202–622–2480; Assistant Director for Regulatory Affairs, 202–622–4855; or Assistant Director for Compliance, 202–622–2490.

SUPPLEMENTARY INFORMATION:

Electronic Availability

This document and additional information concerning OFAC are available on OFAC's website: *https://ofac.treasury.gov.*

Background

On May 31, 2023, OFAC issued GL 69 to authorize certain transactions otherwise prohibited by the Russian Harmful Foreign Activities Sanctions Regulations, 31 CFR part 587. GL 69 was made available on OFAC's website (*https://ofac.treasury.gov*) when it was issued. The text of this GL is provided below.

OFFICE OF FOREIGN ASSETS CONTROL

Russian Harmful Foreign Activities Sanctions Regulations 31 CFR Part 587

GENERAL LICENSE NO. 69

Authorizing Certain Debt Securities Servicing Transactions Involving International Investment Bank

(a) Except as provided in paragraph (c) of this general license, all transactions prohibited by Executive Order (E.O.) 14024 that are ordinarily incident and necessary to the processing of interest or principal payments on debt securities issued by International Investment Bank (IIB) prior to April 12, 2023 are authorized through 12:01 a.m. eastern daylight time June 30, 2023, provided that such interest or principal payments are not made to persons located in the Russian Federation and that any payments to a blocked person, wherever located, are made into a blocked account in accordance with the Russian Harmful Foreign Activities Sanctions Regulations, 31 CFR part 587 (RuHSR).

Note to paragraph (a). For the purposes of this general license, the term ''person located in the Russian Federation'' includes persons in the Russian Federation, individuals ordinarily resident in the Russian Federation, and entities incorporated or organized under the laws of the Russian Federation or any jurisdiction within the Russian Federation.

(b) U.S. financial institutions are authorized to unblock interest or principal payments that were blocked on or after April 12, 2023 but before May 31, 2023 on debt securities issued by IIB prior to April 12, 2023, provided that the funds are unblocked solely to effect transactions authorized in paragraph (a) of this general license.

Note to paragraph (b). U.S. financial institutions unblocking property pursuant to paragraph (b) of this general license are required to file an unblocking report pursuant to 31 CFR 501.603.

(c) This general license does not authorize:

(1) Any transactions prohibited by Directive 2 under E.O. 14024, *Prohibitions Related to Correspondent or Payable-Through Accounts and Processing of Transactions Involving Certain Foreign Financial Institutions;*

(2) Any transactions prohibited by Directive 4 under E.O. 14024, *Prohibitions Related to Transactions Involving the Central Bank of the Russian Federation, the National Wealth Fund of the Russian Federation, and the Ministry of Finance of the Russian Federation;* or

(3) Any transactions otherwise prohibited by the RuHSR, including transactions involving any person blocked pursuant to the RuHSR other than the blocked person described in paragraph (a) of this general license, unless separately authorized.

Andrea M. Gacki,

Director, Office of Foreign Assets Control.

Dated: May 31, 2023

Andrea M. Gacki,

Director, Office of Foreign Assets Control.

[FR Doc. 2023–13117 Filed 6–20–23; 8:45 am]

BILLING CODE 4810–AL–P

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Parts 0, 1, and 64

[WC Docket No. 17–97; FCC 23–18, FR ID 138840]

Call Authentication Trust Anchor

AGENCY: Federal Communications Commission.

ACTION: Final rule.

SUMMARY: In this document, the Federal Communications Commission (Commission) takes further steps to combat illegally spoofed robocalls by strengthening and expanding caller ID authentication and robocall mitigation obligations and creating new mechanisms to hold providers accountable for violations of the Commission's rules.

DATES: *Effective date:* This rule is effective August 21, 2023, except for the amendments codified at 47 CFR 64.6303(c) (amendatory instruction 9) and 64.6305(d), (e), (f), and (g) (amendatory instruction 12) which are delayed. The Commission will publish a document in the **Federal Register** announcing the effective dates for the delayed amendments to 47 CFR 64.6303(c) and 64.6305(d), (e), (f), (g).

FOR FURTHER INFORMATION CONTACT: Jonathan Lechter, Competition Policy Division, Wireline Competition Bureau, at (202) 418–0984, *jonathan.lechter@fcc.gov.*

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's *Sixth Report and Order* in WC Docket No. 17–97 adopted on March 16, 2023 and released on March 17, 2023. The document is available for download at *https://docs.fcc.gov/public/attachments/FCC-23-18A1.pdf.* 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

1. In this document, the Commission continues to strengthen and expand caller ID authentication requirements in the Secure Telephony Identity Revisited/Signature-based Handling of Asserted information using toKENs (STIR/SHAKEN) ecosystem by requiring non-gateway intermediate providers that receive unauthenticated calls directly from an originating provider to use STIR/SHAKEN to authenticate those calls. The STIR/SHAKEN framework is a set of technical standards and protocols that enable providers to authenticate and verify caller ID information transmitted with Session Initiation Protocol (SIP) calls. The STIR/SHAKEN framework consists of two components: (1) the technical process of authenticating and verifying caller ID information; and (2) the certificate governance process that maintains trust in the caller ID authentication information transmitted along with a call.

2. Further, with this document, the Commission expands robocall mitigation requirements for all providers, including those that have not yet implemented STIR/SHAKEN because they lack the necessary infrastructure or are subject to an implementation extension. The Commission empowers the Enforcement Bureau with new tools and penalties to hold providers accountable for failing to comply with its rules. The Commission also defines the STIR/SHAKEN obligations of satellite providers.

3. The STIR/SHAKEN caller ID authentication framework protects consumers from illegally spoofed robocalls by enabling authenticated caller ID information to securely travel with the call itself throughout the entire call path. The Commission, consistent with Congress's direction in the Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, adopted rules requiring voice service providers to implement STIR/SHAKEN in the internet Protocol (IP) portions of their voice networks by June 30, 2021, subject to certain exceptions.

Because the TRACED Act defines ''voice service'' in a manner that excludes intermediate providers, the Commission's authentication and Robocall Mitigation Database rules use ''voice service provider'' in this manner. The Commission's rules in 47 CFR 64.1200, many of which the Commission adopted prior to adoption of the TRACED Act, use a definition of ''voice service provider'' that includes intermediate providers. For purposes of this document, 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.

A. Strengthening the Intermediate Provider Authentication Obligation

1. Requiring the First Intermediate Provider To Authenticate Unauthenticated Calls

4. Under the Commission's caller ID authentication rules, intermediate providers are required to authenticate any unauthenticated caller ID information for the SIP calls they receive or, alternatively, cooperate with the industry traceback consortium and timely and fully respond to all traceback requests received from the Commission, law enforcement, and the industry traceback consortium. In the *Fourth Call Blocking Order,* 86 FR 17726 (Apr. 6, 2021), however, the Commission required all providers in the path of a SIP call—including gateway providers and other intermediate providers—to respond fully and in a timely manner to traceback requests. The Commission later enhanced this obligation for gateway providers to require response within 24 hours in the *Fifth Caller ID Authentication Report and Order,* 87 FR 42916 (July 18, 2022). As a result of that action, intermediate providers may decline to authenticate caller ID information given that compliance with the traceback alternative has been made mandatory. In the *Fifth Caller ID Authentication Further Notice of Proposed Rulemaking (FNPRM),* 87 FR 42670 (July 18, 2022), the Commission proposed closing this gap in the STIR/SHAKEN caller ID authentication regime by requiring all U.S. intermediate providers in the path of a SIP call carrying a U.S. number in the caller ID field to authenticate unauthenticated caller ID information, irrespective of their traceback obligations. Based on its review of the record, the Commission adopts its proposal to establish a mandatory caller ID authentication obligation for intermediate providers, but does so on an incremental basis. Specifically, the Commission amends its rules to require any non-gateway intermediate provider that receives an unauthenticated SIP call directly from an originating provider to authenticate the call. Stated differently, the first intermediate provider in the path of an unauthenticated SIP call will now be subject to a mandatory requirement to authenticate the call.

5. The Commission has previously recognized that the STIR/SHAKEN framework has beneficial network effects and becomes more effective as more providers implement it. The record in this proceeding supports expanding STIR/SHAKEN implementation by requiring non-gateway intermediate providers to authenticate unauthenticated calls, regardless of their traceback obligations. Although originating providers are required to authenticate calls under the Commission's rules—with limited exceptions—some originating providers are not capable of implementing STIR/SHAKEN. In other cases, unscrupulous providers may deliberately fail to comply with the Commission's rules. The record shows that the failure of originating providers to sign calls is one of the key weaknesses in the STIR/SHAKEN regime. By requiring intermediate providers to authenticate unauthenticated SIP calls they receive directly from an originating provider, the Commission closes an important loophole in its caller ID authentication scheme, and incorporates calls that would otherwise go unauthenticated into the STIR/SHAKEN framework. Further, intermediate provider authentication will facilitate analytics, blocking, and traceback efforts by providing more information to downstream providers.

6. The Commission recognizes, however, that a mandatory authentication obligation could subject intermediate providers to significant costs. The Commission believes that the goals of the STIR/SHAKEN framework and the public interest are best served by taking a targeted approach to intermediate provider authentication that focuses on the first intermediate provider in the call path. The Commission therefore opts to take an incremental approach to imposing mandatory authentication obligations on intermediate providers, requiring only the first intermediate provider in the path of a SIP call to authenticate unauthenticated caller ID information, rather than requiring all intermediate providers in the path to do so at this time. Intermediate providers should know whether they receive calls directly from an originating provider pursuant to contracts that provide information to the intermediate provider about the originating provider's customers and expectations for handling their traffic. Further, as explained below, the Commission requires non-gateway intermediate providers to take ''reasonable steps'' to mitigate illegal robocall traffic. That duty, along with other requirements of the Commission's rules, may require an intermediate provider to perform the due diligence necessary to understand the sources of the traffic it receives. Accordingly, in the unlikely event that an intermediate provider does not know through its contracts whether it receives calls directly from an originating provider, it should obtain that information to comply with this and other aspects of the Commission's rules. The Commission finds that this approach, which focuses on the beginning of the call path, will directly address the problem of calls entering the call path without being authenticated by originating providers, as described above. The Commission agrees with YouMail that this targeted approach is likely to have the greatest impact on stopping illegally spoofed robocalls. As YouMail argues, apart from the originating provider, the ''best entity to identify and stop the sources of robocalls is the first 'downstream' provider (*i.e.,* the next provider in line that receives calls placed on the originating provider's network).'' While the Commission may consider expanding a call authentication requirement to all intermediate providers in the future, this targeted approach will provide the Commission with an opportunity to evaluate this first mandatory obligation for intermediate providers, together with other pending expansions of the caller ID authentication regime, and determine whether an authentication requirement for more downstream intermediate providers is warranted.

7. The Commission is not persuaded by the arguments submitted by commenters favoring a mandatory authentication requirement for all intermediate providers. For instance, some commenters argue that the Commission's justifications for adopting a mandatory gateway provider authentication requirement apply with equal force to all non-gateway

intermediate providers in the call path. The Commission disagrees. The gateway provider caller ID authentication rules adopted by the Commission in May 2022 apply to the first domestic intermediate provider in the path of a foreign-originated call. The authentication requirement the Commission adopts in this document similarly applies to the first intermediate provider in the path of a U.S.-originated call. Further, there are fewer gateway providers than other domestic intermediate providers. Therefore, the overall industry cost of an authentication obligation imposed on all domestic intermediate providers is likely to be significantly higher than that of the gateway provider obligation. The record in this proceeding simply does not support requiring all intermediate providers to incur those costs at this time if imposing an authentication obligation on the first intermediate provider that receives an unauthenticated call directly from an originating provider can close significant gaps in the Commission's caller ID authentication regime. The Commission finds that the incremental approach it adopts in this document will target a critical gap in its call authentication regime while minimizing the impact of the requirements on industry, including new entrants to the market.

