path, and do not foreclose the possibility of seeking comment on the remainder of these proposals in a future proposal.

*E. Robocall Mitigation*

47. The Commission adopts several of its robocall mitigation proposals from the *Gateway Provider FNPRM.* First, the Commission adopts its proposal to require gateway providers to respond to traceback requests within 24 hours, with one modification. Second, it requires gateway providers and the providers immediately downstream from the gateway provider to comply with blocking mandates in certain instances. Third, it requires gateway providers to ''know'' the provider immediately upstream from the gateway provider. Finally, the Commission adopts a general mitigation standard.

1. 24-Hour Traceback Requirement

48. The Commission adopts its proposal to require gateway providers to fully respond to traceback requests from the Commission, civil and criminal law enforcement, and the industry traceback consortium within 24 hours of receipt of such a request. (To be clear, the 24-hour clock does not start outside of the business hours of the local time for the responding office. Requests received outside of business hours as defined in the Commission's rules are deemed received at 8 a.m. on the next business day. Similarly, if the 24-hour response period would end on a non-business day, either a weekend or a Federal legal holiday, the 24-hour clock does not run for the weekend or holiday in question, and restarts at 12:01 a.m. on the next business day following when the request would otherwise be due. ''Business day'' for these purposes is Monday through Friday, excluding Federal legal holidays, and ''business hours'' are 8 a.m. to 5:30 p.m. on a business day, consistent with the definition of office hours in the Commission's rules. By way of example, a request received at 3 p.m. on a Friday will be due at 3 p.m. on the following Monday, assuming that Monday is not a Federal legal holiday. The Commission believes that this clarification resolves concerns raised by some parties about the burden of a strict 24-hour requirement.) This is an enhancement of the Commission's existing rule, which requires all domestic providers, including gateway providers, to respond to traceback requests ''fully and in a timely manner.'' The Commission takes this step recognizing the critical role that gateway providers play in stopping the deluge of illegal foreign-originated robocalls, which continue to increase despite its previous efforts to stem the tide.

49. The Commission finds that a mandatory 24-hour response requirement best serves to protect consumers from foreign-originated illegal robocalls, which are a prevalent source of illegal robocalls aimed at U.S. consumers. As the Commission has repeatedly made clear, traceback is an essential part of both identifying and stopping illegal calls, and rapid traceback is key to its success. The process used by the Industry Traceback Group, which is the currently designated industry traceback consortium, is semi-automated, allowing the process to continue very quickly when a provider responds to a traceback request. While time is always of the essence in traceback, time is particularly important in the case of foreign-originated calls. In such cases, reaching the origination point of the call may require working with foreign providers and foreign governments, which could significantly increase the total time for the traceback process. As the 51 State AGs have argued, time is of the essence for traceback of foreign-originated calls because law enforcement may need to work with international regulators to obtain information from providers outside of U.S. jurisdiction. As a result, any unnecessary delay increases the risk that this essential information may become impossible to obtain.

50. The Commission therefore disagrees with commenters that do not support its enhanced 24-hour requirement. First, the Commission disagrees with commenters that argue that a stricter requirement is not warranted here. The Commission acknowledges the work industry has done on improving the traceback process, and recognizes that many, if not most, providers that receive traceback requests already respond in under 24 hours. However, the Commission finds that it is important to act aggressively in the international calling context. The gateway provider's response to a traceback request is often the first step in a process where the entity conducting the traceback must work with multiple foreign providers to trace a call back to the originating foreign provider and caller. The longer this process takes, the higher the risk that a foreign provider will no longer have the information necessary to respond—if they are even willing to do so—or that other factors will change, reducing the ability to fully trace the call. Therefore, this process must both begin and be completed as soon as possible. Many, if not most, providers that receive traceback requests are already responding within 24 hours, and the Commission believes this

enhanced obligation presents no additional burden. For providers that do not already meet this standard, the additional burden is justified by the need to quickly obtain this information. The record does not support the contention that this requirement presents a significant burden for providers. (Some commenters did raise specific concerns about this requirement. However, as discussed further below, these comments appear to either misunderstand the current expectations or to misunderstand the scope of the requirement.) The Commission emphasizes again, as it stated in the *Fourth Call Blocking Order,* 86 FR 17726 (April 6, 2021), that it generally expects *all* domestic providers to respond to traceback within 24 hours in most instances. The rule the Commission adopts simply makes that expectation a requirement in the gateway context. (While the Commission requires response to all traceback requests within 24 hours, it retains its right to exercise discretion in enforcement or consider limited waivers where a provider that normally responds within the 24-hour time frame has an truly unexpected or unpredictable issue that leads to a delayed response in a particular case or for a short period of time.)

51. The Commission also disagrees with commenters who argue that 24 hours is too short a time frame. (One commenter incorrectly indicated that the ''current deadline'' is 36 hours, without indicating the source of that figure.) The Commission notes that, in the *Fourth Call Blocking Order,* it made clear that, in most cases, it expects responses within 24 hours under its existing rule. Further, according to a report by the Industry Traceback Group, the average time to complete a single hop in the traceback process is less than one day, with many providers responding in less than 30 minutes. (While the Industry Traceback Group notes that overall response time is reduced by certain providers responding more quickly, it also notes that ''[t]racebacks that end with non-responsive providers tend to have slower response times, even in completed hops before the non-responsive provider'' and that providers closer to the origination point tend to respond more slowly. Speeding up these responses can only benefit the traceback process.) Many, if not most, providers that receive traceback requests already respond in under 24 hours. The Commission therefore sees no reason to believe that the rule it adopts would unduly burden any gateway providers, nor would the burden of such a requirement outweigh the significant benefits to law enforcement from such a requirement. (Gateway providers for which this requirement poses a unique and significant burden may apply for a waiver of this rule under the ''good cause'' standard of § 1.3 of the Commission's rules. Under that standard, for example, waivers may be available in the event of sudden unforeseen circumstances that prevent compliance for a limited period or for a limited number of calls. The Commission notes that any applicant for waiver ''faces a high hurdle even at the starting gate'' and would need to ''plead with particularity'' the ''special circumstances'' that warrant a waiver and explain how granting a waiver would serve the public interest.)

52. The Commission makes clear that it does not require the gateway provider to identify the caller or originating provider within this 24-hour response period except in the case where the originating provider is the provider from which the gateway provider received the call. Some commenters appear concerned that this rule would require them to trace a call back to the point of origination, or, at least, through several hops. One commenter points to the ''need to obtain information from several other carriers located in foreign countries,'' while another mentions the need for ''detailed investigations.'' The Commission requires the gateway provider to respond with information only about the provider from which it directly received the call. (An appropriate response would include the identity of the upstream provider, as well as, for example, the country, a complete address, contact information for the provider, and a link to that provider's Robocall Mitigation Database filing.)

53. The Commission also encourages gateway providers to determine whether their relationship with upstream providers should change to better facilitate traceback. (For example, a gateway provider may conduct such an investigation as part of compliance with the ''know your upstream provider'' obligation discussed below, which does not have a 24-hour requirement.) The Commission sees no reason that a gateway provider should not be able to identify the immediate upstream provider from its records and respond to the traceback request without further investigation. In fact, one commenter indicated that it currently automates response to traceback.

54. *Compliance Deadline.* The Commission requires gateway providers to comply with this requirement no later than 30 days after publication of notice of OMB approval under the PRA. This allows gateway providers sufficient time to update their processes and come into compliance with the rule.

2. Mandatory Blocking

55. The Commission adopts some, but not all, of the mandatory blocking proposals it sought comment on in the *Gateway Provider FNPRM.* First, the Commission requires gateway providers to block, rather than simply effectively mitigate, illegal traffic when notified of such traffic by the Commission, and it requires providers immediately downstream from the gateway provider to block all traffic from an identified gateway provider that has failed to meet its blocking obligation upon Commission notification. Second, it requires gateway providers to block calls based on any reasonable DNO list. Third, it declines at this time to require gateway providers to block calls based on reasonable analytics. Finally, the Commission addresses related issues including requests for a safe harbor, as well as transparency and redress.

56. The Commission find that the mandatory blocking requirements it adopts, along with the appropriate procedural safeguards described herein, strike an appropriate balance between the benefit of blocking calls likely to be illegal with the risk of blocking lawful calls. The Commission acknowledges that this represents a shift, at least in part, from the Commission's previous approach of permitting, rather than mandating, blocking. The Commission agrees that ''[b]locking calls is a serious and complicated action that must be precisely and judiciously applied to avoid blocking lawful traffic.'' However, the Commission disagrees with commenters that argue mandatory blocking requirements are generally inappropriate. The Commission's existing permissive blocking rules are still in effect; it encourages providers to make use of permissive blocking, where available, to protect American consumers from unwanted and illegal calls. The rules the Commission adopts narrowly target the most obvious foreign-originated illegal calls, including those calls that have already been determined to be illegal, and enlist gateway providers into the fight to block these calls before they enter the U.S. telephone network.

a. Blocking Following Commission Notification

57. The Commission adopts two of its proposals from the *Gateway Provider FNPRM.* First, the Commission requires gateway providers to block, rather than

effectively mitigate, illegal traffic when notified of such traffic by the Commission. Second, it requires providers immediately downstream from a gateway provider to block all traffic from the identified provider when notified by the Commission that the gateway provider failed meet its obligation to block illegal traffic. To ensure that gateway providers are afforded sufficient due process prior to downstream providers blocking all traffic from them, the Commission adopts a clear process that allows ample time for the notified gateway provider to remedy the problem and demonstrate that it can be a good actor in the calling ecosystem before the Commission directs downstream providers to begin blocking. This process, laid out in greater detail below, includes the following steps: (1) the Enforcement Bureau shall provide the gateway provider with an initial Notification of Suspected Illegal Traffic; (2) the gateway provider shall be granted time to investigate and act upon that notice; (3) if the gateway provider fails to respond or its response is deemed insufficient, the Enforcement Bureau shall issue an Initial Determination Order, providing a final opportunity for the gateway provider to respond and; (4) if the gateway provider fails to respond or that response is deemed insufficient, the Enforcement Bureau shall issue a Final Determination Order, directing downstream providers to block all traffic from the identified provider.

58. *Gateway Provider Blocking Following Commission Notification of Suspected Illegal Traffic.* The Commission first adopts its proposal to require gateway providers to block, rather than simply effectively mitigate, illegal traffic when notified of such traffic by the Commission. In order to comply with this requirement, gateway providers must block traffic that is substantially similar to the identified traffic on an ongoing basis. As with the existing requirement for providers to take steps to effectively mitigate illegal traffic when notified, the Commission directs the Commission's Enforcement Bureau to identify suspected illegal calls and provide written notice to gateway providers that clearly indicates that the provider must comply with 47 CFR 64.1200(n)(5).

59. The Commission agrees with commenters that this blocking will help protect American consumers by ensuring less illegal traffic reaches their phones. An affirmative obligation for gateway providers to block upon Commission notification ensures greater protection than an ''effective mitigation'' requirement. This is particularly true because gateway providers, by definition, are intermediate providers and are thus a step removed from the caller, limiting their available effective mitigation options.

60. The Commission therefore disagrees with commenters that urge it to rely on the existing requirement to effectively mitigate this traffic rather than to adopt this enhanced requirement. The Commission also disagrees with providers that a separate set of obligations when acting as a gateway provider complicates or increases the burden of compliance because providers cannot easily determine if they are acting as a gateway provider for a particular call. Here, per the process described below, the Enforcement Bureau makes the initial determination of whether the provider is acting as a gateway provider. (A provider determines whether it is a ''gateway provider'' on a call-by-call basis. A provider may be a gateway provider for some of the calls in the identified traffic and a non-gateway originating provider, non-gateway intermediate provider, or non-gateway terminating provider for other calls in the identified traffic. If the provider is the gateway provider for any of the calls in the traffic identified in the Notification of Suspected Illegal Traffic, the provider must block all traffic that is substantially similar to the identified traffic, regardless of whether the provider is a gateway provider for any particular call.) If the gateway provider is not directed to comply with 47 CFR 64.1200(n)(5), but rather with 47 CFR 64.1200(n)(2), then that provider will not be in violation of the Commission's rules for effectively mitigating, rather than blocking, illegal traffic, regardless of its position in the call path for a particular call.

61. *Downstream Provider Blocking When Gateway Provider Fails to Comply with Blocking Requirement.* The Commission adopts its proposal requiring providers immediately downstream from a gateway provider to block all traffic from the identified provider when notified by the Commission that the gateway provider failed to block. If the Enforcement Bureau determines a gateway provider fails to satisfy 47 CFR 64.1200(n)(5), it shall publish and release an Initial Determination Order as described below giving the provider a final opportunity to respond to the Enforcement Bureau's initial determination. If the Enforcement Bureau determines that the identified gateway provider continues to violate its obligations, the Enforcement Bureau shall release and publish a Final Determination Order in EB Docket No. 22–174 to direct downstream providers to both block and cease accepting all traffic they receive directly from the identified gateway provider starting 30 days from the release date of the Final Determination Order. (Ignorance of a Final Determination Order's release is not sufficient reason for a downstream provider to fail to block all traffic from the gateway provider unless such Order is not posted in EB 22–174.)

62. The Commission agrees with several commenters that support this requirement and disagree with the lone commenter that objects to this mandate. The Commission finds that this requirement is an appropriate and proportional response where a gateway provider actively and willfully refuses to be a good actor in the calling ecosystem. Blocking all traffic from a particular provider is a dramatic step that will likely also block some lawful traffic but is justified by the need to protect consumers from foreign-originated illegal robocalls. Lawful traffic can then be routed through other gateway providers that comply with the Commission's rules.

63. *Process for Issuing a Notification of Suspected Illegal Traffic.* The Enforcement Bureau shall make an initial determination that the provider is a gateway provider for suspected illegal traffic and notify the provider by issuing a written Notification of Suspected Illegal Traffic. The Notification of Suspected Illegal Traffic shall: (1) identify with as much particularity as possible the suspected illegal traffic; (2) provide the basis for the Enforcement Bureau's reasonable belief that the identified traffic is unlawful (the notice should include any relevant nonconfidential evidence from credible sources such as the industry traceback consortium or law enforcement agencies); (3) cite the statutory or regulatory provisions the suspected illegal traffic appears to violate; and (4) direct the provider receiving the notice that it must comply with § 64.1200(n)(5) of the Commission's rules.

64. The Enforcement Bureau's Notification of Suspected Illegal Traffic shall specify a timeframe of no fewer than 14 days for an identified gateway provider to complete its investigation and report its results. Upon receiving such notice, the gateway provider must promptly investigate the traffic identified in the notice and begin blocking the identified traffic within the timeframe specified in the Notification of Suspected Illegal Traffic unless its investigation determines that the traffic is legal.