8. The Commission also declines to impose an authentication obligation on all intermediate providers at this time to address instances in which authentication information is ''stripped out'' by the call transiting a non-IP network. The Commission has launched an inquiry into solutions to enable caller ID authentication over non-IP networks, the nexus between non-IP caller ID authentication and the IP transition generally, and on specific steps the Commission can take to encourage the industry's transition to IP. Widespread adoption of a non-IP authentication solution or IP interconnection would result in authenticated caller ID information being preserved and received by the terminating provider. The Commission therefore declines to impose an authentication obligation on all intermediate providers to address circumstances where a call traverses a non-IP network, but may revisit the subject after the Commission concludes its inquiry into whether non-IP authentication or IP interconnection solutions are feasible and can be timely implemented.

9. The Commission notes that the requirement it adopts here for the first intermediate provider to authenticate a call will arise in limited circumstances, such as where the originating provider failed to comply with their own authentication obligation or where the call is sent directly to an intermediate provider from the limited subset of originating providers that lack an authentication obligation. If the originating provider complies with its authentication obligation, the first intermediate provider in the call chain need only meet its preexisting obligation to pass-on that authentication information to the next provider in the chain. Indeed, the first intermediate provider in the call path may completely avoid the need to authenticate calls if it implements contractual provisions with its upstream originating providers stating that it will only accept authenticated traffic. USTelecom requests that the Commission clarify that non-gateway intermediate providers be deemed in compliance with their authentication obligations if they enter into contractual provisions with originating providers and such providers represent and warrant that they do not originate any unsigned traffic and thereafter ''have no reason to know, and do not know, that their upstream provider is sending unsigned traffic it originated.'' The Commission declines to do so, finding that such a clarification is unnecessary. If a non-gateway intermediate provider were to claim that it has complied with the authentication obligation that the Commission adopts pursuant to terms of a contract with an originating provider, the Commission would evaluate such a claim on a case-by-case basis.

2. Applicable STIR/SHAKEN Standards for Compliance

10. Voice service providers and gateway providers are obligated to comply with, at a minimum, the version of the STIR/SHAKEN standards ATIS–1000074, ATIS–1000080, and ATIS–1000084 and all of the documents referenced therein in effect at the time of their respective compliance deadlines, including any errata as of those dates or earlier. In the *Fifth Caller ID Authentication FNPRM,* the Commission proposed that non-gateway intermediate providers comply with, at a minimum, the versions of these standards in effect at the time of their compliance deadline. The Commission also sought comment on whether all providers should be required to comply with the same versions of the standards as non-gateway intermediate providers and whether it should establish a mechanism for updating the standard that providers must comply with going forward, including through delegation to the Wireline Competition Bureau.

11. The Commission adopts its proposal that non-gateway intermediate providers subject to the authentication obligation described above must comply with, at a minimum, the versions of the standards in effect at the time of their authentication compliance deadline (which is addressed in the following section), along with any errata. Like other providers, non-gateway intermediate providers will have the flexibility to assign the level of attestation appropriate to the call based on the applicable level of the standards and the available call information. This approach is supported in the record.

12. The Commission does not at this time require gateway and voice service providers to comply with versions of the standards that came into effect after their respective compliance deadlines. The Commission reiterates, however, that its requirement that providers must comply with a specific version of a standard ''at a minimum,'' means that while providers are required to comply with these standards, they are permitted to comply with any version of the standard that has been ratified by the Alliance for Telecommunications Industry Solutions (ATIS) subsequent to the standard in effect at the time their authentication implementation deadline. However, any later-adopted or improved version of the standards that a provider chooses to incorporate into its STIR/SHAKEN authentication framework must maintain the baseline call authentication functionality exemplified by the versions of ATIS–1000074, ATIS–1000080, and ATIS–1000084 in effect at the time of its respective compliance date.

13. The Commission nevertheless concludes that there may be significant benefits for all providers to comply with standards as they are updated, particularly where updated versions contain critical new features or functions. Requiring all providers to comply with a single, updated standard would also facilitate enforcement of the Commission's rules and ensure that any new features and functions contained in revised standards spread throughout the STIR/SHAKEN ecosystem. Therefore, the Commission adopts a process to incorporate future standards into its rules where appropriate, similar to the process it has adopted to require compliance with updated technical standards in other contexts.

14. Specifically, the Commission delegates to the Wireline Competition Bureau the authority to determine whether to seek comment on requiring compliance with revised versions of the three ATIS standards associated with the STIR/SHAKEN authentication

framework, and all documents referenced therein. The Commission also delegates to the Wireline Competition Bureau the authority to require providers subject to a STIR/SHAKEN authentication requirement to comply with those revised standards, and the authority to set appropriate compliance deadlines regarding such revised standards. Providers will only be required to implement new standards if the benefits to the STIR/SHAKEN ecosystem outweigh any compliance burdens. Additionally, a process based on delegated authority may allow the adoption of revised standards more quickly than would be the case through Commission-level notice and comment procedures.

15. As with voice service and gateway providers, the Commission also requires any non-gateway intermediate provider subject to the authentication obligation described in this section to either upgrade its network to allow for the initiation, maintenance, and termination of SIP calls and fully implement the STIR/SHAKEN framework, or 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. The Commission finds that expanding the requirements of § 64.6303 to non-gateway intermediate providers will ensure regulatory parity and promote the development of non-IP authentication solutions, while offering flexibility to providers that rely on non-IP infrastructure.

3. Compliance Deadlines

16. The Commission sets a December 31, 2023, deadline for the new authentication obligations adopted in this section. By that date, the first non-gateway intermediate provider in the call chain must authenticate unauthenticated calls it receives. The Commission adopts a deadline longer than the six-month deadline it suggested in the *Fifth Caller ID Authentication FNPRM* because intermediate providers need time to deploy the technical capability to comply with the Commission's requirement to authenticate calls, and providers may wish to amend their contracts with upstream originating providers to meet this new requirement. While the record reflects disagreement as to an appropriate intermediate authentication provider deadline, the Commission concludes that a later deadline is not necessary. Implementation of call authentication technology has likely become faster and less costly for many providers than when the Commission first adopted caller ID authentication requirements, particularly for those that have already implemented STIR/SHAKEN in their other roles in the call stream. Moreover, a non-gateway intermediate provider can avoid the need to implement STIR/SHAKEN where it agrees to only accept authenticated traffic from originating providers. The Commission has previously found that six months is sufficient time for providers to evaluate and renegotiate contracts to address new regulatory requirements. Accordingly, the Commission finds that the approximate nine-month period afforded by the December 31, 2023, deadline provides sufficient time for intermediate providers to amend their contracts with originating providers, if necessary, to comply with the Commission's authentication requirement.

B. Mitigation and Robocall Mitigation Database Filing Obligations

17. The Commission next takes action to strengthen the robocall mitigation requirements and Robocall Mitigation Database filing obligations of all providers. As the Commission proposed in the *Fifth Caller ID Authentication FNPRM,* it requires all providers—including intermediate providers and voice service providers without the facilities necessary to implement STIR/SHAKEN—to: (1) take ''reasonable steps'' to mitigate illegal robocall traffic; (2) submit a certification to the Robocall Mitigation Database regarding their STIR/SHAKEN implementation status along with other identifying information; and (3) submit a robocall mitigation plan to the Robocall Mitigation Database. Consistent with its proposal, the Commission also requires downstream providers to block traffic received directly from all intermediate providers that are not in the Robocall Mitigation Database. These actions have significant support in the record. While the Commission does not require providers to take specific steps to meet their mitigation obligations, it does expand the subjects that providers must describe in their filed mitigation plans and the information that providers must submit to the Robocall Mitigation Database.

1. Applying the ''Reasonable Steps'' Mitigation Standard to All Providers

18. The Commission adopts its proposal in the *Fifth Caller ID Authentication FNPRM* to expand to all providers the obligation to mitigate illegal robocalls under the general ''reasonable steps'' standard. Specifically, the Commission now requires all non-gateway intermediate providers, as well as voice service providers that have fully implemented STIR/SHAKEN, to meet the same ''reasonable steps'' general mitigation standard that is currently applied to gateway providers and voice service providers that have not fully implemented STIR/SHAKEN under the Commission's rules. The general mitigation standard the Commission adopts here for all providers is separate from and in addition to the new robocall mitigation program description obligations for all providers discussed below. The Commission also concludes that voice service providers without the facilities necessary to implement STIR/SHAKEN must mitigate illegal robocalls and meet this same mitigation standard.

19. Requiring all providers to mitigate calls under the ''reasonable steps'' standard will ensure that every provider in the call chain is subject to the same duty to mitigate illegal robocalls, promoting regulatory symmetry and administrability. There is significant support in the record for this approach. For providers with a STIR/SHAKEN authentication obligation, these mitigation duties will serve as an ''effective backstop'' to that authentication obligation and, for those without such an obligation, they will act as a key bulwark against illegal robocalls. As the Commission has noted, STIR/SHAKEN is not a silver bullet and has a limited effect on illegal robocalls where the number was obtained lawfully and not spoofed. Requiring all providers to take reasonable steps to mitigate illegal robocalls will help address these limitations in the STIR/SHAKEN regime.

20. As proposed, the Commission retains a general standard that requires providers to take ''reasonable steps'' to mitigate illegal robocall traffic, rather than mandate that providers include specific measures as part of their mitigation plans. The Commission notes, however, that what constitutes a ''reasonable step'' may depend upon the specific circumstances and the provider's role in the call path. While some commenters argue that the Commission should require providers to take specific measures under the ''reasonable steps'' standard, the Commission agrees that providers should retain ''the necessary flexibility in determining which measures to use to mitigate illegal calls on their networks.'' For this reason, the

Commission rejects ZipDX's request that it require providers to describe specific practices in their robocall mitigation plans, including specific know-your-upstream provider and analytics practices. That said, the Commission agrees that promptly investigating and mitigating illegal robocall traffic that is brought to the provider's attention through measures such as internal monitoring and tracebacks would constitute reasonable steps. Pursuant to this standard, a provider's program is ''sufficient if it includes detailed practices that can reasonably be expected to significantly reduce'' the carrying or processing (for intermediate providers) or origination (for voice service providers) of illegal robocalls. Each provider ''must comply with the practices'' that its program requires, and its program is insufficient if the provider ''knowingly or through negligence'' carries or processes calls (for intermediate providers) or originates (for voice service providers) unlawful robocall campaigns.

21. The Commission declines to adopt Voice On The Net Coalition (VON)'s proposal for a safe harbor from contract breach for providers invoking contract termination provisions against providers originating illegal robocall traffic. VON does not explain why such a safe harbor is necessary or the legal authority for the Commission to adopt such a provision, and the Commission finds it outside the scope of this proceeding. Providers' programs must also commit to respond fully, within the time period required by the Commission's rules, to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping illegal robocallers that use its service to originate, carry, or process illegal robocalls. The Commission declines to adopt Electronic Privacy Information Center and National Consumer Law Center (EPIC/NCLC)'s proposal to replace the ''reasonable steps'' general mitigation standard with the ''affirmative, effective measures'' standard found elsewhere in its rules. Under EPIC/NCLC's proposal, a provider would fail to meet this standard if they allow the origination of any illegal robocalls, even where the provider may have taken ''reasonable steps'' to mitigate such calls. The Commission disagrees with EPIC/NCLC's reading of its rules and conclude that these standards work hand-in-hand to prevent illegal robocalls. A key purpose of the ''reasonable steps'' standard is to ensure that providers enact a robocall mitigation program and describe that program in the Robocall Mitigation Database. If the program is not reasonable as described, or if it is not followed, the provider may be held liable. Further, if the steps described in a mitigation program are followed but are not actually effective in stopping illegal robocalls, the originating provider could be held liable for failing to put in place ''affirmative, effective'' measures to stop robocalls if they do not take further action. Regardless of the mitigation standard the Commission adopts, the Commission disagrees with EPIC/NCLC that providers should be held strictly liable for allowing the origination of any illegal robocalls regardless of whether they have taken ''reasonable steps'' to mitigate such calls, as explained in more detail below.