65. The Commission makes clear that the requirement to block on an ongoing basis is not tied to the number in the caller ID field or any other single criterion. Instead, the Commission requires the identified provider to block on a continuing basis any traffic that is substantially similar to the identified traffic and provide the Enforcement Bureau with a plan as to how it expects to do so. The Commission does not define ''substantially similar traffic'' in any detail here because that will be a case-specific determination based on the traffic at issue. The Commission declines to limit the scope of ''substantially similar traffic'' to only ''traffic sent by the upstream entity that was responsible for sending the illegal robocall traffic that triggered the Commission's notification.'' While gateway providers may propose such a limitation in the blocking plan they submit to the Enforcement Bureau, the Commission does not find that such a limitation is appropriate in all instances. In particular, such a limitation could make it easy for a bad actor to circumvent blocking by simply routing their traffic through multiple upstream providers. The Commission is also concerned that a detailed definition could allow bad actors to circumvent this blocking by providing a roadmap as to how to avoid detection. Additionally, the Commission notes that each calling campaign will have unique qualities that are better addressed on a case-by-case basis, where the analytics used can be tailored to the particular campaign at issue. The Commission nevertheless encourages gateway providers to consider common indicia of illegal calls such as call duration; call completion ratios; large bursts of calls in a short time frame; neighbor spoofing patterns; and sequential dialing patterns. The Commission makes clear that these are not the only criteria that the gateway provider may consider in developing its plan, and that not all criteria may be relevant in all situations. Gateway providers will have flexibility to determine the correct approach for each particular case, but a gateway provider must provide a detailed plan in its response to the Enforcement Bureau so that the Bureau can assess the plan's sufficiency. If the Enforcement Bureau determines that the plan is insufficient, it shall provide the gateway provider an opportunity to remedy the deficiencies prior to taking further action. The Commission will consider the identified provider to be in compliance with its mandatory blocking rule if it blocks traffic in accordance with its approved plan. However, the Commission makes clear that the Enforcement Bureau may require the identified provider to modify its approved plan if it determines that the identified provider is not blocking substantially similar traffic. Additionally, if the Enforcement Bureau finds, based on the evidence, that the identified provider continues to allow suspected illegal traffic onto the U.S. network, it may proceed to an Initial Determination Order or Final Determination Order, as appropriate. Finally, the Commission adopts a limited safe harbor from liability under the Communications Act or its rules for gateway providers that inadvertently block lawful traffic as part of the requirement to block substantially similar traffic in accordance with the gateway provider's approved plan. While the Commission agrees that a safe harbor for inadvertent over-blocking is warranted, it declines to provide a safe harbor for under-blocking within this rule. A gateway provider that is under-blocking and not fully cooperating with the Enforcement Bureau to address the issue should not be granted protection from liability under the very rule with which it fails to comply.

66. *Gateway Provider Investigation.* Each notified provider must investigate the identified traffic and report the results of its investigation to the Enforcement Bureau in the timeframe specified in the Notification of Suspected Illegal Traffic. If the provider's investigation determines that it served as the gateway provider for the identified traffic, it must block the identified traffic within the timeframe specified in the Notification of Suspected Illegal Traffic (unless its investigation determines that the traffic is not illegal) and include in its report to the Enforcement Bureau: (1) a certification that it is blocking the identified traffic and will continue to do so; and (2) a description of its plan to identify and block substantially similar traffic on an ongoing basis. If the provider's investigation determines that the identified traffic is not illegal, it shall provide an explanation as to why the provider reasonably concluded that the identified traffic is not illegal and what steps it took to reach that conclusion. Absent such a showing, or the Enforcement Bureau determines based on the evidence that the traffic is illegal despite the provider's assertions, the identified traffic will be deemed illegal. If a provider's investigation determines it did not serve as a gateway provider for any of the identified traffic, its report shall provide an explanation as to how it reached that conclusion and, if it is a non-gateway intermediate or terminating provider for the identified traffic, the provider must identify the upstream provider(s) from which it received the identified traffic and, if possible, take lawful steps to mitigate this traffic. (Such steps could include, for example, enforcing contract terms, or blocking the calls from bad actor providers consistent with the safe harbor found in 47 CFR 64.1200(k)(4).) If the notified provider determines that it is the originating provider for the identified traffic, or the traffic otherwise comes from a source that does not have direct access to the U.S. public switched telephone network, the notified provider must comply with 47 CFR 64.1200(n)(2) by effectively mitigating the identified traffic and report to the Enforcement Bureau any steps the provider has taken to effectively mitigate the identified traffic. If the gateway provider determines that the traffic is not illegal, it must inform the Enforcement Bureau and explain its conclusion within the specified timeframe.

67. *Process for Issuing an Initial Determination Order.* If the gateway provider fails to respond to the notice within the specified timeframe, the Enforcement Bureau determines that the response is insufficient, the Enforcement Bureau determines that the gateway provider is continuing to allow substantially similar traffic onto the U.S. network, or the Enforcement Bureau determines based on the evidence that the traffic is illegal despite the provider's assertions, the Enforcement Bureau shall issue an Initial Determination Order to the gateway provider stating its determination that the gateway provider is not in compliance with 47 CFR 64.1200(n)(5). This Initial Determination Order must include the Enforcement Bureau's reasoning for its determination and give the gateway provider a minimum of 14 days to provide a final response prior to the Enforcement Bureau's final determination as to whether the gateway provider is in compliance with 47 CFR 64.1200(n)(5).

68. *Process for Issuing a Final Determination Order.* If the gateway provider does not provide an adequate response to the Initial Determination Order or continues to allow substantially similar traffic onto the U.S. network, or the Enforcement Bureau determines based on the evidence that the traffic is illegal despite the provider's assertions, the Enforcement Bureau shall issue a Final Determination Order. The Enforcement Bureau shall publish the Final Determination Order in EB Docket No. 22–174 to direct downstream providers

to both block and cease accepting all traffic they receive directly from the identified gateway provider starting 14 days from the release date of the Final Determination Order. This Final Determination Order may be adopted up to one year after the release date of the Initial Determination Order and may be based on either an immediate failure to comply with 47 CFR 64.1200(n)(5) or a determination that the gateway provider has failed to meet its ongoing obligation to block substantially similar traffic under that rule.

69. Each Final Determination Order shall state the grounds for the Bureau's determination that the gateway provider has failed to comply with its obligation to block illegal traffic and direct downstream providers to initiate blocking 14 days from the release date of the Final Determination Order. A provider that chooses to initiate blocking sooner than 14 days from the release date may do so consistent with the Commission's existing safe harbor in 47 CFR 64.1200(k)(4).

b. Do-Not-Originate

70. The Commission further requires gateway providers to block calls based on a reasonable DNO list. A ''DNO list'' is a list of numbers that should never be used to originate calls, and therefore any calls that include a listed number in the caller ID field can be blocked. The Commission declines to mandate the use of a specific list, but allow gateway providers to use any DNO list so long as the list is reasonable. The Commission declines to mandate the use of a specific list, but gateway providers must use at least one DNO list, so long as the list is reasonable. Such a list may include only invalid, unallocated, and unused numbers, as well as numbers for which the subscriber to the number has requested blocking.

71. Reasonable DNO lists may include only the listed categories of numbers described in the preceding paragraph, but the Commission does not require that such DNO lists include all possible covered numbers in order to be reasonable. In particular, the Commission recognizes that unused numbers may be difficult to identify, and that a reasonable list may err on the side of caution. The Commission makes clear, however, that a list so limited in scope that it leaves out obvious numbers that could be included with little effort may be deemed unreasonable.

72. In the *2017 Call Blocking Order,* 82 FR 44118 (Sept. 21, 2017), the Commission specifically found that, where the subscriber to the originating number requests blocking, calls purporting to be from that number are ''highly likely to be illegal and to violate the Commission's anti-spoofing rule, with the potential to cause harm defraud, or wrongfully obtain something of value.'' Spoofing of this sort is particularly damaging as it can be used to foster consumer trust and bolster imposter scams. Therefore, the Commission finds that a reasonable list would need to include, at a minimum, any inbound-only government numbers where the government entity has requested the number be included. It must additionally include private inbound-only numbers that have been used in imposter scams, when a request is made by the private entity assigned such a number. (The current list maintained by the Industry Traceback Group is reasonable. The Commission declines, however, to deem that list ''presumptively reasonable'' as NCTA-The internet & Television Association suggests. While the Commission agrees that the list, as it currently stands ''would advance the Commission's goal of reducing harmful spoofing and imposter scams,'' it is concerned that deeming it ''presumptively reasonable'' does not account for the fact that the list is not under Commission control and could be modified, or no longer updated, at any time without Commission input.) In either scenario, the provider or the third party that manages the DNO list may impose reasonable requirements on including the numbers, such as requiring that the number is currently being spoofed at a substantial volume. (Multiple parties requested this or a similar clarification, to address concerns that some switches may have limits on the total amount of numbers that can be blocked.) Gateway providers, or those managing such a list on behalf of gateway providers, should ensure that entities can reasonably request inclusion on the list.

73. The Commission agrees with commenters that support a DNO mandate. The Commission further agrees with one commenter that urged the Commission to look to existing DNO lists for this purpose. While the Commission do not endorse a specific list, it encourages industry to either make use of existing tools or develop new ones to serve this purpose. Gateway providers may choose the list that works best for their networks so long as that list is reasonable. Because the Commission finds that a single, centralized list is not the correct approach, it declines to develop a ''high availability application or online tool'' as one commenter suggests. The Commission is concerned that a centralized list could present security concerns and allow bad actors to circumvent blocking by providing a clear list of numbers to avoid spoofing. (In some instances, there is still value in a DNO list even when bad actors know what numbers are included. For example, consumer trust may increase when the caller cannot spoof a known number associated with the caller the bad actor is attempting to impersonate. A non-public list, at a minimum, slows bad actors in their efforts to switch numbers and prevents some calls from reaching consumers.)

74. The Commission disagrees with the commenter that argued the mandate is unnecessary because many providers already use a DNO list to block calls. The Commission recognizes that providers have used DNO lists to reduce the number of illegal calls that reach consumers, and the Commission applauds these industry efforts. The Commission finds that enlisting all gateway providers in this effort will further reduce the risk of illegal calls reaching consumers. There is no legitimate reason for the caller to use numbers that appear on a DNO list. Therefore, these calls, if they reach even a single consumer, cause harm. The Commission also declines to deem gateway providers in compliance with this requirement if they have implemented a reasonable DNO in some parts of their network but not at the gateway. The intent of this rule is to stop foreign-originated illegal calls from entering the U.S. network at all. If these calls are not stopped at the gateway, there is a risk that they will not be blocked at all and will therefore reach consumers.

c. No Analytics-Based Call Blocking Mandate

75. The Commission declines at this time to require gateway providers to block calls that are highly likely to be illegal based on reasonable analytics. The Commission agrees with commenters' concerns regarding mandating such blocking. Additionally, the Commission finds that many of the arguments against mandatory blocking generally, while not persuasive in the context of other rules the Commission adopts, are persuasive in this context. An analytics-based blocking mandate would require the Commission to more strictly define ''reasonable analytics'' in order for gateway providers to be certain that they are in compliance with a mandatory blocking rule. To do so may be counter-productive and prevent providers from responding to evolving threats. The Commission is also concerned that providing a strict

definition, while certainly valuable to lawful callers, could potentially provide a road map bad actors could use to circumvent blocking. These concerns, coupled with the need for truly robust redress mechanisms for callers when the blocking is not initiated by the consumer and therefore cannot be corrected by the consumer, support the Commission's decision not to require such blocking at this time. (Several commenters, while objecting to a blocking mandate, urged the Commission to extend its safe harbor for blocking based on reasonable analytics to all providers in the call path, either in conjunction with a mandate or as an alternative. Because the Commission does not adopt such a mandate, it declines to reach the question of whether a safe harbor would be a necessary part of such a requirement. At this time, the Commission also declines to consider further extending the safe harbor absent such a mandate, as such an extension would be outside the scope of this document).

d. No Blocking Safe Harbor

76. Except as described above, the Commission declines to adopt a safe harbor for providers that block consistent with the rules the Commission adopts. Several comments addressing safe harbors focused on blocking based on reasonable analytics, and in some cases on extending the Commission's existing safe harbor instead of mandating blocking. The Commission does not adopt a reasonable analytics blocking mandate, and extending the existing safe harbor is outside of the scope of this document. Other comments did support a safe harbor more broadly, without tying the request to reasonable analytics. However, the Commission finds that the rules it adopts remove the need for such a safe harbor. In the case of blocking based on Commission notification, there is no need for a safe harbor where there is a clear Commission directive to block particular traffic directed at an individual provider. Nor is a safe harbor necessary for the downstream provider blocking requirement because the immediate downstream provider is required to block all traffic from the identified provider, regardless of whether that provider is a gateway provider for the particular traffic. There is no judgment call for a provider to make that could require a safe harbor. The Commission declines CTIA's request to establish a safe harbor is necessary for blocking based on a reasonable DNO list. First, providers have been permitted to engage in this type of blocking since 2017, and no commenter has pointed to any liability issues regarding over-blocking in this context. A gateway provider that is concerned about the possibility that they may not be able to keep a list containing unallocated or unused numbers fully up to date is not required to include those numbers on the list; while these numbers may be included, they are not mandatory. Providers that are concerned about possible under-blocking should take steps to ensure they are making use of a reasonable DNO list, and the Commission sees no reason to provide additional protection.

e. Protections for Lawful Calls

77. Consistent with the Commission's existing blocking rules, gateway providers must never block emergency calls to 911 and must make all reasonable efforts to ensure that calls from PSAPs and Government emergency numbers are not blocked. The Commission declines to adopt additional transparency and redress requirements at this time or extend any other existing requirements that would not already apply to the blocking mandates the Commission adopts. The new mandatory blocking rules either require the Commission to direct blocking, in which case the blocking provider is not in a position to provide redress, or target categories of calls that have been permissible to block since 2017. Some commenters expressed concerns about transparency and redress. The Commission recognizes some concerns regarding the potential for lawful calls to be blocked are valid, such as when a provider relies on analytics to make blocking decisions. These concerns do not apply here, however, where blocking is either at the direction of the Commission or based on a reasonable DNO list.

f. Compliance Deadline

78. The Commission requires gateway and downstream providers to comply with the requirements to block upon Commission notification no later than 60 days after publication of this document in the **Federal Register**. Additionally, the Commission requires gateway providers to comply with the DNO blocking requirement no later than 30 days after publication of notice of OMB approval under PRA. The Commission finds that requiring gateway providers to comply with these rules quickly imposes a minimal burden. In the case of blocking upon Commission notification, gateway providers need not make any changes to their processes prior to receipt of such a notification, and the Commission allows time for a gateway provider to comply following that notification. The Commission acknowledges that gateway providers that do not already block based on a DNO list may need to identify or develop such a list in order to comply with that particular requirement. However, the PRA approval process gives providers ample time to do so, and providers may use one of the existing DNO lists to meet this requirement with minimal burden.

3. ''Know Your Upstream Provider''

79. The Commission adopts a modified version of its proposal to require gateway providers to ''know the customer.'' Recognizing the difficulty posed by a requirement for gateway providers to know information about the caller, who is likely not their customer and with whom they have no relationship, the Commission instead requires gateway providers to ''know'' the immediate upstream foreign provider from which they receive traffic with U.S. numbers in the caller ID field. Specifically, the Commission requires gateway providers to take reasonable and effective steps to ensure that the immediate upstream foreign provider is not using the gateway provider to carry or process a high volume of illegal traffic onto the U.S. network.

80. The record supports deeming the immediate upstream foreign provider as ''customer'' for these purposes, rather than the caller. Though one commenter favored adopting its original proposal, the Commission agrees with other commenters that it would be difficult, if not impossible, for gateway providers to routinely confirm that a particular caller is authorized to use a U.S. number. By definition, a gateway provider is an intermediate provider and is thus at least one step removed from the caller. By contrast, the gateway provider must have a direct relationship with the upstream foreign provider from which it accepts traffic, which allows the gateway provider to ''know'' that upstream provider. This approach best balances the benefit of holding gateway providers responsible for calls they allow into the U.S. network with the difficulty of determining information about a caller that may be several hops away from the gateway.