22. The Commission also does not adopt VON's proposal of a ''gross negligence'' standard to evaluate whether a mitigation program is sufficient, rather than the Commission's existing standard, which assesses whether a provider ''knowingly or through negligence'' originates, carries, or processes illegal robocalls. The Commission disagrees that its existing standard ''essentially impose[s] strict liability on providers,'' as VON asserts. On the contrary, if a provider is taking sufficient ''reasonable steps'' to mitigate illegal robocall traffic pursuant to a robocall mitigation program that complies with the Commission's rules, the provider is likely not acting negligently.

23. The Commission declines to adopt a heightened mitigation obligation solely for Voice over internet Protocol (VoIP) providers. The Commission acknowledges that there is evidence that VoIP providers are disproportionally involved in the facilitation of illegal robocalls. However, the Commission agrees with commenters opposing such a heightened standard, because the threat of illegal robocalls is an industry issue and impacts every type of provider. The Commission finds that applying its obligations to providers regardless of the technology used to transmit calls better aligns with the competitive neutrality of the TRACED Act.

24. *Deadlines.* Consistent with the obligation placed on other providers and the limited comments filed in the record, the Commission requires providers newly covered by the general mitigation standard to meet that standard within 60 days following **Federal Register** publication of this document. No commenter argued that a greater length of time is needed to comply, and the Commission finds no reason to depart from the same compliance timeframe previously established for other providers.

2. Expanded Robocall Mitigation Database Filing Obligations

25. The Commission next takes steps to strengthen its Robocall Mitigation Database filing obligations to increase transparency and ensure that all providers act to mitigate illegal robocalls. The Commission previously required voice service providers with a STIR/SHAKEN implementation obligation and those subject to an extension to file certifications in the Robocall Mitigation Database regarding their efforts to mitigate illegal robocalls on their networks—specifically, whether their traffic is either signed with STIR/SHAKEN or subject to a robocall mitigation program. By ''STIR/SHAKEN implementation obligation,'' the Commission means the applicable requirement under its rules that a provider implement STIR/SHAKEN in the IP portions of their networks by a date certain, subject to certain exceptions. When referencing those providers ''without'' a STIR/SHAKEN implementation obligation, the Commission means those providers that are subject to an implementation extension, such as a provider with an entirely non-IP network or one that is unable to obtain the necessary Service Provider Code (SPC) token to authenticate caller ID information, or that lack control over the facilities necessary to implement STIR/SHAKEN. Those voice service providers that certified that some or all of their traffic is ''subject to a robocall mitigation program'' were required to submit a robocall mitigation plan detailing the specific ''reasonable steps'' that they have taken ''to avoid originating illegal robocall traffic.'' The Commission did not specifically require voice service providers without the facilities necessary to implement STIR/SHAKEN to file certifications in the database and had previously concluded that they were not subject to the Commission's implementation requirements.

26. The Commission adopts its proposal to expand the obligation to file a robocall mitigation plan along with a certification in the Robocall Mitigation Database to all providers regardless of whether they are required to implement STIR/SHAKEN—including non-gateway intermediate providers and providers without the facilities necessary to implement STIR/SHAKEN—and expand the downstream blocking duty to providers receiving traffic directly from non-gateway intermediate providers not in the Robocall Mitigation Database. As

proposed, providers with a new Robocall Mitigation Database filing obligation must submit the same basic information as providers that had previously been required to file. The Commission also requires all providers to file additional information in certain circumstances, as explained below.

27. *Universal Robocall Mitigation Database Filing Obligation.* There was overwhelming record support for broadening the Robocall Mitigation Database certification and mitigation plan filing obligation to cover all providers. Like the expanded mitigation obligation above, this approach will ensure that every provider in the call chain is covered by the same basic set of rules and will increase transparency and accountability. The Commission also agrees with USTelecom that requiring non-gateway intermediate providers to file a certification and mitigation plan in the Robocall Mitigation Database will facilitate the Commission's enforcement efforts for those providers, as it will for voice service providers newly obligated to file a mitigation plan.

28. Consistent with its proposal and existing providers' obligations, all providers' robocall mitigation plans must describe the specific ''reasonable steps'' the provider has taken to avoid, as applicable, the origination, carrying, or processing of illegal robocall traffic as part of its robocall mitigation program. A provider that plays more than one ''role'' in the call chain should explain the mitigation steps it undertakes in each role, to the extent those mitigation steps are different.

29. *New Robocall Mitigation Program Description Obligations for All Providers.* Under the Commission's current rules, voice service providers are required to describe the specific ''reasonable steps'' that they have taken ''to avoid originating illegal robocall traffic'' as part of their robocall mitigation programs. Gateway providers are required to address this topic and provide a description of how they have complied with the know-your-upstream provider requirement in § 64.1200(n)(4) of the Commission's rules. The Commission now imposes specific additional requirements for the contents of robocall mitigation plans filed in the Robocall Mitigation Database. Specifically, as part of their obligation to ''describe with particularity'' their robocall mitigation techniques, (1) voice service providers must describe how they are meeting their existing obligation to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls; (2) non-gateway intermediate providers and voice service providers must, like gateway providers, describe any ''know-your-upstream provider'' procedures in place designed to mitigate illegal robocalls; and (3) all providers must describe any call analytics systems they use to identify and block illegal traffic, including whether they use a third-party vendor or vendors and the name of the vendor(s). To comply with the new requirements to describe their ''new and renewing customer'' and ''know-your-upstream provider'' procedures, providers must describe any contractual provisions with end-users or upstream providers designed to mitigate illegal robocalls. The Commission does not expect providers to necessarily submit contractual provisions, but to describe them in general terms, including whether such provisions are typically included in their contracts. The Commission concludes that the obligation to describe these procedures is particularly important for voice service providers without a STIR/SHAKEN implementation obligation. While the Commission does not currently require intermediate providers other than gateway providers to engage in ''know-your-upstream provider'' procedures, if they have put such procedures in place, they must be documented in their robocall mitigation plan. While the Commission does not specifically require providers to use call analytics, doing so may be a ''reasonable step'' to mitigate illegal robocall traffic, depending on the circumstances. For example, if a provider is a reseller, it is likely to rely on any analytics software adopted by its wholesale provider to monitor call traffic. In that case, the reseller should describe this practice in its robocall mitigation plan.

30. In the *Fifth Caller ID Authentication Report and Order,* the Commission required gateway providers to comply with a new requirement to ''know'' their upstream provider and required gateway providers to include in their Robocall Mitigation Database-filed mitigation plan a description of how they have complied with this obligation. In the *Fifth Caller ID Authentication FNPRM,* the Commission sought comment on expanding these two requirements to non-gateway intermediate providers. The Commission continues to study the record on whether to do so. Similarly, the Commission continues to consider whether to adopt its proposal to require all providers to respond to traceback requests within 24 hours as gateway providers are currently required to do.

31. The Commission imposes these new requirements because it has become increasingly clear that provider due diligence and the use of call analytics are key ways to stop illegal robocalls. The public and the Commission's understanding of the steps providers take to scrutinize their relationships with other providers in the call path and analyze their traffic will facilitate compliance with and enforcement of the Commission's rules. Recent actions by the Enforcement Bureau demonstrating that some providers are not including meaningful descriptions in their mitigation plans warrants more prescriptive obligations. There is also specific record support for these new requirements.

32. *Baseline Information Submitted with Robocall Mitigation Database Certifications.* Consistent with existing providers' filing obligations and the Commission's proposal in the *Fifth Caller ID Authentication FNPRM,* all providers newly obligated to submit a certification to the Robocall Mitigation Database pursuant to the requirements adopted herein must submit the following information: (1) whether it has fully, partially, or not implemented the STIR/SHAKEN authentication framework in the IP portions of its network; (2) the provider's business name(s) and primary address; (3) other business name(s) in use by the provider; (4) all business names previously used by the provider; (5) whether the provider is a foreign provider; and, (6) the name, title, department, business address, telephone number, and email address of one person within the company responsible for addressing robocall mitigation-related issues. The certification must be signed by an officer of the company. Consistent with the Commission's proposal and current rules, providers with a new filing obligation must update any information submitted within 10 business days of ''any change in the information'' submitted, ensuring that the information is kept up to date. Certifications and robocall mitigation plans must be submitted in English or with a certified English translation.

33. *Additional Information to be Submitted with Mitigation Plans.* In order to effectively implement its new and modified authentication obligations, in addition to the baseline information currently required of all filers, the Commission also requires providers to submit additional information in their Robocall Mitigation Database certifications. The Commission requires all providers: (1) to submit additional information regarding their role(s) in the call chain; (2) asserting they do not have an obligation to implement STIR/SHAKEN to include more detail regarding the basis of that

assertion; (3) to certify that they have not been prohibited from filing in the Robocall Mitigation Database; and (4) to state whether they are subject to a Commission, law enforcement, or regulatory agency action or investigation due to suspected unlawful robocalling or spoofing and provide information concerning any such actions or investigations.

34. First, to increase transparency for the industry and regulators and better facilitate its evaluation of the mitigation plans detailed in the Robocall Mitigation Database, the Commission requires providers to submit additional information to indicate the role or roles they are playing in the call chain. Specifically, providers must indicate whether they are: (1) a voice service provider with a STIR/SHAKEN implementation obligation serving end-users; (2) a voice service provider with a STIR/SHAKEN obligation acting as a wholesale provider originating calls; (3) a voice service provider without a STIR/SHAKEN obligation; (4) a non-gateway intermediate provider with a STIR/SHAKEN obligation; (5) a non-gateway intermediate provider without a STIR/SHAKEN obligation; (6) a gateway provider with a STIR/SHAKEN obligation; (7) a gateway provider without a STIR/SHAKEN obligation; and/or (8) a foreign provider. This requirement expands upon the existing rule that providers indicate in their Robocall Mitigation Database filings whether they are a foreign provider, voice service provider, and/or gateway provider. The Commission notes that certain provider classes have different obligations under its rules and, as explained above, the ''reasonable steps'' necessary to meet the Commission's mitigation standard may differ based on the provider's role in the call path. The Commission concludes, therefore, that the collection of this information is necessary to allow the public and the Commission to determine whether a specific provider's mitigation steps are reasonable.

35. Second, the Commission expands its requirement that providers with a current Robocall Mitigation Database filing obligation must state in their mitigation plan whether a STIR/SHAKEN extension applies, and apply that rule to all current and new Robocall Mitigation Database filers. Specifically, a filer asserting it does not have an obligation to implement STIR/SHAKEN because of an ongoing extension, or because it lacks the facilities necessary to implement STIR/SHAKEN, must both explicitly state the rule that exempts it from compliance (for example, by explaining that it lacks the necessary facilities to implement STIR/SHAKEN or it cannot obtain an SPC token) and explain in detail why that exemption applies to the filer (for example, by explaining that it is a pure reseller with some facilities, but that they are not sufficient to implement STIR/SHAKEN, or the steps it has taken to diligently pursue obtaining a token). The Commission concludes that this limited expansion of its existing rule is necessary to permit the public and Commission to evaluate why a provider believes it is not subject to all or a subset of the Commission's rules and whether that explanation is reasonable.

36. Third, the Commission requires new and existing filers to certify that they have not been prohibited from filing in the Robocall Mitigation Database pursuant to a law enforcement action, including the new enforcement requirements adopted herein. Filers will be required to certify that they have not been barred from filing in the Robocall Mitigation Database by such an enforcement action. This includes, but is not limited to, instances in which a provider has been removed from the Robocall Mitigation Database and has been precluded from refiling unless and until certain deficiencies have been cured and those in which a provider's authorization to file has been revoked due to continued violations of the Commission's robocall mitigation rules. This information will enhance the effectiveness of the new enforcement measures the Commission adopts herein to impose consequences on repeat offenders of its robocall mitigation rules. The Commission disagrees with Cloud Communications Alliance (CCA) that the same purpose can be served by indicating whether a provider filed under a prior name. This is not sufficient information to facilitate the Commission's rule barring related entities of repeated bad actors from filing in the Robocall Mitigation Database. The Commission also adopts its proposal to require providers to submit information regarding their principals, affiliates, subsidiaries, and parent companies in sufficient detail to facilitate the Commission's ability to determine whether the provider has been prohibited from filing in the Robocall Mitigation Database. The Commission delegates to the Wireline Competition Bureau to determine the form and format of such data.

37. Fourth, the Commission requires all providers to: (1) state whether, at any time in the prior two years, the filing entity (and/or any entity for which the filing entity shares common ownership, management, directors, or control) has been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description; and, if so (2) provide a description of any such action or investigation, including all law enforcement or regulatory agencies involved, the date that any action or investigation was commenced, the current status of the action or investigation, a summary of the findings of wrongdoing made in connection with the action or investigation, and whether any final determinations have been issued. The Commission limits this reporting requirement to formal actions and investigations that have been commenced or issued pursuant to a written notice or other instrument containing findings by the law enforcement or regulatory agency that the filing entity has been or is suspected of the illegal activities itemized above, including, but not limited to, notices of apparent liability, forfeiture orders, state or federal civil lawsuits or criminal indictments, and cease-and-desist notices. Providers that must include confidential information to accurately and fully comply with this reporting requirement, as explained below, may seek confidential treatment of that information pursuant to § 0.459 of the Commission's rules. This information will help the Commission evaluate claims made by providers in their mitigation program descriptions and identify potential violations of its rules. The Commission does not adopt USTelecom's request that the reporting requirement the Commission adopts be limited to public actions and investigations. The Commission finds that limiting the reporting requirement to formal actions and investigations that are public would simply reduce the scope of the reporting requirement and is not necessary to clarify it. The Commission agrees with commenters, however, that providers should not be required to submit information concerning mere inquiries from law enforcement or regulatory agencies or investigations that do not include findings of actual or suspected wrongdoing. Thus, for example, traceback requests, Enforcement Bureau letters of inquiry or subpoenas, or investigative demand letters or subpoenas issued by regulatory agencies or law enforcement would not trigger this obligation because they are not

accompanied by findings of actual or suspected wrongdoing. The Commission does not adopt INCOMPAS's proposal that it exempt formal actions and investigations accompanied by findings of actual or suspected wrongdoing that rely ''solely'' on tracebacks from the disclosure requirement the Commission adopts in this document. As stated above, the Commission excludes traceback requests from the disclosure requirement when they are not accompanied by findings of actual or suspected wrongdoing. When a formal action or investigation based solely on traceback requests is accompanied by findings of actual or suspected wrongdoing made by the Commission, law enforcement, or a regulatory agency, disclosure of that information may be useful in evaluating claims made by providers in their mitigation program descriptions and identifying potential violations of the Commission's rules. The Commission finds that inquiries or investigations that do not contain findings of actual or suspected wrongdoing by the law enforcement or regulatory agency would be of limited value to the Commission in evaluating the certifications and robocall mitigation plans submitted to the Robocall Mitigation Database.

38. Finally, the Commission requires filers to submit their Operating Company Number (OCN) if they have one. An OCN is a prerequisite to obtaining an SPC token, and the Commission concludes that filing the OCN or indicating that they do not have one will allow the Commission to more easily determine whether a provider is meeting its requirement to diligently pursue obtaining a token in order to authenticate their own calls and provides an additional way to determine relationships among providers. The Commission does not require filers to include additional identifying information discussed in the *Fourth Caller ID Authentication FNPRM,* 86 FR 59084 (Oct. 26, 2021). There was no support for doing so, and the Commission finds the incremental benefits of providing additional information beyond the OCN are unclear.

39. *Robocall Mitigation Database Filing Deadlines.* Providers newly subject to the Commission's Robocall Mitigation Database filing obligations must submit a certification and mitigation plan to the Robocall Mitigation Database by the later of: (1) 30 days following publication in the **Federal Register** of notice of approval by the Office of Management and Budget (OMB) of any associated Paperwork Reduction Act (PRA) obligations; or (2) any deadline set by the Wireline Competition Bureau through Public Notice. This approach provides additional flexibility to the Wireline Competition Bureau to provide an extended filing window where circumstances warrant. Existing filers subject to new or modified requirements adopted in this document must amend their filings with the newly required information by the same deadline. If a provider is required to fully implement STIR/SHAKEN but has not done so by the Robocall Mitigation Database filing deadline, it must so indicate in its filing. It must then later update the filing within 10 business days of completing STIR/SHAKEN implementation. The Commission recognizes that some of this information may be considered confidential. Providers may make confidential submissions consistent with the Commission's existing confidentiality rules. Providers may only redact filings to the extent appropriate under the Commission's confidentiality rules.

40. *Refusing Traffic From Unlisted Providers.* As proposed, the Commission extends the prohibition on accepting traffic from unlisted (including de-listed) providers to non-gateway intermediate providers. This proposal is well supported in the record and will close the final gap in the Commission's Robocall Mitigation Database call blocking regime. Under this rule, downstream providers will be prohibited from accepting any traffic from a non-gateway intermediate provider not listed in the Robocall Mitigation Database, either because the provider did not file or their certification was removed as part of an enforcement action. The Commission concludes that a non-gateway intermediate provider Robocall Mitigation Database filing requirement and an associated prohibition against accepting traffic from non-gateway intermediate providers not in the Robocall Mitigation Database will ensure regulatory symmetry. By extending this prohibition to non-gateway intermediate providers, the Commission ensures that downstream providers will no longer be required to determine the ''role'' of the upstream provider on a call-by-call basis to determine whether the call should be blocked. Consistent with the Commission's proposal, and the parallel requirements adopted for accepting traffic from gateway providers and voice service providers, compliance will be required no sooner than 90 days following the deadline for non-gateway intermediate providers to submit a certification to the Robocall Mitigation Database.

41. As a result of non-gateway intermediate providers' affirmative obligation to submit a certification in the Robocall Mitigation Database, downstream providers may not rely upon any non-gateway intermediate provider database registration imported from the intermediate provider registry. Any imported Robocall Mitigation Database entry is not sufficient to meet a non-gateway intermediate 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 non-gateway intermediate providers.

42. *Bureau Guidance.* Consistent with its prior delegations of authority concerning the Robocall Mitigation Database submission process, the Commission directs the Wireline Competition Bureau to make the necessary changes to the Robocall Mitigation Database and to provide appropriate Robocall Mitigation Database filing instructions and training materials as necessary and consistent with this document. The Commission delegates to the Wireline Competition Bureau the authority to specify the form and format of any submissions as well as necessary changes to the Robocall Mitigation Database submission interface. The Commission also delegates to the Wireline Competition Bureau the authority to make the necessary changes to the Robocall Mitigation Database to indicate whether a non-gateway intermediate 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, and to announce its determination as part of its guidance. The Commission also directs the Wireline Competition Bureau to release a public notice upon Office of Management and Budget (OMB) approval of any information collection associated with the Commission's Robocall Mitigation Database filing requirements, announcing OMB approval of its rules, effective dates, and deadlines for filing and for providers to block traffic from non-gateway intermediate providers that have not filed.

C. Enforcement

43. In order to further strengthen its efforts to hold illegal robocallers accountable for their actions, the Commission adopts several enforcement proposals described in the *Fifth Caller*

ID Authentication FNPRM. Specifically, the Commission: (1) adopts a per-call forfeiture penalty for failure to block traffic in accordance with its rules and sets maximum forfeitures for such violations; (2) requires the removal of non-gateway intermediate providers from the Robocall Mitigation Database for violations of its rules, consistent with the standard applied to other filers; (3) establishes an expedited process for provider removal for facially deficient certifications; and (4) establishes rules that would impose consequences on repeat offenders of its robocall mitigation rules. The adoption of more robust enforcement tools is supported in the record.

1. Per Call Maximum Forfeitures

44. The Commission first adopts its proposal to establish a forfeiture penalty on a per-call basis for violations of its robocall blocking rules in 47 CFR 64.1200 through 64.1204 and 47 CFR 64.6300 through 64.6308. Commenters generally agreed that aggressive penalties are appropriate. Mandatory blocking is an important tool for protecting American consumers from illegal robocalls. As the Commission has found in its previous robocalling orders and enforcement actions, illegal robocalls cause significant consumer harm. Penalties for failure to comply with mandatory blocking requirements must deter noncompliance and be sufficient to ensure that entities subject to these requirements are unwilling to risk suffering serious economic harm.

45. Consistent with its proposal, the Commission authorizes the maximum forfeiture amount for each violation of the mandatory blocking requirements of $23,727 per call. This is the maximum forfeiture amount the Commission's rules permit it to impose on non-common carriers. Although common carriers may be assessed a maximum forfeiture of $237,268 for each violation, the Commission finds that it should not impose a greater penalty on one class of providers than another for purposes of the mandatory blocking requirements. The Commission also sets a base forfeiture amount of $2,500 per call because it concludes that the failure to block results in a similar consumer harm as the robocall itself (*e.g.,* the consumer receives the robocall itself). The Commission finds that a $2,500 base forfeiture is reasonable in comparison to the $4,500 base forfeiture for violations of the Telephone Consumer Protection Act of 1991 (TCPA). While the failure to block produces significant consumer harm, the harm is not as great and does not carry the same degree of culpability as the initiator of an illegal robocall campaign who may have committed a TCPA violation. While the Commission sought comment on whether it should consider specific additional mitigating or aggravating factors, it did not receive sufficient comment to provide a basis for doing so. As with other violations of its rules, however, existing upward and downward adjustment criteria in § 1.80 of the Commission's rules may apply. Additionally, there may be pragmatic factors in its prosecutorial discretion in calculating the total forfeiture amount—particularly when there is a very large number of calls at issue—as the Commission has done in its enforcement actions pursuant to the TCPA and those actions taken against spoofing.

2. Provider Removal From the Robocall Mitigation Database

46. The Commission also adopts its proposal to provide for the removal of non-gateway intermediate providers from the database for violations of its rules. In the *Second Caller ID Authentication Report and Order,* 85 FR 73360 (Nov. 17, 2020), the Commission set forth consequences for voice service providers that file a deficient robocall mitigation plan or that ''knowingly or negligently'' originate illegal robocall campaigns, including removal from the Robocall Mitigation Database. Gateway providers are now subject to the same rules for calls that they carry or process. To promote regulatory symmetry, the Commission concludes that non-gateway intermediate providers should face similar consequences.

47. Specifically, the Commission finds that a non-gateway intermediate provider with a deficient certification—such as when the certification describes a program that is unreasonable, or if it determines that a provider knowingly or negligently carries or processes illegal robocalls—the Commission will take appropriate enforcement action. This may include, among other actions, removing a certification from the database after providing notice to the intermediate provider and an opportunity to cure the filing, requiring the intermediate provider to submit to more specific robocall mitigation requirements, and/or proposing the imposition of a forfeiture. The Commission declines, however, to adopt other reasons to remove providers from the database. The Commission concludes that the existing basis for removal is appropriately tailored to the underlying purpose of the Robocall Mitigation Database—to facilitate detection and elimination of illegal robocall traffic. As proposed, the Commission explicitly expands its delegation of authority to the Enforcement Bureau to de-list or exclude a provider from the Robocall Mitigation Database to include the removal of non-gateway intermediate providers.