81. The Commission agrees with the commenter that argues that the Commission's existing, flexible approach to know-your-customer requirements, rather than specific mandates, is appropriate in the gateway context. The Commission does not mandate the steps gateway providers must take in order to ''know'' the upstream foreign provider. Instead, the Commission allows gateway providers

the flexibility to determine the exact measures to take, including whether to adopt contractual provisions with their upstream providers to meet this obligation, and the contours of any such provisions. (The Commission notes that several commenters argued contract terms can be a valuable way of meeting a know-your-customer obligation and mitigating robocalls.) This approach is consistent with the Commission's existing requirement for originating providers to implement effective measures to prevent new and renewing customers from originating illegal calls, and allows each gateway provider to determine the best approach for its network and customers. (For the same reason, the Commission does not require gateway providers to enter into contractual provisions with their upstream provider to meet this know-your-upstream-provider requirement or any other new requirements the Commission adopts. However, gateway providers must explain the steps they have taken to meet their know-your-upstream-provider obligation in their Robocall Mitigation Database certification.) The Commission make clear, however, that gateway providers must take effective steps. If a gateway provider repeatedly allows a high volume of illegal traffic onto the U.S. network, the steps that provider has taken are not effective and must be modified for that provider to be in compliance with the Commission's rules.

82. The Commission recognizes concerns about the effectiveness of such a requirement, since the foreign provider upstream of the gateway may not be the source of the calls. The Commission agrees that the ideal approach would be for any obligation to fall to the originating provider, as in the Commission's existing rules. Unfortunately, in the case of foreign-originated calls, the Commission faces substantial difficulties in enforcing such an obligation on the foreign originating provider. (Due to this jurisdictional issue, the Commission imposes this obligation on the gateway provider as the first U.S.-based provider in the call path.) The Commission recognizes that gateway providers cannot prevent all instances of illegal calls from entering the U.S. network. In particular, a gateway provider's previously effective steps may become unexpectedly ineffective due to changes in factors outside of the gateway provider's control, particularly when the gateway provider is multiple hops from the call originator. (The Commission further acknowledges that, no matter how effective a gateway provider's methods are, some illegal calls may make up a portion of the traffic that it originates onto the U.S. network, and make clear that the fact that some illegal calls evade detection does not necessarily make a gateway provider's methods ineffective. The Commission therefore agrees with parties that asked it to clarify that ''occasionally serving as a gateway provider for illegal robocalls, particularly where those illegal calls are an insignificant fraction of that provider's traffic, does not inherently make the provider's practices ineffective.'' The Commission declines, however, to adopt the specific language proposed by the INCOMPAS et al. May 6 Ex Parte. The Commission makes clear, however, that a ''high volume of illegal traffic'' is a relative measure that is determined, in part, by what percentage of the traffic for which the provider is a gateway provider is illegal.) The Commission therefore reiterates that, as with its existing rule, it does not expect perfection. The Commission does require gateway providers to take reasonable steps, and it encourages gateway providers to regularly evaluate and adjust their approach so that they remain reasonable and effective. (Reasonable steps may include, but are not limited to, investigation of the practices of the upstream provider, modification of contracts to allow termination where issues arise, and/or monitoring incoming traffic for issues on an ongoing, proactive, basis.)

83. Because the Commission does not adopt the exact proposal in the *Gateway Provider FNPRM,* it declines to address roaming or adopt a carve-out for emergency calls. (The Commission further address roaming traffic in the accompanying *FNPRM.*) The rule the Commission adopts does not require gateway providers to block calls when they cannot confirm that the caller is authorized to use a particular U.S. number in the caller ID field, and therefore is unlikely to have detrimental effect on roaming or emergency traffic. The Commission also declines to adopt alternative proposals in the record that fall outside the scope of this document, including YouMail's proposal for post-contracting know-your-customer, i3forum's ''know your traffic'' proposal, or ZipDX's proposal to expand the requirement to cover all high-volume, non-conversational traffic even when such traffic is not foreign originated.

84. *Compliance Deadline.* The Commission requires gateway providers to comply with this rule no later than 180 days after publication of this document in the **Federal Register**. The Commission agrees with the commenter that argued that requiring compliance 30 days after publication may be insufficient for such a requirement. Allowing 180 days after publication ensures that gateway providers have sufficient time to develop effective systems and make any modifications to their networks or practices to implement these measures.

4. General Mitigation Standard

85. In addition to the specific mitigation requirements that the Commission adopts above, it also requires gateway providers to meet a general obligation to mitigate illegal robocalls regardless of whether they have fully implemented STIR/SHAKEN on the IP portions of their network. The Commission takes this step now because of the unique and key role that gateway providers play in the call path. Specifically, the Commission now requires all gateway providers to take ''reasonable steps to avoid carrying or processing illegal robocall traffic.'' The Commission does not require that the gateway provider take specific steps to meet this standard, in line with the existing requirement for voice service providers. The majority of commenters support the adoption of a general mitigation standard for gateway providers.

86. As with voice service providers subject to the ''reasonable steps'' standard, gateway providers must also implement a robocall mitigation program and, as explained above, file that plan along with a certification in the Robocall Mitigation Database. The record reflects significant support for adopting, at a minimum, a mitigation duty for gateway providers in addition to requiring them to submit a certification to the Robocall Mitigation Database. The Commission therefore adopts, consistent with its proposal, a mitigation duty for gateway providers that closely tracks the analogous rule for voice service providers. Specifically, a gateway provider's plan is ''sufficient if it includes detailed practices that can reasonably be expected to significantly reduce the [carrying or processing] of illegal robocalls.'' Moreover, a gateway provider ''must comply with the practices'' that its plan requires, and its program is insufficient if the gateway provider ''knowingly or through negligence [carries or processes calls] for unlawful robocall campaigns.''

87. The Commission requires gateway providers to mitigate traffic under the ''reasonable steps'' standard even if they have implemented STIR/SHAKEN for several reasons. First, the Commission notes the strong support in the record

for requiring gateway provider mitigation, regardless of their STIR/SHAKEN status, with certain commenters explicitly advocating for both gateway provider authentication and mitigation. Commenters agree that gateway providers are uniquely positioned to stop the entry of robocalls into this country, increasing the importance of strong mitigation.

88. Second, both the current record and the experience since the *Second Caller ID Authentication Report and Order* have shown that while STIR/SHAKEN is an effective tool to stop illegal robocalls, it is not a ''silver bullet,'' particularly in those cases where a robocaller is using a properly assigned telephone number. Providers, especially gateway providers serving as the entry point to the U.S. marketplace, can and must do more to stop robocalls. This is particularly the case while STIR/SHAKEN mandates by foreign governments and implementation by foreign providers remain limited.

89. Finally, the Commission anticipates that a general mitigation duty applicable to all gateway providers regardless of whether they have implemented STIR/SHAKEN will ''provide a valuable backstop'' to the other obligations the Commission adopts because call blocking, and traceback based on notice ''cannot take the place of the *proactive* dut[y] to mitigate harmful traffic.'' For all these reasons, the Commission disagrees with INCOMPAS and T-Mobile that it should not impose mitigation obligations on gateway providers that have implemented STIR/SHAKEN and find that requiring gateway providers that have implemented STIR/SHAKEN to also meet the Commission's ''reasonable steps'' mitigation standard ''would be an efficient use of their resources.'' The Commission does not adopt an alternative mitigation standard for gateway providers including a requirement proposed in the *Gateway Provider FNPRM* based on the existing duty for providers to take ''affirmative, effective measures to prevent new and renewing customers from using their network to originate illegal calls.'' The Commission notes, however, that under the rules it adopts, gateway providers must also comply with the ''know-your-upstream-provider standard, and steps a gateway provider takes to meet one standard could meet the other, and *vice versa*.

90. The Commission concludes that gateway providers' key role in facilitating the transmission of foreign-originated robocalls to U.S. consumers warrants imposing the ''reasonable steps'' mitigation duty on these providers without delay. While several commenters argue in the record for adopting more specific and broader duties on all domestic providers, the Commission leaves open for consideration such an expansion in the accompanying *FNPRM.* For example, it does not at this time require gateway providers to take specific actions to meet the ''reasonable steps'' standard. Nor does it require voice service providers or other intermediate providers to comply with the unique requirements it adopts for gateway providers, including the obligation to meet a general mitigation obligation even if they have fully implemented STIR/SHAKEN. Given the scope of the *Gateway Provider FNPRM* and the limited record evidence submitted regarding specific proposals, the Commission does not take these additional steps at this time.

91. *Compliance Deadline.* The Commission requires gateway providers to comply with the ''reasonable steps'' standard within 30 days of the effective date of this document. The Commission concludes that this is an appropriate period because the Commission does not mandate specific steps that gateway providers must take to meet this requirement other than submitting a certification to the Robocall Mitigation Database, and many gateway providers are already mitigating illegal call traffic. The compliance date for the requirement to submit a certification and mitigation plan to the Robocall Mitigation Database is 30 days following **Federal Register** notice of OMB approval of the relevant information collection requirements, and the Commission expects providers to refine their ''reasonable steps'' in light of additional time and marketplace developments prior to submission into the Robocall Mitigation Database.

*F. Summary of Cost Benefit Analysis*

92. The Commission finds that the benefits of the rules it adopts will greatly outweigh the costs imposed on gateway providers. The Commission sought comment on its belief that the proposed rules, viewed collectively, would account for a large share of the annual $13.5 billion minimum benefit the Commission originally estimated in the *First Caller ID Authentication Report and Order,* 85 FR 22029 (April 21, 2020), and *FNPRM,* 85 FR 22099 (April 21, 2022), because of the large share of illegal calls originating outside of the United States. While some commenters argue that the individual requirements may not provide substantial benefit taken individually or that there is no benefit to imposing obligations solely on gateway providers, others agree that the requirements the Commission adopts will benefit consumers and the calling ecosystem. The Commission finds that these requirements, taken together, will achieve a large share of the annual $13.5 billion minimum benefit. In addition, the Commission finds that there are many additional, non-quantifiable benefits from these rules, including restoring confidence in the U.S. telephone network and reliable access to the emergency and healthcare communications that save lives, reduce human suffering, and prevent the loss of property.

93. The Commission finds that the costs imposed on gateway providers are, in many instances, minimal and in all cases do not exceed the benefits. For example, a number of gateway providers are already required to implement STIR/SHAKEN in some portions of their networks because they do not solely act as gateway or intermediate providers, but may also serve as originating or terminating providers for some calls. In these cases, the additional burden to implement STIR/SHAKEN where a provider is acting as a gateway provider may be limited and has declined over time. Similarly, requiring gateway providers to block, rather than effectively mitigate, illegal traffic when notified by the Commission does not represent a burden increase, and in some cases may even be a burden decrease by eliminating the need to determine what mitigation is effective in a particular instance. As explained, the Commission disagrees with the burden estimates proffered by some commenters. However, even if the Commission does credit those claims, the expected minimum benefit is, as explained, so large that it will greatly outweigh the expected burden. (Contrary to USTelecom's assertion, the Commission does not take the position that it ''can adopt any individual regulation to fight illegal robocalls, no matter the cost or benefit of that particular regulation, as long as the aggregate cost of requirements is less than $13.5 billion.'' Rather, the Commission concludes that the requirements it adopts here will result in a ''large share'' of the $13.5 billion annual projected benefits from eliminating illegal robocalls, and no party has asserted that the purported costs of any or all of these regulations would cost either in one year or over several years a ''large share'' of $13.5 billion.)

94. Moreover, although the rules the Commission adopts will impose higher short-term costs on gateway providers

for implementation, it finds that they will lead to lower long-term costs. Specifically, the Commission finds that an overall reduction in illegal robocalls will greatly lower network costs for the gateway providers and other domestic service providers by eliminating both the unwanted traffic congestion and labor costs of handling numerous customer complaints, and by enabling those providers to trace calls back to the originator more quickly and efficiently.

*G. Legal Authority*

95. Consistent with its proposals, the Commission adopts the foregoing obligations pursuant to the legal authority the Commission relied on in prior caller ID authentication and call blocking orders. The Commission notes that no commenter questioned its proposed legal authority. (USTelecom suggests that because C-level attestations are ''untethered to the call authentication goal,'' the TRACED Act does not provide authority to adopt a gateway provider authentication requirement. But USTelecom's argument is inapposite because the Commission does not rely on the TRACED Act for its authority to impose this obligation, and USTelecom does not assert that the Commission otherwise lacks authority to impose a gateway provider authentication obligation.)

96. *Caller ID Authentication.* The Commission finds authority to impose caller ID authentication obligations on gateway providers under section 251(e) of the Communications Act of 1934 (the Act) and the Truth in Caller ID Act. In the *Second Caller ID Authentication Report and Order,* the Commission found it had the authority to impose caller ID authentication obligations on intermediate providers under these provisions. It reasoned that ''[c]alls that transit the networks of intermediate providers with illegally spoofed caller ID are exploiting numbering resources'' and so found authority under section 251(e). It found ''additional, independent authority under the Truth in Caller ID Act'' on the basis that such rules were necessary to ''prevent . . . unlawful acts and to protect voice service subscribers from scammers and bad actors,'' stressing that intermediate providers ''play an integral role in the success of STIR/SHAKEN across the voice network.'' While the *Second Caller ID Authentication Report and Order* did not specifically discuss gateway providers, the Commission uses the same legal authority to impose an authentication obligation on gateway providers because it defines gateway providers as a subset of intermediate providers.

97. *Robocall Mitigation and Call Blocking.* The Commission adopts its robocall mitigation and call blocking provisions for gateway providers pursuant to sections 201(b), 202(a), 251(e), the Truth in Caller ID Act, and its ancillary authority, consistent with the authority it invoked to adopt analogous rules.

98. The Commission concludes that section 251(e) and the Truth in Caller ID Act authorizes it to prohibit intermediate providers and voice service providers from accepting traffic from gateway providers that do not appear in the Robocall Mitigation Database. In the *Second Caller ID Authentication Report and Order,* the Commission concluded, ''section 251(e) gives us authority to prohibit intermediate providers and voice service providers from accepting traffic from both domestic and foreign voice service providers that do not appear in [the Robocall Mitigation Database],'' noting that its ''exclusive jurisdiction over numbering policy provides authority to take action to prevent the fraudulent abuse of NANP resources.'' The Commission observed that ''[i]llegally spoofed calls exploit numbering resources whenever they transit any portion of the voice network—including the networks of intermediate providers'' and that ''preventing such calls from entering an intermediate provider's or terminating voice service provider's network is designed to protect consumers from illegally spoofed calls.'' The Commission found that the Truth in Caller ID Act provided additional authority for its actions to protect voice service subscribers from illegally spoofed calls.

99. The Commission also concludes that sections 201(b), 202(a), and 251(e) of the Act, as well as the Truth in Caller ID Act and its ancillary authority, support the mandatory mitigation and blocking obligations the Commission imposes on gateway providers here. In the *Fourth Call Blocking Order,* the Commission required providers ''to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls,'' which includes a duty to ''know'' their customers. Additionally, the Commission required providers, to ''take steps to effectively mitigate illegal traffic when notified by the Commission,'' which may require blocking when applied to gateway providers. The Commission also adopted traceback obligations.

100. The Commission concluded that it had the authority to adopt these requirements pursuant to sections 201(b), 202(a), and 251(e) of the Act, as well as the Truth in Caller ID Act and its ancillary authority. Sections 201(b) and 202(a) provide the Commission with ''broad authority to adopt rules governing just and reasonable practices of common carriers.'' Accordingly, the Commission found that the new blocking rules were ''clearly within the scope of our section 201(b) and 202(a) authority'' and ''that it is essential that the rules apply to all voice service providers,'' applying its ancillary authority in section 4(i). The Commission also found that section 251(e) and the Truth in Caller ID Act provided the basis ''to prescribe rules to prevent the unlawful spoofing of caller ID and abuse of NANP resources by all voice service providers,'' a category that includes Voice over internet Protocol (VoIP) providers and, in the context of the Commission's call blocking orders, gateway providers. The Commission concludes that the same authority provides a basis to adopt the mitigation and blocking obligations on gateway providers the Commission adopts in this document to the extent that gateway providers are acting as common carriers.

101. While the Commission concludes that its direct sources of authority provide an ample basis to adopt its proposed rules on all gateway providers, its ancillary authority in section 4(i) provides an independent basis to do so with respect to gateway providers that have not been classified as common carriers. The Commission concludes that the regulations adopted in this document are ''reasonably ancillary to the Commission's effective performance of its . . . responsibilities'' because gateway providers that interconnect with the public switched telephone network and exchange IP traffic clearly offer ''communication by wire and radio.''

102. Requiring gateway providers to comply with the Commission's proposed rules is reasonably ancillary to the Commission's effective performance of its statutory responsibilities under sections 201(b), 202(a), 251(e), and the Truth in Caller ID Act as described above. With respect to sections 201(b) and 202(a), absent application of the Commission's proposed rules to gateway providers that are not classified as common carriers, originators of international robocalls could circumvent its proposed scheme by sending calls only to such gateway providers to reach the U.S. market.

103. *Indirect Effect on Foreign Service Providers.* The Commission confirms its conclusion in the *Gateway Provider FNPRM* that, to the extent any of the rules it adopts have an effect on foreign

service providers, that effect is only indirect and therefore consistent with the Commission's authority, and the Commission finds that it does not conflict with any of its international treaty obligations. (The Commission expressly sought comment on ''whether any of our proposed rules would be contrary to any of our international treaty obligations.'' No commenter identified any international treaty obligations that would be contravened by the Commission's new requirement, nor is the Commission aware of any.) No commenter argues otherwise. In the *Second Caller ID Authentication Report and Order,* the Commission acknowledged an indirect effect on foreign providers but concluded that it was permissible under Commission precedent affirmed by the courts. This includes the authority, pursuant to section 201, for the Commission to require that U.S. providers modify their contracts with foreign providers with respect to ''foreign communication'' to ensure that the charges and practices are ''just and reasonable,'' as the Commission does here. The obligations the Commission adopts only impose such an indirect effect.

104. Several parties argue that foreign providers may not be able to file in the Robocall Mitigation Database because foreign legal obligations may prevent them from satisfying the traceback obligations imposed on all such filers. (The Commission notes that these obligations arise out of the prohibition established in the *Second Caller ID Authentication Report and Order* on receiving calls carrying U.S. NANP numbers from foreign providers not listed in the Robocall Mitigation Database.) To the extent that foreign providers face *bona fide* domestic legal constraints that conflict with any of the certifications or attestations required of Robocall Mitigation Database filers, the Commission clarifies that they may still submit a certification to the Robocall Mitigation Database. The Commission recommends that foreign providers explain any such domestic legal constraints as part of their certification. The Commission directs the Wireline Competition Bureau to make any limited, necessary changes to the Robocall Mitigation Database to ensure that foreign providers are able to provide any necessary explanations.

## II. Order on Reconsideration

105. In this document, the Commission expands the requirement that voice service providers only accept calls carrying U.S. NANP numbers from foreign-originating providers listed in the Robocall Mitigation Database so that domestic providers may only accept calls carrying U.S. NANP numbers sent directly from foreign-originating or intermediate providers that are listed in the Robocall Mitigation Database, including those that have not been de-listed through enforcement action. (The Commission adopts this change in response to both CTIA's and Voice on the Net Coalition's (VON) Petitions, as well as the *Gateway Provider FNPRM,* which sought comment on whether to eliminate, retain, or enhance the requirement that voice service providers only accept calls carrying U.S. NANP numbers from foreign providers listed in the Robocall Mitigation Database.) In doing so, the Commission resolves the petitions of CTIA and VON seeking reconsideration of the existing requirement, and end the stay of enforcement of that requirement in the *Gateway Provider FNPRM.* (The VON Petition also seeks reconsideration of ''the requirement in § 64.6305(b)(4) that voice service providers filing certifications provide the name, telephone number and email address of a central point of contact within the company responsible for addressing robocall-mitigation-related issues.'' The Commission does not address that issue at this time, but may do so at a later date.)

### *A. Ending the Stay of Enforcement and Extending the Requirement To Include Calls Received Directly From Intermediate Foreign Providers*

106. In response to the *Gateway Provider FNPRM* and the Petitions for Reconsideration filed by CTIA and VON, the Commission has reconsidered the requirement that voice service providers only accept calls carrying U.S. NANP numbers from foreign voice service providers listed in the Robocall Mitigation Database and have concluded that amendment of the initial requirement is necessary to ensure that it more comprehensively protects American consumers from foreign-originated illegal robocalls. The Commission now resumes enforcement of the requirement and expand its scope so that domestic providers now may only accept calls directly from a foreign provider that originates, carries, or processes a call if that foreign provider is registered in the Robocall Mitigation Database and has not been de-listed pursuant to enforcement action. The Commission finds that such an extension of the requirement to include calls received from foreign intermediate providers as well as foreign-originating providers is consistent with the record and will better equip domestic providers to protect American consumers from foreign-originated illegal robocalls without causing widespread disruptions of lawful traffic.

107. Several commenters support this approach, including CTIA. In its comments, CTIA notes that industry stakeholders have made significant strides in encouraging their foreign partners to implement robocall mitigation programs so that they can register in the Robocall Mitigation Database, with many reporting that ''all, or nearly all, of their foreign partners that originate traffic have now registered,'' even absent enforcement of the requirement. Indeed, as of May 17, 2022, 875 foreign voice service providers have filed in the Robocall Mitigation Database, out of a total 6,285 voice service provider filings. To further enhance the effectiveness of the Robocall Mitigation Database in protecting against foreign-originated robocalls, CTIA argues that the Commission should clarify that foreign intermediate providers must also implement robocall mitigation programs and certify to such in the database in order for their traffic to be accepted by domestic providers. CTIA notes that promoting robocall mitigation by foreign intermediate providers in this fashion will promote use of the techniques by all entities in the call path and will help protect U.S. networks from illegal traffic.

108. The Commission agrees with CTIA's conclusions. Given the number of different entities that are typically involved in originating, carrying, processing, and terminating a call, a requirement that applies only to calls received directly from the foreign provider that originated them will capture only a small fraction of the total number of calls that domestic providers accept from foreign providers on a daily basis. To increase the effectiveness of the requirement and to better protect American consumers from foreign-originated illegal robocalls, it is necessary to expand the scope of the requirement to include all calls received directly from a foreign provider that originates, carries, or processes the call in question. This approach obviates the concerns of commenters that a gateway provider likely does not know which provider originated a particular call or where it was originated; it only knows the upstream foreign provider that handed off the call. Indeed, this is one of the reasons the Commission defines ''gateway provider'' in this document as the U.S.-based intermediate provider that receives a call directly from a foreign originating or foreign intermediate provider at its U.S.-based facilities before transmitting the call

downstream to another U.S.-based provider.

109. To ensure that foreign providers have sufficient time to take steps in light of this expanded rule and to facilitate consistent obligations, the Commission will begin enforcing the requirement that providers accept only traffic received directly from foreign providers that originate, carry, or process calls that have filed a certification in the database on the deadline for gateway providers to block traffic sent from foreign providers that originate, carry, or process calls established in this document. That is, enforcement will begin 90 days following the deadline for gateway providers to submit a certification to the Robocall Mitigation Database. This same blocking deadline will also apply to providers to block traffic from foreign *intermediate* providers that were not subject to the prior blocking rule. The date of this deadline is subject to OMB approval for any new information collection requirements. The Commission concludes that this extended period will provide sufficient time for all affected foreign providers to submit a certification to the Robocall Mitigation Database in order to remain on the Database. For similar reasons, the Commission adds ''in the caller ID field'' to the expanded rule to clarify the scope of the requirement and make it consistent with the newly adopted blocking obligation for providers receiving calls from gateway providers.

110. Contrary to the dire outcomes contemplated in CTIA and VON's Petitions discussed below, the requirement that voice service providers only accept calls carrying U.S. NANP numbers from foreign voice service providers listed in the Robocall Mitigation Database has not resulted in mass confusion or a widespread failure on the part of foreign voice service providers to register in the Robocall Mitigation Database. In reality, a significant number of foreign voice service providers have been made aware of the requirement and have registered in the Robocall Mitigation Database. Now that the Commission has taken the time to ensure that the requirement can be implemented without causing significant disruptions to legitimate, legal traffic, it is time to ensure that the requirement adequately protects American consumers from as many foreign-originated illegal robocalls as possible, and not merely a tiny fraction of such calls. The Commission knows the requirement can work on a practical level, and the Commission finds that the expected benefits will far outweigh any minimal costs that may be imposed on gateway providers. While the rules the Commission adopts in this document provide some additional tools to domestic providers to combat illegal robocalls originating outside the U.S., the Commission must give domestic providers as many tools as it can to protect their customers from as wide a swathe of foreign-originated illegal robocalls as possible. (To quote T-Mobile, the tools the new gateway provider rules represent ''may not be foolproof.'')

111. Several commenters have urged the Commission to reach out to its counterparts in foreign governments and inform them of its latest efforts to protect consumers from illegal robocalls while also encouraging regulators abroad to promote foreign provider participation in robocall mitigation and the Robocall Mitigation Database. The Commission takes this opportunity to reiterate its commitment to continue engaging actively with its international partners abroad to inform them of its latest efforts to combat illegal robocalls and to encourage robocall mitigation efforts on their part as well as participation in the Robocall Mitigation Database among their domestic providers. The Commission recognizes that it is only through active dialogue and cooperation with its international counterparts that it will be able to fully address the scourge of illegal robocalls here at home.

112. *Legal Authority.* The Commission concludes that section 251(e) gives it authority to require intermediate providers and voice service providers to accept traffic only from foreign intermediate providers using U.S. NANP numbering resources in the caller ID field that appear in the Robocall Mitigation Database. As the Commission concluded in the *First Caller ID Authentication Report and Order* and *FNPRM* and affirmed in the *Second Caller ID Authentication Report and Order,* its exclusive jurisdiction over numbering policy provides authority to take action to prevent the fraudulent abuse of U.S. NANP resources. Illegally spoofed calls exploit numbering resources whenever they transit any portion of the voice network—including the networks of intermediate and terminating providers. The Commission's action preventing such calls from entering an intermediate provider's or terminating provider's network is designed to protect consumers from illegally spoofed calls, even while STIR/SHAKEN is not yet ubiquitous. No commenters have challenged the Commission's authority to require voice service providers to accept traffic only from foreign providers that do appear in the Robocall Mitigation Database. (T-Mobile does not challenge the Commission's authority to require intermediate providers and voice service providers to only accept traffic directly from foreign providers that appear in the Robocall Mitigation Database, but it asserts that ''the FCC has no authority over foreign voice service providers.'' The revised rule the Commission adopts does not constitute the exercise of jurisdiction over foreign voice service providers. The Commission acknowledges that this rule will have an indirect effect on foreign voice service providers by incentivizing them to certify to be listed in the database. An indirect effect on foreign voice service providers, however, ''does not militate against the validity of rules that only operate directly on voice service providers within the United States.'' In addition, several commenters raise concerns about whether registering in the Robocall Mitigation Database would have U.S. tax implications for foreign providers, whether registration would subject foreign providers to universal service contributions, and whether such providers would be subject to the Commission's enforcement authority regarding certifications or other matters, such as compliance with traceback requests. In the absence of any showing of any significant tax consequences for foreign providers, and in light of the overwhelming pace at which they have already registered, the Commission concludes that the benefits obtained by its new rules substantially outweigh any such possible consequences. The Commission clarifies that the act of registration in the Robocall Mitigation Database, by itself, would not create a universal service contribution obligation for a foreign provider. Finally, the Commission confirms that the Commission has authority to enforce its rules by ensuring that the Robocall Mitigation Database includes only accurate certifications.) One of the only parties to even touch upon the subject in response to the *First Caller ID Authentication Report and Order* and *FNPRM,* Verizon, agrees that section 251(e) gives the Commission ample authority to ensure foreign VoIP providers ''submit to the proposed registration and certification regime by prohibiting regulated U.S. carriers from accepting their traffic if they do not.''

113. The Commission additionally finds authority in the Truth in Caller ID Act. It finds that the rule the Commission adopts is necessary to enable voice service providers and intermediate providers to help prevent illegal spoofed robocalls and to protect

voice service subscribers from scammers and bad actors that spoof caller ID numbers, and that section 227(e) thus provides additional independent authority for the revised rule the Commission adopts.

*B. Petitions for Reconsideration*

114. In expanding the scope of the requirement and concluding that domestic providers may only accept calls directly from a foreign provider that originates, carries, or processes a call if that foreign provider is registered in the Robocall Mitigation Database, the Commission plainly disagrees with the CTIA and VON Petitions for Reconsideration requesting that the Commission eliminate or otherwise curtail the requirement or asserting that the Commission violated the Administrative Procedure Act's (APA) notice-and-comment requirement when it adopted this rule in the *Second Caller ID Authentication Report and Order.* The Commission resolves the Petitions as described below.

1. CTIA Petition

115. The Commission denies CTIA's Petition because the evidence in the record demonstrates that the requirement is unlikely to have the negative consequences CTIA fears, and the Commission has already followed CTIA's recommendations to focus on other mitigation efforts and to delay enforcement of the requirement while developing a more substantial record. In its Petition, CTIA raises three primary arguments against the requirement that domestic providers only accept calls carrying U.S. NANP numbers from foreign voice service providers listed in the Robocall Mitigation Database: (1) the requirement will cause issues with international roaming that will harm American mobile wireless consumers in the U.S. and abroad; (2) the Commission's other efforts enable providers to protect consumers from illegal and unwanted robocalls from overseas without the need for a requirement that domestic providers only accept calls carrying U.S. NANP numbers from foreign voice service providers listed in the Robocall Mitigation Database; and (3) reconsideration is necessary because evidence of the requirement's impact on American wireless consumers is now available. The Commission addresses each of these arguments in turn.

a. International Roaming

116. CTIA asserts in its Petition that wireless roaming is a ''complex endeavor, which is more complicated internationally, as U.S. mobile network operators have roaming agreements with hundreds of overseas network operators to enable U.S. consumers to remain connected no matter where they travel or move.'' When a mobile wireless consumer abroad uses a U.S. phone number to call a consumer in the U.S., ''that call may be routed from an originating foreign provider's network over long distance routes that involve multiple foreign mobile network operators often on the basis of least cost routing to reach a U.S. intermediate or terminating provider for delivery to the intended recipient.'' Because of this, there are a ''number of hand-offs for a call on its way back to a U.S. consumer, and any one of hundreds of foreign providers could be chosen as the final foreign provider in the call path that interconnects with a U.S. intermediate or terminating provider.'' CTIA asserts that, if that final foreign voice service provider fails to implement a robocall mitigation program and certify to such in the Robocall Mitigation Database, all of its traffic—including legal, legitimate traffic—would be ''prohibited from reaching the intended recipients. . . .'' Thus, CTIA claims that the requirement that domestic providers only accept calls carrying U.S. NANP numbers from foreign voice service providers listed in the Robocall Mitigation Database would risk ''significant call completion issues for wireless calls from hundreds of foreign providers' networks, from any mobile wireless consumer using a U.S. phone number to make a call from abroad.'' CTIA also claims that foreign voice service providers that interconnect with U.S. providers will ''likely fail to register'' with the Robocall Mitigation Database in a timely manner. (And BT Americas Inc. asserts in its comments in support of the CTIA Petition that ''the certification process may place foreign carriers in the impossible situation of either having to violate their commitment to the FCC or violate the laws of their home country.'' As the Commission states earlier in this document, to the extent that foreign providers face *bona fide* domestic legal constraints that conflict with any of the certifications or attestations required of Robocall Mitigation Database filers, they may still submit a certification to the Robocall Mitigation Database and explain any such domestic legal constraints as part of their certification.) Thus, CTIA argues that reconsideration of the requirement is needed to prevent unintended blocking of legitimate, legal traffic and to give foreign providers sufficient time to develop robocall mitigation implementation plans and to register with the Commission.