48. Downstream providers must refuse traffic sent by a non-gateway intermediate provider that is not listed in the Robocall Mitigation Database, as described above and consistent with the existing safeguards applicable to the Commission's existing rules for refusing traffic for calls to 911, public safety answering points, and government emergency numbers. The Commission agrees with VON that any sanctions for failure to block calls from a provider removed from the database should not occur without sufficient notice to the industry. The Commission concludes, however, that the existing Enforcement Bureau process, where providers are given two business days to block calls following Commission notice of removal from the database, is sufficient, as it appropriately balances the public's interest in blocking unwanted robocalls against the need to allow providers sufficient time to take the necessary steps to block traffic.

3. Expedited Removal Procedure for Facially Deficient Filings

49. The Commission agrees with commenters that there are certain instances in which a provider should be removed from the Robocall Mitigation Database on an expedited basis. Specifically, the Commission finds that where the Enforcement Bureau determines that a provider's filing is facially deficient, the Enforcement Bureau may remove a provider from the Robocall Mitigation Database using an expedited two-step procedure, which entails providing notice and an opportunity to cure the deficiency. This streamlined process will allow the Enforcement Bureau to move more quickly against providers whose filings clearly fail to meet the Commission's requirements.

50. In the *Second Caller ID Authentication Report and Order,* the Commission required that providers be given notice of any deficiencies in their certification and an opportunity to cure prior to removal from the Robocall Mitigation Database, but did not prescribe a specific removal procedure. Pursuant to that requirement and the Commission's prior delegation, the Wireline Competition Bureau and Enforcement Bureau have implemented the following three-step removal procedure: (1) the Wireline Competition Bureau contacts the provider, notifying

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

51. While this procedure is appropriate in cases where there may be questions about the sufficiency of the steps described in a mitigation plan, the Commission concludes that an expedited approach is warranted where the certification is facially deficient. A certification is ''facially deficient'' where the provider fails to submit a robocall mitigation plan within the meaning of the Commission's rules. That is, it fails to submit any information regarding the ''specific reasonable steps'' it is taking to mitigate illegal robocalls. While it is not practical to provide an exhaustive list of reasons why a filing would be considered ''facially deficient,'' examples include, without limitation, instances where the provider only submits: (1) a request for confidentiality with no underlying substantive filing; (2) only non-responsive data or documents (*e.g.,* a screenshot from the Commission's website of a provider's FCC Registration Number data or other document that does not describe robocall mitigation efforts); (3) information that merely states how STIR/SHAKEN generally works, with no specific information about the provider's own robocall mitigation efforts; or (4) a certification that is not in English and lacks a certified English translation. In these and similar cases, the Commission need not reach the question of whether the steps the provider is taking to mitigate robocalls are reasonable because the provider has failed to submit even the most basic information required to do so.

52. The Commission concludes that where a provider's filing is facially deficient, it has ''willfully'' violated its Robocall Mitigation Database filing obligation within the meaning of that term in section 9(b) of the Administrative Procedure Act (APA), 5 U.S.C. 558(c), which applies to revocations of licenses. Although the Commission does not reach a definitive conclusion here, the removal of a provider's certification from the Robocall Mitigation Database—which will lead to the mandatory blocking of the provider's traffic by downstream providers—is arguably equivalent to the revocation of a license. This finding is consistent with precedent concluding that a party acts ''willfully'' within the meaning of section 558(c) where it acts with ''careless disregard.'' As such, where a ''willful'' violation has occurred, the provider's Robocall Mitigation Database certification may be removed without a separate notice prior to the initiation of an ''agency proceeding'' to remove the certification. While the Commission does not specifically conclude that a Robocall Mitigation Database certification is a license within the meaning of that section, the Commission's expedited procedure would be compliant with section 558 if it reached such a conclusion. The Commission does not adopt Professional Association for Customer Engagement (PACE)'s proposal to provide a complete list of reasons for why a provider's filing might be facially deficient, and the specific steps it must take in response to avoid removal. It is not practical to provide an exhaustive list of all potential examples of facially deficient filings and methods to cure such deficiencies. Further, attempting to do so would limit the Commission's flexibility to respond to changing tactics by bad actors and could provide a roadmap for bad actors to avoid expedited removal. Moreover, the Commission concludes that PACE's due process concerns are addressed under the expedited removal process it adopts: The Enforcement Bureau's notice to the provider in the first step will explain the basis for its conclusion that the filing is facially deficient, while the second step offers providers an opportunity to cure that deficiency prior to removal. Therefore, the Commission adopts the following two-step expedited procedure for removing a facially deficient certification: (1) issuance of a notice by the Enforcement Bureau to the provider explaining the basis for its conclusion that the certification is facially deficient and providing an opportunity for the provider to cure the deficiency or explain why its certification is not deficient within 10 days; and (2) if the deficiency is not cured or the provider fails to establish that there is no deficiency within that 10-day period, the Enforcement Bureau will issue an order removing the provider from the database. The Commission notes that a number of providers have responded within 14 days to Enforcement Bureau requests to correct their deficient filings and concludes that employing a marginally shorter time period for this expedited process will further the Commission's interest in swiftly resolving these willful violations without materially affecting a providers' ability to respond to the Enforcement Bureau's notice.

53. The Commission finds that this expedited two-step procedure is also consistent with providers' Fifth Amendment due process rights under the Supreme Court's three factor test. While providers have a significant ''private interest'' under the first factor of the test that would be affected by removal from the Robocall Mitigation Database, the risk of an erroneous deprivation of such interest through the procedures used and the probable value, if any, of additional or substitute procedural safeguards under the second factor is exceedingly low, given that (1) the filings in question are facially deficient, and (2) providers would have a reasonable opportunity to cure the deficient filings by submitting a valid robocall mitigation plan. Given the extremely low risk of erroneous deprivation of a private interest in these situations, the Commission finds that these first two factors do not outweigh the third factor—the ''Government's interest''—which is very weighty here: The Government has a strong interest in ensuring that providers adopt valid robocall mitigation plans as soon as possible to further its continuing efforts to reduce the number of illegal robocalls and harm to consumers, and in blocking traffic of providers that are unable or unwilling to implement or document effective mitigation measures.

54. The Commission concludes that this expedited approach is preferable to EPIC/NCLC's proposal to automatically remove certain ''high-risk'' VoIP providers from the Robocall Mitigation Database or impose forfeitures through a bespoke, expedited process. As explained above, the Commission does not believe that a separate set of rules for VoIP providers is appropriate and the expedited procedure the Commission adopts in this document complies with the APA and due process. EPIC/NCLC do not explain how removal from the database prior to any opportunity to respond is consistent with the APA or due process.

4. Consequences for Continued Violations

55. In order to address continued violations of its robocall mitigation rules, the Commission proposed in the *Fifth Caller ID Authentication FNPRM* to subject repeat offenders to proceedings to revoke their section 214 operating authority and to ban offending companies and/or their individual company owners, directors, officers, and principals from future significant association with entities regulated by the Commission. The Commission further proposed to find that providers that are not common carriers operating pursuant to blanket section 214 authority hold other Commission authorizations sufficient to subject them to the Commission's jurisdiction for purposes of enforcing its rules pertaining to preventing illegal robocalls. The Commission also proposed to find that providers not classified as common carriers but that are registered in the Robocall Mitigation Database hold a Commission certification such that they are subject to the Commission's jurisdiction. The Commission adopts its proposal to revoke the section 214 operating authority of entities that engage in continued violations of its robocall mitigation rules. The Commission also finds that non-common carriers holding Commission authorizations and/or certifications are similarly subject to revocation of their authorizations and/or certifications. The Commission further finds that it will consider whether it is in the public interest for individual company owners, directors, officers, and principals of entities for which the Commission has revoked an authority or a certification, or for other entities with which those individuals are affiliated, to obtain future Commission authorizations, licenses, or certifications at the time that they apply for them.

56. *Revocation of Section 214 Authority and Other Commission Authorizations.* In the *Fifth Caller ID Authentication FNPRM,* the Commission proposed to find that entities engaging in continued violations of its robocall mitigation rules, be subject to revocation of their section 214 operating authority, where applicable. The Commission concludes that the ''robocall mitigation rules'' within the scope of this requirement means the specific obligations to: (1) implement a robocall mitigation program that includes specific ''reasonable steps'' to mitigate illegal robocalls and comply with the steps outlined in the plan; (2) submit a plan describing the mitigation program to the Robocall Mitigation database; and (3) not accept traffic from providers not in the Robocall Mitigation database. This includes obligations that the Commission previously adopted as well as those that it adopts in this document.

57. The Commission concludes that this requirement also pertains to continued violation of providers' authentication obligations. While in certain instances the Commission has referred to provider mitigation obligations as separate from authentication, the Commission has also concluded that they work hand in hand to stop illegal robocalls. Indeed, analytics providers often use authentication information to determine whether to block or label a call. The Commission therefore concludes that call authentication serves to mitigate illegal robocalls, and failure to follow the Commission's authentication rules falls within the scope of the enforcement authority it adopts in this document.

58. The Commission did not receive comments regarding the scope of the specific rules covered by the consequences proposed in the *Fifth Caller ID Authentication FNPRM.* The Commission finds, however, that it is reasonable to fully enforce the foregoing robocall mitigation rules by holding accountable those who engage in continued violations of those rules. The Commission will exercise its ability to revoke the section 214 authorizations for providers engaging in continued violations of those rules, consistent with its long-standing authority to revoke the section 214 authority of any provider for serious misconduct.

59. The Commission's authority to revoke section 214 authority in order to protect the public interest is well established. The Commission intends to apply that authority as necessary to address entities engaging in continued violations of its rules. Specifically, an entity engaging in continued violations of the Commission's robocall mitigation rules as defined in this section will be required to explain to the Enforcement Bureau why the Commission should not initiate proceedings to revoke its domestic and/or international section 214 authorizations. Consistent with established Commission procedures, the Commission may then adopt an order to institute a proceeding to revoke domestic and/or international section 214 authority. Should the entity fail to address concerns regarding its retention of section 214 authority, the Commission would then issue an Order on Revocation consistent with its authority to revoke section 214 authority when warranted to protect the public interest.

60. The Commission also adopts its proposals that providers not classified as common carriers but that hold other types of Commission authorizations, including a certification as a result of being registered in the Robocall Mitigation Database, are subject to the Commission's jurisdiction for the purpose of the consequences the Commission adopts in this section. Interconnected VoIP providers are subject to Title II of the Communications Act of 1934, as amended (Communications Act or Act) through their requirement to file applications to discontinue service under section 214 and § 63.71 of the Commission's rules. As explained below, this approach does not constitute an improper exercise of jurisdiction over domestic non-common carriers or foreign providers. The *Fifth Caller ID Authentication FNPRM* listed the providers that the Commission contemplated would be subject to its enforcement authority. These providers have domestic and international section 214 authorizations, have applied for and received authorization for direct access to numbering resources, are designated as eligible telecommunications carriers under section 214(e) of the Communications Act in order to receive federal universal service support, or are registered in the Robocall Mitigation Database. Where the Commission grants a right or privilege, it unquestionably has the right to revoke or deny that right or privilege in appropriate circumstances. In addition, holders of these and all Commission authorizations have a clear and demonstrable duty to operate in the public interest. Continued violations of the Commission's robocall mitigation rules are wholly inconsistent with the public interest, and the Commission finds it necessary to exercise its authority to institute a proceeding and, if warranted, revoke the authorizations, licenses, and/or certifications of all repeat offenders. Indeed, there is no opposition in the record to the Commission instituting revocation proceedings when warranted, and the Commission agrees with VON that when providers, including those without section 214 authority, have clearly and repeatedly been responsible for originating or transporting illegal robocalls and have had a sufficient opportunity to be heard through the enforcement process, there may be grounds for termination of Commission authorizations. The Commission's established section 214 revocation

process described above satisfies due process requirements, and the Commission intends to apply it to all entities that it finds to be continually violating its robocall mitigation rules.