117. The Commission believes that CTIA's concerns are overstated, and in any event the Commission does not find them sufficient to outweigh the benefits of the requirement. In light of the prevalence of foreign-originated illegal robocalls aimed at U.S. consumers, the requirement is a critical tool in combatting such calls. And far from resulting in a widespread failure to register with the Robocall Mitigation Database among foreign service providers, the requirement—along with the diligent and concerted efforts of U.S. providers—seems to have actively encouraged foreign voice service providers to institute robocall mitigation programs abroad and file certifications to be listed in the database and thus have their traffic continue to be accepted by domestic intermediate and terminating providers. As CTIA itself notes in its comments, since the establishment of the requirement in 2020, ''U.S. providers have worked diligently to educate their foreign counterparts about call authentication, robocall mitigation, and registration expectations,'' outreach that has included individual providers engaging directly with their foreign counterparts, as well as efforts to increase awareness of these changes through existing industry bodies such as the GSM Association (GSMA), the Communications Fraud Control Association, and the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG). According to CTIA, this work has produced results, with many foreign voice service providers implementing robocall mitigation plans and registering in the Robocall Mitigation Database even as the requirement has been held in abeyance. Based on the education and outreach efforts of CTIA members, 99% of AT&T's international traffic now comes from carriers registered in the Robocall Mitigation Database. Similarly, T-Mobile reports receiving all of its inbound international traffic from providers registered in the Robocall Mitigation Database, and Verizon states that approximately 99% of the traffic it receives from foreign voice service providers is from those registered in the Robocall Mitigation Database, thus mooting T-Mobile's arguments that the *Second Caller ID Authentication Report and Order* contains little evidence ''showing the likelihood of widespread compliance as a result of industry pressure'' and that the requirement ''will punish U.S. wireless subscribers when they are abroad, along with those in the U.S. whom they may try to call.'' (This result also runs counter to IDT

Telecom, Inc.'s (IDT) concerns that the requirement would be anticompetitive for U.S. companies because it would ''incline toward a handful of foreign wholesalers dominating the aggregation of USA termination, leading to only a small number of US carriers connecting with them.'') Beyond high levels of Robocall Mitigation Database registration among foreign voice service providers, CTIA reports that ''domestic voice service providers have continued to modify their interconnection contracts with foreign providers to focus on the need to mitigate illegal robocall traffic.''

118. Given the extraordinarily high levels at which foreign voice service providers have implemented robocall mitigation programs and registered with the Robocall Mitigation Database even absent enforcement of the requirement, the Commission finds CTIA's initial concerns that foreign voice service providers would fail to register with the database to no longer be an issue. (Nor has there been, as IDT feared, a rash of reciprocal registration and filing requirements for U.S. providers from foreign regulators. As for IDT's concern that the requirement would lead to ''an unequal enforcement problem, as many small operators may turn a blind eye to the requirement of their customers' registration, yet will go undetected because of a low profile,'' such a generalized risk could be said to apply equally to every regulation the Commission adopts and is not a valid reason to refrain from adopting a specific policy or regulation. Moreover, this argument imparts a heightened degree of malicious intent to small providers based purely upon the size of their operations. The Commission do not believe that small providers are any more or less likely to engage in illegal or malicious conduct than are large ones, and the Commission thus rejects the assumptions underpinning this argument.) Indeed, it appears that, much as CTIA intended, the Commission's decision to hold the requirement in abeyance has permitted domestic providers to interface with their foreign counterparts and encourage them to develop robocall mitigation implementation plans and register with the Robocall Mitigation Database. The Commission, therefore, concludes that the requirement should not result in significant call completion issues and that reconsideration based on this concern is unwarranted.

b. Other Efforts To Curb Illegal Robocalls

119. CTIA's second argument is that the Commission's other actions to prevent illegal and unwanted robocalls from outside the United States—including enforcement actions against VoIP providers facilitating illegal voice traffic, encouraging providers to protect international gateways from robocalls, and adopting a safe harbor for blocking traffic from bad actors—are more targeted and less disruptive than the requirement that domestic providers only accept calls carrying U.S. NANP numbers from foreign voice service providers listed in the Robocall Mitigation Database. Thus, the Commission ''should continue to focus on these and similar efforts while developing the record'' on the requirement.

120. After having developed a more fulsome record on the requirement in the wake of the *Gateway Provider FNPRM,* the Commission finds that the requirement that domestic providers only accept calls carrying U.S. NANP numbers from foreign voice service providers listed in the Robocall Mitigation Database is not disruptive and that its other actions to prevent illegal and unwanted robocalls from overseas are insufficient on their own to properly address the problem of foreign-originated illegal robocalls. As CTIA itself has noted since filing its initial petition, industry outreach to foreign voice service providers has met with great success, with numerous foreign voice service providers implementing robocall mitigation plans and registering in the Robocall Mitigation Database. With 99% of AT&T and Verizon's and 100% of T-Mobile's inbound international traffic now coming from carriers who are registered in the Robocall Mitigation Database, the Commission finds it unlikely that enforcement of the requirement that domestic providers only accept calls carrying U.S. NANP numbers from foreign voice service providers listed in the Robocall Mitigation Database will result in widespread call completion issues. At the same time, the Commission believes that the requirement is necessary to supplement its other actions, including enforcement actions against VoIP providers facilitating illegal voice traffic, encouraging providers to protect international gateways from robocalls, and adopting a safe harbor for blocking traffic from bad actors. While these steps are certainly important, merely encouraging providers to protect international gateways from illegal foreign-originated robocalls and adopting a safe harbor for those who block traffic from bad actors is not sufficient. If the Commission is to adequately address the significant problem of foreign-originated robocalls, just as with U.S. originated robocalls, those receiving such calls (here, gateway providers) must explicitly be required to accept only those calls carrying U.S. NANP numbers from foreign voice service providers that are listed in the Robocall Mitigation Database. To address the endemic practice of illegal robocalling, the Commission must use every tool at its disposal, especially those which have been shown not to result in significant call completion issues. The Commission thus finds CTIA's second argument unpersuasive.

c. Availability of Additional Evidence

121. CTIA's final argument is that reconsideration is appropriate because the Commission did not, in the *Second Caller ID Authentication Report and Order,* seek comment on the impacts of the requirement on international wireless roaming. Without such record evidence, CTIA contends, the Commission lacked ''sufficient support to prohibit domestic intermediate and terminating providers from completing calls from foreign voice service providers that have not certified in the [Robocall Mitigation Database].'' Thus, CTIA claims that the Commission should reconsider the requirement and further develop its record so that it can craft a ''more reasonable approach to encourage international provider certification'' without jeopardizing U.S. consumers or the U.S. voice network.

122. As noted above, the Commission solicited a more robust record in response to the *Gateway Provider FNPRM* regarding the requirement and its possible effects. As that record shows, efforts to educate foreign voice service providers and encourage implementation of robocall mitigation programs and registration with the Robocall Mitigation Database have met with great success. Foreign providers have been granted time to develop robocall mitigation implementation plans and register with the Robocall Mitigation Database, and they appear to have used that time well. In light of this success, the Commission feels confident that it may proceed with enforcement of the requirement that domestic providers only accept calls carrying U.S. NANP numbers from foreign voice service providers listed in the Robocall Mitigation Database without causing significant disruption to the completion of legal, legitimate traffic. The requirement, as crafted, is already ''reasonable,'' and addresses illegal robocalls originating from outside the United States without jeopardizing U.S. consumers or the U.S. voice network.

123. For the forgoing reasons, the Commission denies CTIA's petition.

2. VON Petition

124. VON's Petition relies largely on a single argument in seeking reconsideration of the requirement that domestic providers only accept calls carrying U.S. NANP numbers from foreign providers listed in the Robocall Mitigation Database—that the requirement violates the APA because the Commission failed to solicit and consider public comment on it. Thus, VON contends that the Commission should seek additional comments on the proposal to ''allow for a more thoughtful vetting of an otherwise very complicated issue.'' The Commission denies the VON Petition on substantive grounds for the reasons stated below. The Commission alternatively dismisses the Petition as mooted by the Commission's decision to hold enforcement of the requirement in abeyance until a final decision was reached regarding whether to eliminate, retain, or enhance the requirement and the Commission's request for comments on the scope of the requirement in the *Gateway Provider FNPRM.*

a. The Requirement That Domestic Providers Only Accept Calls From Foreign Voice Service Providers Listed in the Robocall Mitigation Database Complies With APA Notice-and-Comment Requirements

125. In the *First Caller ID Authentication Report and Order* and *FNPRM,* the Commission proposed that, when an intermediate provider receives an unauthenticated call that it will exchange with another intermediate or voice service provider as a SIP call, it must authenticate such a call with a ''gateway'' or C-level attestation. In seeking comment on that proposal, the Commission noted that multiple commenters had supported imposing STIR/SHAKEN requirements on gateway providers as a way to identify robocalls that originate abroad and to identify which provider served as the entry point for these calls to U.S. networks. The Commission then sought comment on whether this was an effective way to combat illegal calls originating outside the U.S. and whether there were ''other rules involving STIR/SHAKEN that we should consider regarding intermediate providers to further combat illegal calls originating abroad.'' The Commission also reiterated Verizon's suggestion that the Commission impose an obligation to use STIR/SHAKEN on any provider, regardless of its geographic location, if it intends to allow its customers to use U.S. telephone numbers, as well as USTelecom's proposal that the Commission consider obligating gateway providers to pass international traffic only to downstream providers that have implemented STIR/SHAKEN. The Commission sought comment on both proposals and asked if there were any other actions it could take to promote caller ID authentication implementation to combat robocalls originating abroad.

126. In response to the *First Caller ID Authentication Report and Order* and *FNPRM,* several commenters filed initial comments expressing support for combating robocalls originating abroad by requiring foreign voice service providers that appear in the Robocall Mitigation Database to follow the same requirements as domestic voice service providers.

127. Courts have long held that the APA requires that the final rule that an agency adopts be a ''logical outgrowth of the rule proposed.'' While the Commission did not explicitly propose a rule in the *First Caller ID Authentication Report and Order* and *FNPRM* requiring domestic intermediate and terminating providers to accept calls only from foreign voice service providers that use U.S. NANP numbers and are listed in the Robocall Mitigation Database, it did seek comment on: (1) whether to impose STIR/SHAKEN requirements on gateway providers as a way to identify robocalls that originate abroad; (2) whether there were other rules involving STIR/SHAKEN that the Commission should consider regarding intermediate providers to further combat illegal calls originating abroad; (3) Verizon's suggestion to impose on any provider, regardless of its geographic location, an obligation to use STIR/SHAKEN; (4) USTelecom's proposal that the Commission consider obligating gateway providers to pass international traffic only to downstream providers that have implemented STIR/SHAKEN; and (5) whether there were any other actions the Commission could take to promote caller ID authentication implementation to combat robocalls originating abroad. The Commission concludes that the requirement that domestic providers only accept calls carrying U.S. NANP numbers from foreign voice service providers listed in the Robocall Mitigation Database is a logical outgrowth of these repeated and specific requests for comment on the types of obligations the Commission should impose on gateway providers that accept traffic from foreign voice service providers. Indeed, while it did not specifically mention the requirement in its final adopted form, the Commission did seek comment on whether to impose STIR/SHAKEN requirements on gateway providers, as well as other actions that would promote caller ID authentication implementation and combat foreign-originated robocalls.

128. That this requirement is a logical outgrowth of such requests for comment is evident from the fact numerous entities filed comments in response to the *First Caller ID Authentication Report and Order* and *FNPRM* voicing support for combating robocalls originating abroad by requiring foreign voice service providers that appear in the Robocall Mitigation Database to follow the same requirements as domestic voice service providers. While the two are not exactly the same, this notion of requiring foreign voice service providers who file with the Robocall Mitigation Database to fulfill the same requirements as domestic providers is quite similar to the requirement the Commission eventually adopted, and the fact that it was mentioned by multiple commenters indicates that the requirement was indeed a logically foreseeable outgrowth of the language in the *First Caller ID Authentication Report and Order* and *FNPRM.* Even were it not a logical outgrowth of the *First Caller ID Authentication Report and Order* and *FNPRM,* the possibility of a requirement that domestic providers only accept calls carrying U.S. NANP numbers from foreign providers listed in the Robocall Mitigation Database was raised in the initial comments and was open to consideration and comment during the reply stage.

129. The Commission thus finds VON's claim that the adoption of the requirement violated the APA to be baseless and, accordingly, deny their Petition on substantive grounds.

b. VON's Petition Is Moot

130. Independently, and in the alternative, the Commission finds that the Commission's decision to hold enforcement of the requirement in abeyance until it reached a final decision regarding whether to eliminate, retain, or enhance the requirement, together with the Commission's request for comments on the scope of the requirement in the *Gateway Provider FNPRM,* renders the VON Petition moot. Even assuming *arguendo* that the initial adoption of the requirement in the *Second Caller ID Authentication Report and Order* violated the notice and comment requirements of the APA, the same cannot be said of the *Gateway Provider FNPRM,* which specifically and extensively sought comment on

whether ''to eliminate, retain, or enhance'' the requirement.

131. Much like CTIA in its own Petition, VON did not call for the wholesale elimination of the requirement that domestic providers only accept calls carrying U.S. NANP numbers from foreign voice service providers listed in the Robocall Mitigation Database, but merely time to solicit additional comment and allow for further consideration of the requirement. Regardless of whether the *First Caller ID Authentication Report and Order* and *FNPRM* provided notice and an opportunity to comment on the requirement, the *Gateway Provider FNPRM* undoubtedly provided both. The Commission in the *Gateway Provider FNPRM* stated that, until a final decision was made regarding whether to eliminate, retain, or enhance the requirement, it would not enforce the requirement that domestic voice service providers and intermediate providers accept only traffic carrying U.S. NANP numbers sent directly from foreign voice service providers listed in the Robocall Mitigation Database. (The Commission treats its holding enforcement of the prohibition in abeyance the same as a stay.) As the Commission has satisfied the terms of VON's Petition, the Commission dismisses it as moot. (As with the CTIA Petition, the Commission notes that the concerns raised in the VON Petition—namely, that the requirement would limit the number of foreign carriers who can terminate calls in the U.S., restrict the ability of U.S. carriers to terminate calls on behalf of U.S. customers to foreign points, and lead to the disruption of legitimate, non-harmful traffic—have proved to be largely unfounded in the wake of adoption of the requirement, and as noted above, 99% of AT&T and Verizon's and 100% of T-Mobile's inbound international traffic currently comes from carriers who are registered in the Robocall Mitigation Database. Thus, as with CTIA's concerns, the Commission finds VON's concerns about the potential failure of foreign providers to register in the database to be largely baseless in reality.)