61. *Future Review of Entities, Individual Company Owners, Directors, Officers, and Principals Applying for Commission Authorizations, Licenses, or Certifications.* Once the Commission has revoked the section 214 or other Commission authorization, license, or certification of an entity that has engaged in continued violations of its robocall mitigation rules, the Commission will consider the public interest impact of granting other future Commission authorizations, licenses, or certifications to the entity that was subject to the revocation, as well as individual company owners, directors, officers, and principals (either individuals or entities) of such entities. The Commission expects that owners, directors, officers, and principals, whether or not they have control of the entity, have influence, management, or supervisory responsibilities for the entity subject to the revocation. The Commission will consider the public interest impact as part of its established review processes for Commission applications at the time that they are filed. For example, a principal of a provider that had its section 214 authority revoked or that was removed from the Robocall Mitigation Database as a result of an enforcement action may be subject to a denial of other Commission authorizations, licenses, or certifications, including for international section 214 authority, or for approval to acquire an entity that holds blanket domestic section 214 authority or international section 214 authority. This is consistent with the Commission's current process in which it reviews many public interest factors in determining whether to grant an application, including whether an applicant for a license has the requisite citizenship, character, financial, technical, and other qualifications. To ensure that the Commission can accurately identify individual company owners, directors, officers, and principals of an entity for which it revoked authority, the Commission intends to rely on information contained in providers' registrations filed in the Robocall Mitigation Database. Where that information is insufficient for this purpose, the Commission will require entities undergoing revocation proceedings to identify their individual company owners, directors, officers, and principals as part of the revocation process.

62. The Commission proposed in the *Fifth Caller ID Authentication FNPRM* that principals and others associated with entities subject to revocation would be banned from holding a 5% or greater ownership interest in any entity that applies for or already holds any FCC license or instrument of authorization for the provision of a regulated service subject to Title II of the Act or of any entity otherwise engaged in the provision of voice service for a period of time to be determined. The record contains no information on how the Commission would undertake the complex process of identifying the providers or applicants that would be impacted by the 5% ownership trigger threshold, or whether it would risk negatively impacting the operations and customers of providers associated with the targeted principal, but which were not involved in the robocall offenses. Should the Commission see an increased volume of repeat offenses of the robocall mitigation rules, it will consider whether to adopt rules permanently barring principals and others associated with entities subject to revocation from holding both existing and future Commission authorizations. Going forward now, the Commission will generally consider whether it is in the public interest for individual company owners, directors, officers, and principals associated with an entity for which it has revoked a Commission authorization to obtain new Commission authorizations or licenses at the time that they, or an entity with which they are affiliated, apply for them. This is consistent with the Commission's stated intent in the *Fifth Caller ID Authentication FNPRM* to consider the impact these principals and others may have on ''future'' significant association with entities regulated by the Commission.

63. The Commission concludes that these new enforcement tools, acting in tandem with its new requirement for providers to submit their related entities and principals in their robocall mitigation plans, will ensure that bad actor providers and their principals will face potentially serious consequences for their repeated violation of the Commission's robocall mitigation rules. These potential consequences reach beyond a forfeiture and appropriately subject these entities and principals to specified consequences and a thorough public interest review as required. The Commission makes clear that revoking a Commission authorization or license does not transform entities that have not been classified as common carriers into common carriers or extend its general jurisdiction over foreign providers. Rather, this consequence merely allows the Commission discretion to revoke a Commission authorization or license that a provider, person, or entity would otherwise be eligible for or to deny an application for a Commission license or authorization by a principal of an entity subject to revocation. For this reason, the Commission need not exempt foreign providers from this rule, as some commenters argue.

5. Other Enforcement Matters

64. The Commission does not adopt EPIC/NCLC's proposal to base enforcement actions, including removal from the Robocall Mitigation Database, solely on the number of tracebacks a provider receives. In enforcement actions, the Commission has considered a high volume of tracebacks as a factor in determining whether a provider engaged in egregious and intentional misconduct. While receiving a high number of traceback requests may be evidence of malfeasance in certain instances, this is not always the case. The Commission's rules independently require providers to commit to respond to traceback requests—and to actually respond to such requests—in a certain time period, and they may be subject to forfeiture or removal for failure to do so. The Commission also declines to adopt licensing or bonding requirements for certain VoIP providers as EPIC/NCLC proposes.

65. The Commission declines to adopt EPIC/NCLC's strict liability standard for forfeiture or removal from the Robocall Mitigation Database for failure to block any illegal calls regardless of the circumstances, or their suggestion of an ''interim'' standard of assessing liability for transmitting illegal robocall traffic based on whether a provider ''knew or should have known that [a] call was illegal.'' The Commission concludes that expectations to stop all illegal calls are not realistic and that a strict liability standard could lead to significant market disruptions. Similarly, the Commission declines to adopt NCTA or ACA Connect's proposed ''good faith'' or CCA's proposed ''reasonableness'' standards.

D. STIR/SHAKEN Obligations of Satellite Providers

66. The Commission concludes that satellite providers that do not use North American Numbering Plan (NANP) numbers to originate calls or only use such numbers to forward calls to non-NANP numbers are not ''voice service providers'' under the TRACED Act and therefore do not have a STIR/SHAKEN

implementation obligation. The Commission also provides an ongoing extension from TRACED Act obligations to satellite providers that are small voice service providers and use NANP numbers to originate calls on the basis of a finding of undue hardship.

67. The Commission previously provided small voice services providers, including satellite providers, an extension from STIR/SHAKEN implementation until June 30, 2023. In the *Fifth Caller ID Authentication FNPRM,* the Commission sought comment on whether the TRACED Act requirements apply to some or all satellite providers and, if so, whether the Commission should grant certain satellite providers a STIR/SHAKEN extension. In addition to the questions raised in the *Fifth Caller ID Authentication FNPRM,* the Wireline Competition Bureau in August 2022 sought comment on the small provider extension generally and its applicability to satellite providers.

68. *Satellite Providers Originating Calls Using Non-NANP Numbers.* The Commission concludes that, where satellite providers originate calls using non-NANP numbers, they are not acting as ''voice service providers'' within the meaning of the TRACED Act. This conclusion is consistent with the TRACED Act's definition of voice service which requires that voice communications must use resources from the NANP. The Commission also concludes that where satellite providers utilize NANP resources for call forwarding to non-NANP numbers, such calls also fall outside of the definition of voice service. This finding is consistent with the underlying purpose of the STIR/SHAKEN regime. One of the key aims of the TRACED Act, STIR/SHAKEN, and the Commission's implementing rules, is to prevent call spoofing. Where a phone number is not displayed to the end user, as is the case in the satellite call forwarding scenario, call spoofing is not a concern.

69. *Satellite Providers Originating Calls Using NANP Numbers.* The Commission next permits an indefinite extension of time for small voice providers that are satellite providers originating calls using NANP numbers. There are de minimis instances where satellite providers may assign NANP resources to their subscribers for caller ID purposes. While the Commission finds that, in these cases, satellite providers are acting as voice service providers, the Commission believes it is also appropriate to provide an indefinite extension for STIR/SHAKEN implementation to these providers by applying the TRACED Act's ''undue hardship'' standard.

70. The TRACED Act directed the Commission to assess burdens or barriers to the implementation of STIR/SHAKEN, and granted the Commission discretion to extend the implementation deadline for a ''reasonable period of time'' based upon a ''public finding of undue hardship.'' In considering whether the hardship is ''undue'' under the TRACED Act—as well as whether an extension is for a ''reasonable period of time''—it is appropriate to balance the hardship of compliance due to the ''the burdens and barriers to implementation'' faced by a voice service provider or class of voice service providers with the benefit to the public of implementing STIR/SHAKEN expeditiously.

71. The Commission concludes that an indefinite extension is appropriate under this standard for small voice providers that are satellite providers originating calls using NANP numbers. The number of satellite subscribers using NANP resources is miniscule. There is little evidence that satellite providers or their users are responsible for illegal robocalls and satellite service costs make the high-volume calling necessary for robocallers uneconomical. The balancing of the benefits and burdens, therefore, counsels against requiring such providers to implement STIR/SHAKEN.

72. The Commission notes that it must annually reevaluate TRACED Act extensions granted, ensuring that the Commission will be able to act quickly to prevent any unforeseen abuses. While the Commission provides small voice service satellite providers an extension from STIR/SHAKEN implementation, the Commission makes clear that they must, like other voice service providers with an extension, submit a certification to the Robocall Mitigation Database pursuant to its existing rules and the new obligations the Commission adopts in this document.

E. Differential Treatment of International Roaming Traffic

73. The Commission next declines to adopt rules in this document concerning the differential treatment of international roaming traffic. The Commission also declines to adopt rules concerning differential treatment of non-conversational traffic in this document. The Commission continues to consider the record on this issue. In the *Fifth Caller ID Authentication FNPRM,* the Commission sought comment on stakeholders' assertions that international cellular roaming traffic involving NANP numbers (*i.e.,* traffic originated abroad from U.S. mobile subscribers carrying U.S. NANP numbers and terminated in the U.S.) is unlikely to carry illegal robocalls and therefore should be treated with a ''lighter'' regulatory touch. As part of that inquiry, the Commission also asked whether any separate regulatory regime for such traffic could be ''gamed'' by illegal robocallers by disguising their traffic as cellular roaming traffic.

74. Given the limited record on this issue, particularly with respect to whether and how providers could readily identify or segregate such traffic for differential treatment, the Commission directs the Wireline Competition Bureau to refer the issue to the North American Numbering Council for further investigation.

F. Summary of Cost Benefit Analysis

75. The Commission finds that the benefits of the rules it adopts in this document will greatly outweigh the costs imposed on providers. As it explained in the *First Caller ID Authentication Report and Order,* 85 FR 22029 (Apr. 21, 2020), the Commission concluded that its STIR/SHAKEN rules are likely to result in, at a minimum, $13.5 billion in annual benefits. In the *Fifth Caller ID Authentication FNPRM,* the Commission sought comment on its belief that its proposed rules and actions would achieve a large share of the annual $13.5 billion benefit and that the benefits will far exceed the costs imposed on providers. After reviewing the record in this proceeding, the Commission confirms this conclusion.

76. Limiting the ability of illegal robocallers to evade existing rules will preserve and extend the benefits of STIR/SHAKEN. The new enforcement tools the Commission adopts, as well as expanded call authentication and robocall mitigation obligations, will increase the effectiveness of its authentication regime, thereby allowing more illegal robocalls to be readily identified and stopped. As the Commission found previously, it again concludes that an overall reduction in illegal robocalls from new rules will lower network costs by eliminating both unwanted traffic congestion and the labor costs of handling numerous customer complaints. This reduction in robocalls will also help restore confidence in the U.S. telephone network and facilitate reliable access to emergency and healthcare services.

77. In this document the Commission adopts a targeted obligation applicable to the first intermediate provider in the call path. By limiting the authentication obligation to the intermediate provider at the beginning of the call chain, the

Commission maximizes the benefits of the requirement while minimizing its costs. Indeed, intermediate providers can avoid any authentication burden if they require their upstream providers to only send them authenticated traffic.

78. The Commission acknowledges that the revised and expanded mitigation and Robocall Mitigation Database filing obligations it adopts in this document will impose limited short-term implementation costs. Nevertheless, the Commission concludes that the benefits of bringing all providers within the mitigation and Robocall Mitigation Database regime will produce significant benefits to the Commission and the public by increasing transparency and accountability, and by facilitating the enforcement of the Commission's rules.