132. Because the Commission finds that adoption of the requirement that domestic voice service providers and domestic intermediate providers only accept calls carrying U.S. NANP numbers from foreign voice service providers listed in the Robocall Mitigation Database did not violate the APA's notice-and-comment requirements and that VON's Petition is mooted by the Commission's decision to hold enforcement of the requirement in abeyance while the Commission sought comment on whether to eliminate, retain, or enhance the requirement, the Commission denies VON's Petition on substantive grounds and independently, and in the alternative, dismiss it as moot.

## III. Order

133. In this document, the Commission makes a ministerial change to a codified rule required to correct an inadvertent typographical error and spell out an undefined acronym. The Commission revises § 64.6300(f) of its rules, which defines the term ''intermediate provider,'' to change the word ''carriers'' to ''carries'' and to change the reference to ''PSTN'' to ''public switched telephone network.'' The Commission finds that there is good cause for adopting this amendment here because the typographical error may confuse those seeking to understand how the Commission defines the term ''intermediate provider'' for purposes of complying with its rules governing caller ID authentication, and the use of undefined acronyms, even if well known, is not preferable.

134. Section 553 of the Administrative Procedure Act permits the Commission to amend the Commission's rules without undergoing notice and comment where the Commission finds good cause that doing so is ''impracticable, unnecessary, or contrary to the public interest.'' The Commission has previously determined that notice and comment is not necessary for ''editorial changes or corrections of typographical errors.'' Consistent with Commission precedent, in this instance the Commission finds that notice and comment is unnecessary for adopting a ministerial revision to § 64.6300(f) to correct an inadvertent typographical error and spell out an undefined acronym in the definition of ''intermediate provider.''

## IV. Final Regulatory Flexibility Analysis

135. As required by the Regulatory Flexibility Act of 1980 (RFA), as amended, an Initial Regulatory Flexibility Analysis (IRFA) was incorporated into the *Further Notice of Proposed Rulemaking* adopted in September 2021 (*Gateway Provider FNPRM*). (The RFA, 5 U.S.C. 601–612, has been amended by the Contract With America Advancement Act of 1996, Public Law 104–121, 110 Stat. 847 (1996) (CWAAA). Title II of the CWAAA is the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA)). The Commission sought written public comment on the proposals in the *Gateway Provider FNPRM,* including comment on the IRFA. The comments received are discussed below. This Final Regulatory Flexibility Analysis (FRFA) conforms to the RFA.

### *A. Need for, and Objectives of, the Order*

136. First, this document takes important steps in the fight against foreign-originated illegal robocalls by holding gateway providers responsible for the calls they allow onto the U.S. network. Finally, the *Order on Reconsideration* in this document strengthens the prohibition on receiving calls carrying U.S. NANP numbers from foreign providers not listed in the Robocall Mitigation Database. The decisions the Commission makes here protect American consumers from unwanted and illegal calls while balancing the legitimate interests of callers placing lawful calls.

137. *Gateway Provider Report and Order.* This document takes important steps to protect consumers from foreign-originated illegal robocalls. These steps help stem the tide of foreign-originated illegal robocalls, which are a significant portion, if not the majority, of illegal robocalls. As the entry point onto the U.S. network for these calls, gateway providers are best positioned to protect all American consumers. Because there is no single solution to the illegal robocall problem, this document addresses this issue from several angles, all focused on reducing the number of foreign-originated illegal calls American consumers receive and aiding in identifying bad actors.

138. First, this document requires gateway providers to submit a certification and plan to the Robocall Mitigation Database describing their robocall mitigation practices and stating that they are adhering to those practices, regardless of whether they have fully implemented STIR/SHAKEN, and requires downstream domestic providers receiving traffic from gateway providers to block traffic from such a provider if the gateway provider has not submitted a certification in the Robocall Mitigation Database. Second, this document requires gateway providers to implement STIR/SHAKEN to authenticate SIP calls that are carrying a U.S. number in the caller ID field. Third, it requires gateway providers to fully respond to traceback requests from the Commission, civil and criminal law enforcement, and the industry traceback consortium within 24 hours of receipt of such a request. Fourth, it requires gateway providers to block illegal traffic when notified of such traffic by the

Commission and the providers immediately downstream from the gateway to block all traffic from the identified provider when notified by the Commission that the gateway provider failed to meet its obligation to block illegal traffic. This rule builds on the Commission's existing effective mitigation requirement and bad-actor provider blocking safe harbor, and proscribes specific steps that the Enforcement Bureau must take before directing downstream providers to block. Fifth, it requires gateway providers to block using a reasonable do-not-originate (DNO) list. Sixth, it requires gateway providers to take reasonable and effective steps to ensure that the immediate upstream provider is not using the gateway provider to originate a high volume of illegal traffic onto the U.S. network. Finally, it requires gateway providers to meet a general obligation to mitigate illegal robocalls regardless of whether they have fully implemented STIR/SHAKEN on the IP portions of their network.

139. *Order on Reconsideration.* The *Order on Reconsideration* in this document strengthens the existing prohibition on receiving calls carrying U.S. NANP numbers from foreign providers not listed in the Robocall Mitigation Database. To ensure that all foreign providers are brought within the prohibition, the *Order on Reconsideration* in this document modifies the rule such that the prohibition applies to calls directly from a foreign provider that originates, carries, or processes a call if that foreign provider is not listed in the Robocall Mitigation Database.

*B. Summary of Significant Issues Raised by Public Comments in Response to the IRFA*

140. There were no comments raised that specifically addressed the proposed rules and policies presented in the *Gateway Provider FNPRM* IRFA. Nonetheless, the Commission considered the potential impact of the rules proposed in the IRFA on small entities and took steps where appropriate and feasible to reduce the compliance burden for small entities in order to reduce the economic impact of the rules enacted herein on such entities.

*C. Response to Comments by the Chief Counsel for Advocacy of the Small Business Administration*

141. Pursuant to the Small Business Jobs Act of 2010, which amended the RFA, the Commission is required to respond to any comments filed by the Chief Counsel for Advocacy of the Small Business Administration (SBA), and to provide a detailed statement of any change made to the proposed rules as a result of those comments. The Chief Counsel did not file any comments in response to the proposed rules in this proceeding.

*D. Description and Estimate of the Number of Small Entities to Which the Rules Will Apply*

142. 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 rules adopted herein. 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. (Pursuant to 5 U.S.C. 601(3), the statutory definition of a small business applies ''unless an agency, after consultation with the Office of Advocacy of the Small Business Administration and after opportunity for public comment, establishes one or more definitions of such term which are appropriate to the activities of the agency and publishes such definition(s) in the **Federal Register**.'') 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.

143. *Small Businesses, Small Organizations, Small Governmental Jurisdictions.* The Commission's actions, over time, may affect small entities that are not easily categorized at present. The Commission therefore describes here, 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 32.5 million businesses.

144. 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. (The IRS benchmark is similar to the population of less than 50,000 benchmark in 5 U.S.C. 601(5) that is used to define a small governmental jurisdiction. Therefore, the IRS benchmark has been used to estimate the number small organizations in this small entity description. The Commission notes that the IRS data does not provide information on whether a small exempt organization is independently owned and operated or dominant in its field.) Nationwide, for tax year 2020, there were approximately 447,689 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. (The IRS Exempt Organization Business Master File (E.O. BMF) Extract provides information on all registered tax-exempt/non-profit organizations. The data utilized for purposes of this description was extracted from the IRS E.O. BMF data for businesses for the tax year 2020 with revenue less than or equal to $50,000, for Region 1—Northeast Area (58,577), Region 2—Mid-Atlantic and Great Lakes Areas (175,272), and Region 3—Gulf Coast and Pacific Coast Areas (213,840) which includes the continental U.S., Alaska, and Hawaii. This data does not include information for Puerto Rico.)

145. 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 2017 Census of Governments (the Census of Governments survey is conducted every five (5) years compiling data for years ending with ''2'' and ''7'') indicates that there were 90,075 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States. (Local governmental jurisdictions are made up of general purpose governments (county, municipal and town or township) and special purpose governments (special districts and independent school districts).) Of this number there were 36,931 general purpose governments (county, municipal and town or township) with populations of less than 50,000 and 12,040 special purpose governments—independent school districts with enrollment populations of less than 50,000. (There were 2,105 county governments with populations less than 50,000. This category does not include subcounty (municipal and township) governments. There were

18,729 municipal and 16,097 town and township governments with populations less than 50,000. There were 12,040 independent school districts with enrollment populations less than 50,000. While the special purpose governments category also includes local special district governments, the 2017 Census of Governments data does not provide data aggregated based on population size for the special purpose governments category. Therefore, only data from independent school districts is included in the special purpose governments category.) Accordingly, based on the 2017 U.S. Census of Governments data, the Commission estimates that at least 48,971 entities fall into the category of ''small governmental jurisdictions.'' (This total is derived from the sum of the number of general purpose governments (county, municipal and town or township) with populations of less than 50,000 (36,931) and the number of special purpose governments—independent school districts with enrollment populations of less than 50,000 (12,040), from the 2017 Census of Governments—Organizations tbls. 5, 6 & 10.)

1. Wireline Carriers

146. *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 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. (Fixed Local Service Providers include the following types of providers: Incumbent Local Exchange Carriers (ILECs), Competitive Access Providers (CAPs) and Competitive Local Exchange Carriers (CLECs), Cable/Coax CLECs, Interconnected VOIP Providers, Non-Interconnected VOIP Providers, Shared-Tenant Service Providers, Audio Bridge Service Providers, and Other Local Service Providers. Local Resellers fall into another U.S. Census Bureau industry group and therefore data for these providers is not included in this industry.)

147. 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. (The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.) Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 5,183 providers that reported they were engaged in the provision of fixed local services. Of these providers, the Commission estimates that 4,737 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.

148. *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. (Fixed Local Exchange Service Providers include the following types of providers: Incumbent Local Exchange Carriers (ILECs), Competitive Access Providers (CAPs) and Competitive Local Exchange Carriers (CLECs), Cable/Coax CLECs, Interconnected VOIP Providers, Non-Interconnected VOIP Providers, Shared-Tenant Service Providers, Audio Bridge Service Providers, Local Resellers, and Other 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. (The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.) Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 5,183 providers that reported they were fixed local exchange service providers. Of these providers, the Commission estimates that 4,737 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.

149. *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. (The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.) Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 1,227 providers that reported they were incumbent local exchange service providers. Of these providers, the Commission estimates that 929 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.

150. *Competitive 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 several types of competitive local exchange service providers. (Competitive Local Exchange Service Providers include the following types of providers: Competitive Access Providers (CAPs) and Competitive Local Exchange Carriers (CLECs), Cable/Coax CLECs, Interconnected VOIP Providers, Non-Interconnected VOIP Providers, Shared-Tenant Service Providers, Audio Bridge Service Providers, Local Resellers, and Other Local 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. (The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.) Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 3,956 providers that reported they were competitive local exchange service providers. Of these providers, the Commission estimates that 3,808 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.

151. *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. (The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.) Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 151 providers that reported they were engaged in the provision of interexchange services. Of these providers, the Commission estimates that 131 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.

152. *Cable System Operators (Telecom Act Standard).* The Communications Act of 1934, as amended, contains a size standard for small cable system operators, which classifies ''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,'' as small. As of December 2020, there were approximately 45,308,192 basic cable video subscribers in the top Cable multiple system operators (MSOs) in the United States. Accordingly, an operator serving fewer than 453,082 subscribers shall be deemed a small operator if its annual revenues, when combined with the total annual revenues of all its affiliates, do not exceed $250 million in the aggregate. Based on available data, all but five of the cable operators in the Top Cable MSOs have less than 453,082 subscribers and can be considered small entities under this size standard. The Commission notes 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. (The Commission does receive such information on a case-by-case basis if a cable operator appeals a local franchise authority's finding that the operator does not qualify as a small cable operator pursuant to § 76.901(e) of the Commission's rules.) Therefore, the Commission is 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.

153. *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. (The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.) Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 115 providers that reported they were engaged in the provision of other toll services. Of these providers, the Commission estimates that 113 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.

2. Wireless Carriers

154. *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. (The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.) Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 797 providers that reported they were engaged in the provision of wireless services. Of these providers, the Commission estimates that 715 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.

155. *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 $35 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. (The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. The Commission also notes that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably.) Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 71 providers that reported they were engaged in the provision of satellite

telecommunications services. Of these providers, the Commission estimates that approximately 48 providers have 1,500 or fewer employees. Consequently, using the SBA's small business size standard, a little more than of these providers can be considered small entities.

3. Resellers

156. *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. (The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.) Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 293 providers that reported they were engaged in the provision of local resale services. Of these providers, the Commission estimates that 289 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.

157. *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. 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. (The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.) Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 518 providers that reported they were engaged in the provision of toll services. Of these providers, the Commission estimates that 495 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.

158. *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. 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. (The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard.) Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were 58 providers that reported they were engaged in the provision of payphone services. Of these providers, the Commission estimates that 57 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.

4. Other Entities

159. *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 internet service providers (ISPs)) or voice over internet protocol (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. (The available U.S. Census Bureau data does not provide a more precise estimate of the number of firms that meet the SBA size standard. The Commission also notes that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably.) Based on this data, the Commission estimates that the majority of ''All Other Telecommunications'' firms can be considered small.

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

160. The *Gateway Provider Report and Order and Order on Reconsideration* require providers, primarily but not exclusively gateway providers, to meet certain obligations. These changes affect small and large companies equally and apply equally to all the classes of regulated entities identified above.

161. *Gateway Provider Report and Order.* This document requires gateway providers to submit a certification and plan to the Robocall Mitigation Database describing their robocall mitigation practices and stating that they are adhering to those practices, regardless of whether they have fully implemented

STIR/SHAKEN. Additionally, downstream domestic providers receiving traffic from gateway providers must block traffic from such a provider if the gateway provider has not submitted a certification in the Robocall Mitigation Database. Gateway providers are not required to describe their mitigation program in a particular manner, but must clearly explain how they are complying with the know-your-upstream-provider obligation adopted in this document.

162. A gateway provider must certify whether it has fully, partially, or not implemented STIR/SHAKEN, and include a statement in its certification that it commits to responding fully to all traceback requests from the Commission, law enforcement, and the industry traceback consortium and cooperate with such entities in investigating and stopping illegal robocalls. Submissions may be made confidentially consistent with the Commission's existing confidentiality rules. All information must be submitted in English or with a certified English translation and updated within 10 business days. Gateway providers must provide the same identifying information submitted by voice service providers.

163. Gateway providers must also implement STIR/SHAKEN to authenticate SIP calls that are carrying a U.S. number in the caller ID field. To comply with this requirement, a gateway provider must authenticate caller ID information for all SIP calls it receives for which the caller ID information has not been authenticated and which it will exchange with another provider as a SIP call consistent with the relevant ATIS standards. Gateway providers have the flexibility to assign the level of attestation appropriate to the call based on the current version of the standards and the call information available to the gateway provider. A gateway provider using non-IP network technology in all or a portion of its network must provide the Commission, upon request, with documented proof that it is participating, either on its own or through a representative, as a member of a working group, industry standards group, or consortium that is working to develop a non-IP solution, or actively testing such a solution. Under this rule, a gateway provider satisfies its obligations if it participates through a third-party representative, such as a trade association of which it is a member or vendor.

164. Gateway providers, and, in one case, any intermediate or terminating provider immediately downstream from the gateway, must also satisfy several robocall mitigation requirements. These requirements apply to any gateway provider, regardless of whether or not they have fully implemented STIR/SHAKEN on the IP portions of their network.

165. First, gateway providers must fully respond to traceback requests from the Commission, civil and criminal law enforcement, and the industry traceback consortium within 24 hours of receipt of such a request. The gateway provider should respond with information about the provider from which it directly received the call.