G. Legal Authority

79. Consistent with its proposals, the Commission adopts the foregoing obligations pursuant to the legal authority it relied on in prior caller ID authentication and call blocking orders.

80. *Caller ID Authentication.* The Commission concludes that the same authority through which it imposed caller ID authentication obligations on gateway providers—a subset of intermediate providers—applies equally to its rules that impose caller ID authentication obligations on non-gateway intermediate providers. Specifically, the Commission finds authority to impose caller ID authentication obligations on the first intermediate providers in the call chain under section 251(e) of 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 calls that transit the networks of intermediate providers with illegally spoofed caller ID are exploiting numbering resources and so found authority under section 251(e). The Commission 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. The Commission relied on this reasoning in adopting authentication obligations on gateway providers and it therefore relies on this same legal authority to impose an authentication obligation on the first intermediate providers in the call chain.

81. *Robocall Mitigation.* The Commission adopts its robocall mitigation provisions for non-gateway intermediate providers and voice service providers, including those without the facilities necessary to implement STIR/SHAKEN, pursuant to sections 201(b), 202(a), and 251(e) of the Communications Act; the Truth in Caller ID Act; and the Commission's ancillary authority, consistent with the authority the Commission invoked to adopt analogous rules in the *Fifth Caller ID Authentication Report and Order* and *Second Caller ID Authentication Report and Order.* The Commission sought comment on whether it should impose a mitigation duty on voice providers without the facilities necessary to implement STIR/SHAKEN on the basis of an ongoing extension from the TRACED Act. The Commission concludes that because such providers were not granted an initial extension as a class under the TRACED Act, the clearest basis of authority for imposing a mitigation obligation is found in sections 201(b), 202(a), and 251(e) of the Communications Act; the Truth in Caller ID Act; and the Commission's ancillary authority. The Commission concludes that section 251(e) of the Act and the Truth in Caller ID Act authorize it to prohibit domestic intermediate providers and voice service providers from accepting traffic from non-gateway intermediate providers that have not filed in the Robocall Mitigation Database. In the *Second Caller ID Authentication Report and Order,* the Commission concluded that section 251(e) gives it 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 illegally 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.

82. 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 its sections 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 VoIP providers and, in the context of its call blocking orders, intermediate providers. The Commission concludes that the same authority provides a basis to adopt the mitigation obligations it adopts in this document to the extent that providers are acting as common carriers.

83. While the Commission concludes that its direct sources of authority provide an ample basis to adopt its proposed rules on all providers, its ancillary authority in section 4(i) provides an independent basis to do so with respect to providers that have not been classified as common carriers. The Commission may exercise ancillary jurisdiction when two conditions are satisfied: (1) the Commission's general jurisdictional grant under Title I of the Communications Act covers the regulated subject; and (2) the regulations are reasonably ancillary to the Commission's effective performance of its statutorily mandated responsibilities. The Commission concludes that the regulations adopted in this document satisfy the first prong because providers that interconnect with the public switched telephone network and exchange IP traffic clearly offer ''communication by wire and radio.''

84. With regard to the second prong, requiring providers to comply with its proposed rules is reasonably ancillary to the Commission's effective performance of its statutory responsibilities under sections 201(b), 202(a), and 251(e) of the Communications Act and the Truth in Caller ID Act as described above. With respect to sections 201(b) and 202(a), absent application of its proposed rules to providers that are not classified as common carriers, originators of robocalls could circumvent the Commission's proposed scheme by sending calls only via providers that

have not yet been classified as common carriers.

85. *Enforcement.* The Commission adopts its additional enforcement rules above pursuant to sections 501, 502, and 503 of the Act. These provisions allow the Commission to take enforcement action against common carriers as well as providers not classified as common carriers following a citation. The Commission relies on this same authority to revise § 1.80 of its rules by adding new maximum and base forfeiture amounts.

II. Final Regulatory Flexibility Analysis

86. As required by the Regulatory Flexibility Act of 1980 (RFA), as amended, an Initial Regulatory Flexibility Analysis (IRFA) was incorporated into the *FNPRM* adopted in May 2022 (*Fifth Caller ID Authentication FNPRM*). The Commission sought written public comment on the proposals in the *Fifth Caller ID Authentication 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

87. This document takes important steps in the fight against illegal robocalls by strengthening caller ID authentication obligations, expanding robocall mitigation rules, and granting an indefinite extension for small voice service providers that are also satellite providers originating calls using NANP numbers on the basis of undue hardship. The decisions the Commission makes here protect consumers from unwanted and illegal calls while balancing the legitimate interests of callers placing lawful calls.

88. First, this document requires any non-gateway intermediate provider that receives an unauthenticated SIP call directly from an originating provider to authenticate the call. Second, it requires non-gateway intermediate providers subject to the authentication obligation to comply with, at a minimum, the version of the standards in effect on December 31, 2023, along with any errata. Third, it requires all providers—including intermediate providers and voice service providers without the facilities necessary to implement STIR/SHAKEN—to: (1) take ''reasonable steps'' to mitigate illegal robocall traffic; (2) submit a certification to the Robocall Mitigation Database regarding their STIR/SHAKEN implementation status along with other identifying information; and (3) submit a robocall mitigation plan to the Robocall Mitigation Database. Fourth, it requires all providers to commit to fully respond to traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping illegal robocallers that use its services to originate, carry, or process illegal robocalls. Fifth, it requires downstream providers to block traffic received directly from non-gateway intermediate providers that have not submitted a certification in the Robocall Mitigation Database or have been removed through enforcement actions. Finally, this document grants an ongoing STIR/SHAKEN implementation extension on the basis of undue hardship for satellite providers that are small service providers using NANP numbers to originate calls.

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

89. There were no comments raised that specifically addressed the proposed rules and policies presented in the *Fifth Caller ID Authentication 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

90. 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 Rules Will Apply

91. The RFA directs agencies to provide a description of, and where feasible, an estimate of the number of small entities that may be affected by the rules adopted herein. The RFA generally defines the term ''small entity'' as having the same meaning as the terms ''small business,'' ''small organization,'' and ''mall 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 SBA 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.

92. *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, 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 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.

93. 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. 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) that includes the continental U.S., Alaska, and Hawaii. This data does not include information for Puerto Rico.

94. 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 indicate there were 90,075 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States. The Census of Governments survey is conducted every five (5) years compiling data for years ending with ''2'' and ''7''. 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.

95. *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.

96. 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.

97. *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.

98. *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.

99. *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 a 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.

100. *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 a 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.

101. *Cable System Operators (Telecom Act Standard).* The Communications Act of 1934, as amended, contains a size standard for a ''small cable operator,'' which is a cable operator that, directly or through an affiliate, serves in the aggregate fewer than one percent of all subscribers in the United States and is not affiliated with any entity or entities whose gross annual revenues in the aggregate exceed $250,000,000. For purposes of the Telecom Act Standard, the Commission determined that a cable system operator that serves fewer than 677,000 subscribers, either directly or through affiliates, will meet the definition of a small cable operator based on the cable subscriber count established in a 2001 Public Notice. Based on industry data, only six cable system operators have more than 677, 000 subscribers. Accordingly, the Commission estimates that the majority of cable system operators are small under this size standard. The Commission notes however, that it 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.

102. *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 a 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.

103. *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.

104. *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.

105. *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 a 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.

106. *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.

107. *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 a 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.

108. *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) or VoIP services, via client-supplied telecommunications connections are also included in this industry. The SBA small business size standard for this industry classifies firms with annual receipts of $35 million or less as small. U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year. Of those firms, 1,039 had revenue of less than $25 million. 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

109. This document requires 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. Specifically, this document adopts a limited intermediate provider authentication requirement. It requires a non-gateway intermediate provider that receives an unauthenticated SIP call directly from an originating provider to authenticate the call. The requirement will arise in limited circumstances—where the originating provider failed to comply with their own authentication obligation, or where the call is sent directly to an intermediate provider from the limited subset of originating providers that lack an authentication obligation. Indeed, if the first intermediate provider in the call path implements contractual provisions with its upstream originating providers stating that it will only accept authenticated traffic, it will completely avoid the need to authenticate calls. Non-gateway intermediate providers that are subject to the authentication obligation 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. A non-gateway intermediate provider using non-IP network technology in its network has the flexibility to either upgrade its network to allow for the initiation, maintenance, and termination of SIP calls and fully implement the STIR/SHAKEN framework, or 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 non-gateway intermediate provider satisfies its obligation if it participates through a third-party representative, such as a trade association of which it is a member or vendor.

110. This document also requires all providers to take ''reasonable steps'' to mitigate illegal robocalls. The new classes of providers subject to the ''reasonable steps'' standard are not required to implement specific measures to meet that standard, but providers' programs must include detailed practices that can reasonably be expected to significantly reduce the carrying, processing, or origination of illegal robocalls. In addition, all providers must implement a robocall mitigation program and comply with the practices that its program requires. The providers must also commit to respond fully to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping illegal robocalls.

111. All providers must submit a certification and robocall mitigation plan to the Robocall Mitigation Database regardless of whether they are required to implement STIR/SHAKEN, including providers without the facilities necessary to implement STIR/SHAKEN. The robocall mitigation plan must describe the specific ''reasonable steps'' that the provider has taken to avoid, as applicable, the origination, carrying, or processing of illegal robocall traffic. This document also requires providers to ''describe with particularity'' certain mitigation techniques in their robocall mitigation plans. Specifically, (1) voice service providers must describe how they are complying with their existing obligation to take affirmative effective measures to prevent new and renewing customers from originating illegal calls; (2) non-gateway intermediate providers and voice service providers must describe any ''know-your-upstream provider'' procedures; and (3) all providers must describe any call analytics systems used to identify and block illegal traffic. To comply with the new requirements to describe their ''new and renewing customer'' and ''know-your-upstream provider'' procedures, providers must describe any contractual provisions with end-users or upstream providers designed to mitigate illegal robocalls.

112. All providers with new filing obligations must submit a certification to the Robocall Mitigation Database that includes the following baseline information:

(1) whether the provider has fully, partially, or not implemented the STIR/SHAKEN authentication framework in the IP portions of its network;

(2) the provider's business name(s) and primary address;

(3) other business name(s) in use by the provider;

(4) all business names previously used by the provider;

(5) whether the provider is a foreign service provider;

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

113. Certifications and robocall mitigations plans must be submitted in English or with certified English translation, and providers with new filing obligations must update any submitted information within 10 business days.

114. This document also adopts rules requiring providers to submit additional information in their Robocall Mitigation certifications. Specifically, (1) all providers must submit additional information regarding their role(s) in the call chain; (2) all providers asserting they do not have an obligation to implement STIR/SHAKEN must include more detail regarding the basis of that assertion; (3) all providers must certify that they have not been prohibited from filing in the Robocall Mitigation Database pursuant to a law enforcement action; (4) all providers must state whether they have been subject to a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to unlawful robocalling or spoofing and provide information concerning any such actions or investigations; and (5) all filers must submit their OCN if they have one. Submissions may be made confidentially, consistent with the Commission's existing confidentiality rules.

115. This document requires downstream providers to block traffic received from a non-gateway intermediate provider that is not listed in the Robocall Mitigation Database, either because the provider did not file or their certification was removed as part of an enforcement action. After receiving notice from the Commission that a provider has been removed from the Robocall Mitigation Database, downstream providers must block all traffic from the identified provider within two business days.

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

116. 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.

117. Generally, the decisions the Commission made in this document apply to all providers, and do not impose unique burdens or benefits on small providers. The Commission took several steps to minimize the economic impact of the rules adopted in this document on small entities.