166. Second, gateway providers, and in one case, any intermediate or terminating provider immediately downstream from the gateway, must block calls in certain instances. Specifically, the gateway provider must block illegal traffic once notified of such traffic by the Commission through its Enforcement Bureau. In order to comply with this requirement, gateway providers must block traffic that is substantially similar to the identified traffic on an ongoing basis. When a gateway provider fails to comply with this requirement, the Commission may require providers immediately downstream from a gateway provider to block all traffic from the identified provider when notified by the Commission. As part of this requirement, a notified gateway provider must promptly report the results of its investigation to the Enforcement Bureau, including, unless the gateway provider determines it is either not a gateway provider for any of the identified traffic or that the identified traffic is not illegal, both a certification that it is blocking the identified traffic and will continue to do so and a description of its plan to identify the traffic on an ongoing basis. In order to comply with the downstream provider blocking requirement, all providers must monitor EB Docket No. 22–174 and initiate blocking within 30 days of a Blocking Order being released. Gateway providers must also block based on a reasonable do-not-originate (DNO list). Gateway providers are allowed flexibility to select the list that works best for them, so long as it is reasonable and only includes invalid, unallocated, and unused numbers, as well as numbers for which the subscriber to the number has requested blocking.

167. Third, gateway providers must take reasonable and effective steps to ensure that the immediate upstream provider is not using the gateway provider to originate a high volume of illegal traffic onto the U.S. network. Gateway providers have flexibility to determine the exact measures to take, so long as those steps are effective. Finally, gateway providers must meet a general obligation to mitigate illegal robocalls. Gateway providers are not required to take specific steps to satisfy this obligation, but must implement ''reasonable steps'' to avoid carrying or processing illegal robocall traffic and must also implement a robocall mitigation program and, as explained below, file that plan along with a certification in the Robocall Mitigation Database.

168. The *Order on Reconsideration* in this document strengthens the existing rule requiring downstream providers to block calls carrying U.S. NANP numbers sent from foreign providers not listed in the Robocall Mitigation Database. It modifies the requirement to apply to calls sent directly from a foreign provider that originates, as well as carries or processes a call carrying a U.S. NANP number. Therefore, a downstream domestic provider must block such calls sent directly from any foreign provider not listed in the Robocall Mitigation Database.

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

169. The RFA requires an agency to describe any significant alternatives that it has considered in reaching its 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 or reporting requirements under the rule for 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 small entities.

170. Generally, the decisions the Commission made in this document apply to all providers generally, and do not impose unique burdens or benefits on small providers. Small providers are as capable of being the entry-point onto the U.S. network for illegal calls as large providers, which necessitates equal treatment if the Commission is to protect consumers from these calls. However, the Commission did take steps to ensure that providers, including small providers, would not be unduly burdened by these requirements. Specifically, the Commission allowed flexibility where appropriate to ensure that providers, including small providers, can determine the best

approach for compliance based on the needs of their networks. For example, gateway providers have the flexibility to determine their proposed approach to blocking illegal traffic when notified by the Commission, to choose a reasonable DNO list, and to determine the steps they take to ''know the upstream provider.'' A similarly flexible approach applies to the requirement for gateway providers to implement and describe their mitigation plan filed in the Robocall Mitigation Database.

*G. Report to Congress*

171. The Commission will send a copy of the *Gateway Provider Report and Order and Order on Reconsideration,* including the FRFA, in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act. In addition, the Commission will send a copy of the *Gateway Provider Report and Order and Order on Reconsideration,* including the FRFA, to the Chief Counsel for Advocacy of the Small Business Administration. A copy of the *Gateway Provider Report and Order and Order on Reconsideration* (or summaries thereof) will also be published in the **Federal Register**.

**V. Procedural Matters**

172. *Paperwork Reduction Act.* This document may contain new and modified information collection requirements subject to the PRA, Public Law 104–13. Specifically, the rules adopted in 47 CFR 64.1200(n)(1) and (o), 64.6303(b), 64.6305(b), (c)(2), and (d) may require new or modified information collections. This document will be submitted to the Office of Management and Budget (OMB) for review under Section 3507(d) of the PRA. OMB, the general public, and other Federal agencies will be invited to comment on the new or modified information collection requirements contained in this proceeding. The modification to 47 CFR 64.6305(c)(2) is non-substantive and will be submitted to OMB in accordance with its process for non-substantive changes. In addition, the Commission notes that pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107–198, the Commission previously sought specific comment on how the Commission might further reduce the information collection burden for small business concerns with fewer than 25 employees.

173. *Final Regulatory Flexibility Analysis.* As required by the Regulatory Flexibility Act of 1980 (RFA), an Initial Regulatory Flexibility Analysis (IRFA) was incorporated into the *Gateway Provider FNPRM.* The Commission sought written public comment on the possible significant economic impact on small entities regarding the proposals addressed in the *Gateway Provider FNPRM,* including comments on the IRFA. Pursuant to the RFA, a Final Regulatory Flexibility Analysis is set forth in Section II above. The Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, will send a copy of the *Gateway Provider Report and Order,* including the Final Regulatory Flexibility Analysis (FRFA), to the Chief Counsel for Advocacy of the Small Business Administration (SBA).

174. *Congressional Review Act.* The Commission has determined, and the Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget (OMB), concurs, that this rule is ''major'' under the Congressional Review Act, 5 U.S.C. 804(2). The Commission will send a copy of the *Gateway Provider Report and Order* to Congress and the Government Accountability Office pursuant to 5 U.S.C. 801(a)(1)(A). The Commission will send a copy of the *Gateway Provider Report and Order and Order on Reconsideration* to Congress and the Government Accountability Office pursuant to 5 U.S.C. 801(a)(1)(A).

**VI. Ordering Clauses**

175. Accordingly, pursuant to sections 4(i), 4(j), 201, 202, 217, 227, 227b, 251(e), 303(r), and 403 of the Communications Act of 1934, as amended, 47 U.S.C. 154(i), 154(j), 201, 202, 217, 227, 227b, 251(e), 303(r), and 403, *it is ordered* that the *Gateway Provider Report and Order is adopted.*

176. *It is further ordered that,* pursuant to sections 4(i), 4(j), 201, 202, 217, 227, 227b, 251(e), 303(r), 403, and 405 of the Communications Act of 1934, as amended, 47 U.S.C. 154(i), 154(j), 201, 202, 217, 227, 227b, 251(e), 303(r), 403, and 405, the *Order on Reconsideration is adopted.*

177. *It is further ordered that,* 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), the *Gateway Provider Report and Order is adopted.*

178. *It is further ordered* that parts 0 and 64 of the Commission's rules *are amended* as set forth in the Final Rules.

179. *It is further ordered* that, pursuant to §§ 1.4(b)(1) and 1.103(a) of the Commission's rules, 47 CFR 1.4(b)(1), 1.103(a), and the *Gateway Provider Report and Report and Order shall be effective* 60 days after publication in the **Federal Register**. Compliance with 47 CFR 64.1200(n)(1) and (o) will not be required until OMB completes any review that the Consumer and Governmental Affairs Bureau determines is required under the PRA. The Commission directs the Consumer and Governmental Affairs Bureau to announce a compliance date by subsequent notification and to cause 47 CFR 64.1200(n)(1) and (o) to be revised accordingly. Compliance with 47 CFR 64.6303(b) and 64.6305(b), (c)(2), and (d) will not be required until OMB completes any review that the Wireline Competition Bureau determines is required under the PRA. The Commission directs the Wireline Competition Bureau to announce a compliance date by subsequent notification and to cause 47 CFR 64.6303(b) and 64.6305(b), (c)(2), and (d) to be revised accordingly.

180. *It is further ordered* that the Petition for Partial Reconsideration filed by CTIA *is denied.*

181. *It is further ordered that* the Petition for Reconsideration filed by Voice on the Net Coalition *is denied in part* and, in the alternative, *dismissed in part.*

182. *It is further ordered* that the *Order on Reconsideration* and *Gateway Provider Report and Order shall be* effective 60 days after publication in the **Federal Register**.

183. *It is further ordered* that the Office of the Managing Director, Performance Evaluation and Records Management, *shall send* a copy of the *Gateway Provider Report and Order and Order on Reconsideration* in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act, see 5 U.S.C. 801(a)(1)(A).

184. *It is further ordered* that the Commission's Consumer & Governmental Affairs Bureau, Reference Information Center, *shall send* a copy of the *Gateway Provider Report and Order and Order on Reconsideration,* including the Final Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

**List of Subjects**

*47 CFR Part 0*

Authority delegations (Government agencies), Communications, Communications common carriers, Classified information, Freedom of information, Government publications, Infants and children, Organization and functions (Government agencies), Postal Service, Privacy, Reporting and

recordkeeping requirements, Sunshine Act, Telecommunications.

*47 CFR Part 64*

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

Federal Communications Commission.

**Marlene Dortch,**

*Secretary.*

**Final Rules**

The Federal Communications Commission amends parts 0 and 64 of title 47 of the Code of Federal Regulations as follows:

## PART 0—COMMISSION ORGANIZATION

### Subpart A—Organization

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

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

■ 2. Amend § 0.111 by revising paragraph (a)(27) and adding paragraph (a)(28) to read as follows:

**§ 0.111 Functions of the Bureau.**

(a) * * *

(27) Identify suspected illegal calls and provide written notice to voice service providers. The Enforcement Bureau shall:

(i) Identify with as much particularity as possible the suspected traffic;

(ii) Cite the statutory or regulatory provisions the suspected traffic appears to violate;

(iii) Provide the basis for the Enforcement Bureau's reasonable belief that the identified traffic is unlawful, including any relevant nonconfidential evidence from credible sources such as the industry traceback consortium or law enforcement agencies; and

(iv) Direct the voice service provider receiving the notice that it must comply with § 64.1200(n)(2) or (5) of this chapter.

(28) Take enforcement action, including de-listing from the Robocall Mitigation Database, against any provider:

(i) Whose certification described in § 64.6305(c) and (d) of this chapter is deficient after giving that provider notice and an opportunity to cure the deficiency; or

(ii) Who accepts calls directly from a domestic voice service provider, gateway provider, or foreign provider not listed in the Robocall Mitigation Database in violation of § 64.6305(e) of this chapter.

* * * * *

## PART 64—MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

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

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

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

■ 4. Amend § 64.1200 by:

■ a. Adding paragraphs (f)(19);

■ b. Revising paragraphs (k)(5) and (6) and (n)(1); and

■ c. Adding paragraphs (n)(4) through (6), (o), and (p).

The additions and revisions read as follows:

**§ 64.1200 Delivery restrictions.**

* * * * *

(f) * * *

(19) The term *gateway provider* means a U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider. For purposes of this paragraph (f)(19):

(i) *U.S.-based* means that the provider has facilities located in the United States, including a point of presence capable of processing the call; and

(ii) *Receives a call directly* from a provider means the foreign provider directly upstream of the gateway provider in the call path sent the call to the gateway provider, with no providers in-between.

* * * * *

(k) * * *

(5) A provider may not block a voice call under paragraphs (k)(1) through (4), paragraph (k)(11), paragraphs (n)(5) and (6), or paragraph (o) of this section if the call is an emergency call placed to 911.

(6) When blocking consistent with paragraphs (k)(1) through (4), paragraph (k)(11), paragraphs (n)(5) and (6), or paragraph (o) of this section, a provider must making all reasonable efforts to ensure that calls from public safety answering points and government emergency numbers are not blocked.

* * * * *

(n) * * *

(1) Upon receipt of a traceback request from the Commission, civil law enforcement, criminal law enforcement, or the industry traceback consortium:

(i) If the provider is an originating, terminating, or non-gateway intermediate provider for all calls specified in the traceback request, the provider must respond fully and in a timely manner;

(ii) If the provider receiving a traceback request is the gateway provider for any calls specified in the traceback request, the provider must fully respond to the traceback request within 24 hours of receipt of the request. The 24-hour clock does not start outside of business hours, and requests received during that time are deemed received at 8 a.m. on the next business day. If the 24-hour response period would end on a non-business day, either a weekend or a Federal legal holiday, the 24-hour clock does not run for the weekend or holiday in question, and restarts at 12:01 a.m. on the next business day following when the request would otherwise be due. For example, a request received at 3 p.m. on a Friday will be due at 3 p.m. on the following Monday, assuming that Monday is not a Federal legal holiday. For purposes of this paragraph (n)(1)(ii), *business day* is defined as Monday through Friday, excluding Federal legal holidays, and *business hours* is defined as 8 a.m. to 5:30 p.m. on a business day. For purposes of this paragraph (n)(1)(ii), all times are local time for the office that is required to respond to the request.

* * * * *

(4) If the provider acts as a gateway provider, take reasonable and effective steps to ensure that any foreign originating provider or foreign intermediate provider from which it directly receives traffic is not using the gateway provider to carry or process a high volume of illegal traffic onto the U.S. network. Compliance with this paragraph (n)(4) will not be required until January 16, 2023.

(5) If the provider acts as a gateway provider, and is properly notified under this section, block identified illegal traffic and any substantially similar traffic on an ongoing basis (unless its investigation determines that the traffic is not illegal) when it receives actual written notice of such traffic by the Commission through its Enforcement Bureau. The gateway provider will not be held liable under the Communications Act or the Commission's rules in this chapter for gateway providers that inadvertently block lawful traffic as part of the requirement to block substantially similar traffic so long as it is blocking consistent with the requirements of this paragraph (n)(5). For purposes of this paragraph (n)(5), *identified traffic* means the illegal traffic identified in the Notification of Suspected Illegal Traffic

issued by the Enforcement Bureau. The following procedures shall apply:

(i)(A) The Enforcement Bureau will issue a Notification of Suspected Illegal Traffic that identifies with as much particularity as possible the suspected illegal traffic; provides the basis for the Enforcement Bureau's reasonable belief that the identified traffic is unlawful; cites the statutory or regulatory provisions the identified traffic appears to violate; and directs the provider receiving the notice that it must comply with this section. The Enforcement Bureau's Notification of Suspected Illegal Traffic shall give the identified provider a minimum of 14 days to comply with the notice. Each notified provider must promptly investigate the identified traffic and report the results of that investigation to the Enforcement Bureau within the timeframe specified in the Notification of Suspected Illegal Traffic. If the provider's investigation determines that it served as the gateway provider for the identified traffic, it must block the identified traffic within the timeframe specified in the Notification of Suspected Illegal Traffic and include in its report to the Enforcement Bureau:

(*1*) A certification that it is blocking the identified traffic and will continue to do so; and

(*2*) A description of its plan to identify and block substantially similar traffic on an ongoing basis.

(B) If the provider's investigation determines that the identified traffic is not illegal, it shall provide an explanation as to why the provider reasonably concluded that the identified traffic is not illegal and what steps it took to reach that conclusion. Absent such a showing, or if the Enforcement Bureau determines based on the evidence that the traffic is illegal despite the provider's assertions, the identified traffic will be deemed illegal. If the notified provider determines during this investigation that it did not serve as the gateway provider for any of the identified traffic, it shall provide an explanation as to how it reached that conclusion and, if it is a non-gateway intermediate or terminating provider for the identified traffic, it must identify the upstream provider(s) from which it received the identified traffic and, if possible, take lawful steps to mitigate this traffic. If the notified provider determines that it is the originating provider, or the traffic otherwise comes from a source that does not have direct access to the U.S. public switched telephone network, it must promptly comply with paragraph (n)(2) of this section by effectively mitigating the identified traffic and reporting to the Enforcement Bureau any steps it has taken to effectively mitigate the identified traffic. If the Enforcement Bureau finds that an approved plan is not blocking substantially similar traffic, the identified provider shall modify its plan to block such traffic. If the Enforcement Bureau finds, that the identified provider continues to allow suspected illegal traffic onto the U.S. network, it may proceed under paragraph (n)(5)(ii) or (iii) of this section as appropriate.

(ii) If the provider fails to respond to the Notification of Suspected Illegal Traffic, the Enforcement Bureau determines that the response is insufficient, the Enforcement Bureau determines that the gateway provider is continuing to allow substantially similar traffic onto the U.S. network after the timeframe specified in the Notification of Suspected Illegal Traffic, or the Enforcement Bureau determines based on the evidence that the traffic is illegal despite the provider's assertions, the Enforcement Bureau shall issue an Initial Determination Order to the gateway provider stating the Bureau's initial determination that the gateway provider is not in compliance with this section. The Initial Determination Order shall include the Enforcement Bureau's reasoning for its determination and give the gateway provider a minimum of 14 days to provide a final response prior to the Enforcement Bureau making a final determination on whether the provider is in compliance with this section.

(iii) If the gateway provider does not provide an adequate response to the Initial Determination Order within the timeframe permitted in that Order or continues to allow substantially similar traffic onto the U.S. network, the Enforcement Bureau shall issue a Final Determination Order finding that the gateway provider is not in compliance with this section. The Final Determination Orders shall be published in EB Docket No. 22–174 at *https://www.fcc.gov/ecfs/search/search-filings.* A Final Determination Order may be issued up to one year after the release date of the Initial Determination Order, and may be based on either an immediate failure to comply with this rule or a determination that the gateway provider has failed to meet its ongoing obligation under this rule to block substantially similar traffic.

(6) When notified by the Commission through its Enforcement Bureau that a Final Determination Order has been issued finding that a gateway provider has failed to block as required under paragraph (n)(5) of this section, block and cease accepting all traffic received directly from the identified gateway provider beginning 30 days after the release date of the Final Determination Order. This paragraph (n)(6) applies to any provider immediately downstream from the gateway provider. The Enforcement Bureau shall provide notification by publishing the Final Determination Order in EB Docket No. 22–174 at *https://www.fcc.gov/ecfs/search/search-filings.* Providers must monitor EB Docket No. 22–174 and initiate blocking no later than 30 days from the release date of the Final Determination Order. A provider that chooses to initiate blocking sooner than 30 days from the release date may do so consistent with paragraph (k)(4) of this section.

(o) A provider that serves as a gateway provider for particular calls must, with respect to those calls, block any calls purporting to originate from a number on a reasonable do-not-originate list. A list so limited in scope that it leaves out obvious numbers that could be included with little effort may be deemed unreasonable. The do-not-originate list may include only:

(1) Numbers for which the subscriber to which the number is assigned has requested that calls purporting to originate from that number be blocked because the number is used for inbound calls only;

(2) North American Numbering Plan numbers that are not valid;

(3) Valid North American Numbering Plan Numbers that are not allocated to a provider by the North American Numbering Plan Administrator; and

(4) Valid North American Numbering Plan numbers that are allocated to a provider by the North American Numbering Plan Administrator, but are unused, so long as the provider blocking the calls is the allocatee of the number and confirms that the number is unused or has obtained verification from the allocatee that the number is unused at the time of blocking.

(p) Paragraphs (n)(1) and (o) of this section may contain an information-collection and/or recordkeeping requirement. Compliance with paragraphs (n)(1) and (o) will not be required until this paragraph (p) is removed or contains a compliance date, which will not occur until after the Office of Management and Budget completes review of such requirements pursuant to the Paperwork Reduction Act or until after the Consumer and Governmental Affairs Bureau determines that such review is not required. The Commission directs the Consumer and Governmental Affairs Bureau to announce a compliance date for paragraphs (n)(1) and (o) by subsequent Public Notice and

notification in the **Federal Register** and to cause paragraphs (n)(1) and (o) to be revised accordingly.

## Subpart HH—Caller ID Authentication

■ 5. Amend § 64.6300 by:

■ a. Redesignating paragraphs (d) through (m) as paragraphs (e) through (n);

■ b. Adding a new paragraph (d); and

■ c. Revising newly redesignated paragraph (g).

The addition and revision read as follows:

**§ 64.6300 Definitions.**

* * * * *

(d) *Gateway provider.* The term ''gateway provider'' means a U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider. For purposes of this paragraph (d):

(1) *U.S.-based* means that the provider has facilities located in the United States, including a point of presence capable of processing the call; and

(2) *Receives a call directly* from a provider means the foreign provider directly upstream of the gateway provider in the call path sent the call to the gateway provider, with no providers in-between.

* * * * *

(g) *Intermediate provider.* The term ''intermediate provider'' means any entity that carries or processes traffic that traverses or will traverse the public switched telephone network at any point insofar as that entity neither originates nor terminates that traffic.

* * * * *

■ 6. Amend § 64.6302 by adding paragraph (c) to read as follows:

**§ 64.6302 Caller ID authentication by intermediate providers.**

* * * * *

(c) Notwithstanding paragraph (b) of this section, a gateway provider must, not later than June 30, 2023, authenticate caller identification information for all calls it receives that use North American Numbering Plan resources that pertain to the United States in the caller ID field and for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call, unless that gateway provider is subject to an applicable extension in § 64.6304.

■ 7. Revise § 64.6303 to read as follows:

**§ 64.6303 Caller ID authentication in non-IP networks.**

(a) Except as provided in §§ 64.6304 and 64.6306, not later than June 30, 2021, a voice service provider shall either:

(1) Upgrade its entire network to allow for the initiation, maintenance, and termination of SIP calls and fully implement the STIR/SHAKEN framework as required in § 64.6301 throughout its network; or

(2) Maintain and be ready to provide the Commission on request with documented proof that it is participating, either on its own or through a representative, including third party representatives, as a member of a working group, industry standards group, or consortium that is working to develop a non-internet Protocol caller identification authentication solution, or actively testing such a solution.

(b) Except as provided in § 64.6304, not later than June 30, 2023, a gateway provider shall either:

(1) Upgrade its entire network to allow for the processing and carrying of SIP calls and fully implement the STIR/SHAKEN framework as required in § 64.6302(c) throughout its network; or

(2) Maintain and be ready to provide the Commission on request with documented proof that it is participating, either on its own or through a representative, including third party representatives, as a member of a working group, industry standards group, or consortium that is working to develop a non-internet Protocol caller identification authentication solution, or actively testing such a solution.

(3) Paragraph (b) of this section may contain an information collection and/or recordkeeping requirement. Compliance with paragraph (b) will not be required until this paragraph (b)(3) is removed or contains a compliance date, which will not occur until after the Office of Management and Budget completes review of such requirements pursuant to the Paperwork Reduction Act or until after the Wireline Competition Bureau determines that such review is not required. The Commission directs the Wireline Competition Bureau to announce a compliance date for paragraph (b) by subsequent Public Notice and notification in the **Federal Register** and to cause paragraph (b) to be revised accordingly.

■ 8. Amend § 64.6304 by revising paragraphs (b) and (d) to read as follows:

**§ 64.6304 Extension of implementation deadline.**

* * * * *

(b) *Voice service providers and gateway providers that cannot obtain an SPC token.* Voice service providers that are incapable of obtaining an SPC token due to Governance Authority policy are exempt from the requirements of § 64.6301 until they are capable of obtaining a SPC token. Gateway providers that are incapable of obtaining an SPC token due to Governance Authority policy are exempt from the requirements of § 64.6302(c) regarding call authentication.

* * * * *

(d) *Non-IP Networks.* Those portions of a voice service provider or gateway provider's network that rely on technology that cannot initiate, maintain, carry, process, and terminate SIP calls are deemed subject to a continuing extension. A voice service provider subject to the foregoing extension shall comply with the requirements of § 64.6303(a) as to the portion of its network subject to the extension, and a gateway provider subject to the foregoing extension shall comply with the requirements of § 64.6303(b) as to the portion of its network subject to the extension.

* * * * *

■ 9. Revise § 64.6305 to read as follows:

**§ 64.6305 Robocall mitigation and certification.**

(a) *Robocall mitigation program requirements for voice service providers.* (1) Any voice service provider subject to an extension granted under § 64.6304 that has not fully implemented the STIR/SHAKEN authentication framework on its entire network shall implement an appropriate robocall mitigation program as to those portions of its network on which it has not implemented the STIR/SHAKEN authentication framework.

(2) Any robocall mitigation program implemented pursuant to paragraph (a)(1) of this section shall include reasonable steps to avoid originating illegal robocall traffic and shall include a commitment to respond fully and in a timely manner 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.

(b) *Robocall mitigation program requirements for gateway providers.* (1) Each gateway provider shall implement an appropriate robocall mitigation program with respect to calls that use North American Numbering Plan resources that pertain to the United States in the caller ID field.

(2) Any robocall mitigation program implemented pursuant to paragraph (b)(1) of this section shall include reasonable steps to avoid carrying or processing illegal robocall traffic and shall include a commitment to respond fully and 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 carry or process calls.

(3) Paragraph (b)(2) of this section may contain an information-collection and/or recordkeeping requirement. Compliance with paragraph (b)(2) will not be required until this paragraph (b)(3) is removed or contains a compliance date, which will not occur until after the Office of Management and Budget completes review of such requirements pursuant to the Paperwork Reduction Act or until after the Wireline Competition Bureau determines that such review is not required. The Commission directs the Wireline Competition Bureau to announce a compliance date for paragraph (b) of this section by subsequent Public Notice and notification in the **Federal Register** and to cause paragraph (b) to be revised accordingly.

(c) *Certification by voice service providers in the Robocall Mitigation Database.* (1) Not later than June 30, 2021, a voice service provider, regardless of whether it is subject to an extension granted under § 64.6304, shall certify to one of the following:

(i) It has fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it originates are compliant with § 64.6301(a)(1) and (2);

(ii) It has implemented the STIR/SHAKEN authentication framework on a portion of its network and calls it originates on that portion of its network are compliant with § 64.6301(a)(1) and (2), and the remainder of the calls that originate on its network are subject to a robocall mitigation program consistent with paragraph (a) of this section; or

(iii) It has not implemented the STIR/SHAKEN authentication framework on any portion of its network, and all of the calls that originate on its network are subject to a robocall mitigation program consistent with paragraph (a) of this section.

(2) A voice service provider that certifies that some or all of the calls that originate on its network are subject to a robocall mitigation program consistent with paragraph (a) of this section shall include the following information in its certification in English or with a certified English translation:

(i) Identification of the type of extension or extensions the voice service provider received under § 64.6304, if the voice service provider is not a foreign voice service provider;

(ii) The specific reasonable steps the voice service provider has taken to avoid originating illegal robocall traffic as part of its robocall mitigation program; and

(iii) A statement of the voice service provider's commitment to respond fully and in a timely manner 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.

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

(i) Be filed in the appropriate portal on the Commission's website; and

(ii) Be signed by an officer in conformity with 47 CFR 1.16.

(4) A voice service provider filing a certification shall submit the following information in the appropriate portal on the Commission's website:

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

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

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

(iv) Whether the voice service provider is a foreign voice service provider; and

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

(5) A voice service provider shall update its filings within 10 business days of any change to the information it must provide pursuant to paragraphs (c)(1) through (4) of this section.

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

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

(6) Paragraph (c)(2) of this section may contain an information collection and/or recordkeeping requirement. Compliance with paragraph (c)(2) will not be required until this paragraph (c)(6) is removed or contains a compliance date, which will not occur until after the Office of Management and Budget completes review of such requirements pursuant to the Paperwork Reduction Act or until after the Wireline Competition Bureau determines that such review is not required. The Commission directs the Wireline Competition Bureau to announce a compliance date for paragraph (c)(2) by subsequent Public Notice and notification in the **Federal Register** and to cause paragraph (c)(2) to be revised accordingly.

(d) *Certification by gateway providers in the Robocall Mitigation Database.* (1) 30 days following **Federal Register** notification of OMB approval of the relevant information collection obligations, a gateway provider shall certify to one of the following:

(i) It has fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it carries or processes are compliant with § 64.6302(b);

(ii) It has implemented the STIR/SHAKEN authentication framework on a portion of its network and calls it carries or processes on that portion of its network are compliant with § 64.6302(b); or

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

(2) A gateway provider shall include the following information in its certification made pursuant to paragraph (d)(1) of this section, in English or with a certified English translation:

(i) Identification of the type of extension or extensions the gateway provider received under § 64.6304;

(ii) The specific reasonable steps the gateway provider has taken to avoid carrying or processing illegal robocall traffic as part of its robocall mitigation program, including a description of how it has complied with the know-your-upstream provider requirement in § 64.1200(n)(4); and

(iii) A statement of the gateway provider's commitment to respond fully and 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 carry or process calls.

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

(i) Be filed in the appropriate portal on the Commission's website; and

(ii) Be signed by an officer in conformity with 47 CFR 1.16.

(4) A gateway provider filing a certification shall submit the following information in the appropriate portal on the Commission's website:

(i) The gateway provider's business name(s) and primary address;

(ii) Other business names in use by the gateway provider;

(iii) All business names previously used by the gateway provider;

(iv) Whether the gateway provider or any affiliate is also a foreign voice service provider; and

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

(5) A gateway provider shall update its filings within 10 business days of any change to the information it must provide pursuant to paragraphs (d)(1) through (4) of this section, subject to the conditions set forth in paragraphs (c)(5)(i) and (ii) of this section.

(6) Paragraphs (d)(1) through (5) of this section may contain an information collection and/or recordkeeping requirement. Compliance with paragraphs (d)(1) through (5) will not be required until this paragraph (d)(6) is removed or contains a compliance date, which will not occur until after the Office of Management and Budget completes review of such requirements pursuant to the Paperwork Reduction Act or until after the Wireline Competition Bureau determines that such review is not required. The Commission directs the Wireline Competition Bureau to announce a compliance date for paragraph (d) of this section by subsequent Public Notice and notification in the **Federal Register** and to cause paragraph (d) to be revised accordingly.

(e) *Intermediate provider and voice service provider obligations*—(1) *Accepting traffic from domestic voice service providers.* Intermediate providers and voice service providers shall accept calls directly from a domestic voice service provider only if that voice service provider's filing appears in the Robocall Mitigation Database in accordance with paragraph (c) of this section and that filing has not been de-listed pursuant to an enforcement action.

(2) *Accepting traffic from foreign providers.* Beginning 90 days after the deadline for filing certifications pursuant to paragraph (d)(1) of this section, intermediate providers and voice service providers shall accept calls directly from a foreign voice service provider or foreign intermediate provider that uses North American Numbering Plan resources that pertain to the United States in the caller ID field to send voice traffic to residential or business subscribers in the United States, only if that foreign provider's filing appears in the Robocall Mitigation Database in accordance with paragraph (c) of this section and that filing has not been de-listed pursuant to an enforcement action.

(3) *Accepting traffic from gateway providers.* Beginning 90 days after the deadline for filing certifications pursuant to paragraph (d) of this section, intermediate providers and voice service providers shall accept calls directly from a gateway provider only if that gateway provider's filing appears in the Robocall Mitigation Database in accordance with paragraph (d) of this section, showing that the gateway provider has affirmatively submitted the filing, and that filing has not been de-listed pursuant to an enforcement action.

(4) *Public safety safeguards.* Notwithstanding paragraphs (e)(1) through (3) of this section:

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

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

[FR Doc. 2022–13436 Filed 7–15–22; 8:45 am]

**BILLING CODE 6712–01–P**