118. This document imposes a limited intermediate provider authentication obligation that requires the first non-gateway intermediate provider in the call chain to authenticate unauthenticated calls received directly from an originating provider. Limiting the application of the authentication obligation to first non-gateway intermediate providers helps reduce the burden on intermediate providers, including small providers, and minimizes the potential costs associated with a broader authentication requirement for all intermediate providers that were identified in the record.

119. The Commission also 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, non-gateway intermediate providers have the flexibility to assign the level of attestation appropriate to the call based on the applicable level of the standards and the available call information. Additionally, the new classes of providers subject to the ''reasonable steps'' standard have the flexibility to determine which measures to use to mitigate illegal robocall traffic on their networks. In reaching this approach, the Commission considered and declined to adopt a ''gross negligence'' standard for evaluating whether a mitigation program is sufficient. The Commission also declined to adopt a heightened mitigation obligation solely for VoIP providers in order to ensure that the obligation applies to providers regardless of the technology used to transmit calls. Likewise, the Commission allowed non-gateway intermediate providers subject to its call authentication requirements that rely on non-IP infrastructure the flexibility to either upgrade their networks to implement STIR/SHAKEN or participate as a member of a working group, industry standards group, or consortium that is working to develop a non-IP caller ID authentication solution. This flexibility will reduce compliance costs for non-gateway intermediate providers, including small providers. The Commission also declined to require providers to submit information concerning inquiries from law enforcement or regulatory agencies or investigations that do not include findings of actual or suspected wrongdoing. And the Commission declined to require Robocall Mitigation Database filers to include certain additional identifying information discussed in the *Fourth Caller ID Authentication FNPRM* beyond their OCN.

120. This document also grants an indefinite STIR/SHAKEN implementation extension to satellite providers that are small voice service providers and use NANP numbers to originate calls.

G. Report to Congress

121. The Commission will send a copy of the *Sixth Report and Order,* including this 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 *Sixth Report and Order,* including this FRFA, to the Chief Counsel for Advocacy of the Small Business Administration. A copy of the *Sixth Report and Order* (or summaries thereof) will also be published in the **Federal Register**.

III. Procedural Matters

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

123. *Paperwork Reduction Act.* This document may contain new or modified information collection requirements subject to the PRA, Public Law 104–13. Specifically, the rules adopted in 47 CFR 64.6303(c) and 64.6305(d), (e), and (f) may require new or modified information collections. All such new or modified information collection requirements will be submitted to 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. In addition, the Commission notes that pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107–198, it previously sought specific comment on how the Commission might further reduce the information collection burden for small business concerns with fewer than 25 employees. In this document, the Commission describes several steps it has taken to minimize the information collection burdens on small entities.

124. *Congressional Review Act.* The Commission has determined, and the Administrator of the Office of Information and Regulatory Affairs, 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 *Sixth Report and Order* to Congress and the Government Accountability Office pursuant to 5 U.S.C. 801(a)(1)(A).

IV. Ordering Clauses

125. Accordingly, pursuant to sections 4(i), 4(j), 201, 202, 214, 217, 227, 227b, 251(e), 303(r), 501, 502, and 503 of the Communications Act of 1934, as amended, 47 U.S.C. 154(i), 154(j), 201, 202, 214, 217, 227, 227b, 251(e), 303(r), 501, 502, and 503, *it is ordered* that the *Sixth Report and Order is adopted.*

126. *It is further ordered* that parts 0, 1, and 64 of the Commission's rules *are amended* as set forth in the Final Rules.

127. *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), the *Sixth Report and Order,* including the rule revisions and redesignations described in the Final Rules, *shall be effective* 60 days after publication in the **Federal Register**, except that: (1) the additions of 47 CFR 64.6303(c) and 64.6305(f) and the revisions to redesignated 47 CFR 64.6305(d) and (e) as described in the Final Rules will not be effective until OMB completes any review that the Wireline Competition Bureau determines is required under the Paperwork Reduction Act; and (2) the revisions to redesignated 47 CFR 64.6305(g) as described in the Final

Rules will not be effective until an effective date is announced by the Wireline Competition Bureau. The Commission directs the Wireline Competition Bureau to announce effective dates for the additions of and revisions to 47 CFR 64.6303(c) and 64.6305(d) through (g), as redesignated by the *Sixth Report and Order,* by subsequent notification.

128. *It is further ordered* that the Office of the Managing Director, Performance Evaluation and Records Management, *shall send* a copy of the *Sixth Report and Order* 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).

129. *It is further ordered* that the Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, *shall send* a copy of the *Sixth Report and Order,* 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 1

Administrative practice and procedure, Civil rights, Claims, Communications, Communications common carriers, Communications equipment, Cuba, Drug abuse, Environmental impact statements, Equal access to justice, Equal employment opportunity, Federal buildings and facilities, Government employees, Historic preservation, Income taxes, Indemnity payments, Individuals with disabilities, internet, Investigations, Lawyers, Metric system, Penalties, Radio, Reporting and recordkeeping requirements, Satellites, Security measures, Telecommunications, Telephone, Television, Wages.

47 CFR Part 64

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

Federal Communications Commission.

Marlene Dortch,

Secretary.

Final Rules

For the reasons discussed in the preamble, the Federal Communications Commission amends 47 CFR parts 0, 1, and 64 as follows:

PART 0—COMMISSION ORGANIZATION

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

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

Subpart A—Organization

■ 2. Amend § 0.111 by revising paragraph (a)(28)(i) and (ii) and adding paragraph (a)(29) to read as follows:

§ 0.111 Functions of the Bureau.

(a) * * *

(28) * * *

(i) Whose certification required by § 64.6305 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 provider not listed in the Robocall Mitigation Database in violation of § 64.6305(g) of this chapter.

(29) Take enforcement action, including revoking an existing section 214 authorization, license, or instrument for any entity that has repeatedly violated § 64.6301, § 64.6302, or § 64.6305 of this chapter. The Commission or the Enforcement Bureau under delegated authority will provide prior notice of its intent to revoke an existing license or instrument of authorization and follow applicable revocation procedures, including providing the authorization holder with a written opportunity to demonstrate why revocation is not warranted.

* * * * *

PART 1—PRACTICE AND PROCEDURE

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

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

Subpart A—General Rules of Practice and Procedure

■ 4. Amend § 1.80 by:

■ a. Redesignating paragraphs (b)(9) through (11) as paragraphs (b)(10) through (12);

■ b. Adding new paragraph (b)(9);

■ c. Revising newly redesignated paragraph (b)(10);

■ d. In newly redesignated paragraph (b)(11):

■ i. Revising table 1;

■ ii. Revising the headings for tables 2 and 3;

■ iii. Revising the heading and footnote 1 for table 4; and

■ iv. Revising note 2 following table 4;

■ e. In newly redesignated paragraph (b)(12)(ii), revising the heading for table 5; and

■ f. Revising note 3 following table 5 to newly redesignated paragraph (b)(12)(ii).

The addition and revisions read as follows:

§ 1.80 Forfeiture proceedings.

* * * * *

(9) *Forfeiture penalty for a failure to block.* Any person determined to have failed to block illegal robocalls pursuant to §§ 64.6305(g) and 64.1200(n) of this chapter shall be liable to the United States for a forfeiture penalty of no more than $23,727 for each violation, to be assessed on a per-call basis.

(10) *Maximum forfeiture penalty for any case not previously covered.* In any case not covered in paragraphs (b)(1) through (9) of this section, the amount of any forfeiture penalty determined under this section shall not exceed $23,727 for each violation or each day of a continuing violation, except that the amount assessed for any continuing violation shall not exceed a total of $177,951 for any single act or failure to act described in paragraph (a) of this section.

(11) * * *

TABLE 1 TO PARAGRAPH (b)(11)—BASE AMOUNTS FOR SECTION 503 FORFEITURES

Forfeitures	Violation amount
Misrepresentation/lack of candor	(1)
Failure to file required DODC required forms, and/or filing materially inaccurate or incomplete DODC information	$15,000
Construction and/or operation without an instrument of authorization for the service	10,000
Failure to comply with prescribed lighting and/or marking	10,000

TABLE 1 TO PARAGRAPH (b)(11)—BASE AMOUNTS FOR SECTION 503 FORFEITURES—Continued

Forfeitures	Violation amount
Violation of public file rules	10,000
Violation of political rules: Reasonable access, lowest unit charge, equal opportunity, and discrimination	9,000
Unauthorized substantial transfer of control	8,000
Violation of children's television commercialization or programming requirements	8,000
Violations of rules relating to distress and safety frequencies	8,000
False distress communications	8,000
EAS equipment not installed or operational	8,000
Alien ownership violation	8,000
Failure to permit inspection	7,000
Transmission of indecent/obscene materials	7,000
Interference	7,000
Importation or marketing of unauthorized equipment	7,000
Exceeding of authorized antenna height	5,000
Fraud by wire, radio or television	5,000
Unauthorized discontinuance of service	5,000
Use of unauthorized equipment	5,000
Exceeding power limits	4,000
Failure to Respond to Commission communications	4,000
Violation of sponsorship ID requirements	4,000
Unauthorized emissions	4,000
Using unauthorized frequency	4,000
Failure to engage in required frequency coordination	4,000
Construction or operation at unauthorized location	4,000
Violation of requirements pertaining to broadcasting of lotteries or contests	4,000
Violation of transmitter control and metering requirements	3,000
Failure to file required forms or information	3,000
Per call violations of the robocall blocking rules	2,500
Failure to make required measurements or conduct required monitoring	2,000
Failure to provide station ID	1,000
Unauthorized pro forma transfer of control	1,000
Failure to maintain required records	1,000

Table 2 to Paragraph (b)(11)—Violations Unique to the Service

* * * * *

Table 3 to Paragraph (b)(11)—Adjustment Criteria for Section 503 Forfeitures

* * * * *

Table 4 to Paragraph (b)(11)—Non-Section 503 Forfeitures That Are Affected by the Downward Adjustment Factors [1]

* * * * *

[1] Unlike section 503 of the Act, which establishes maximum forfeiture amounts, other sections of the Act, with two exceptions, state prescribed amounts of forfeitures for violations of the relevant section. These amounts are then subject to mitigation or remission under section 504 of the Act. One exception is section 223 of the Act, which provides a maximum forfeiture per day. For convenience, the Commission will treat this amount as if it were a prescribed base amount, subject to downward adjustments. The other exception is section 227(e) of the Act, which provides maximum forfeitures per violation, and for continuing violations. The Commission will apply the factors set forth in section 503(b)(2)(E) of the Act and this table 4 to determine the amount of the penalty to assess in any particular situation. The amounts in this table 4 are adjusted for inflation pursuant to the Debt Collection Improvement Act of 1996 (DCIA), 28 U.S.C. 2461. These non-section 503 forfeitures may be adjusted downward using the ''Downward Adjustment Criteria'' shown for section 503 forfeitures in table 3 to this paragraph (b)(11).

Note 2 to paragraph (b)(11): *Guidelines for Assessing Forfeitures.* The Commission and its staff may use the guidelines in tables 1 through 4 of this paragraph (b)(11) in particular cases. The Commission and its staff retain the discretion to issue a higher or lower forfeiture than provided in the guidelines, to issue no forfeiture at all, or to apply alternative or additional sanctions as permitted by the statute. The forfeiture ceilings per violation or per day for a continuing violation stated in section 503 of the Communications Act and the Commission's rules are described in paragraph (b)(12) of this section. These statutory maxima became effective September 13, 2013. Forfeitures issued under other sections of the Act are dealt with separately in table 4 to this paragraph (b)(11).

(12) * * *

(ii) * * *

Table 5 to Paragraph (b)(12)(ii)

* * * * *

Note 3 to paragraph (b)(12): Pursuant to Public Law 104–134, the first inflation adjustment cannot exceed 10 percent of the statutory maximum amount.

* * * * *

PART 64—MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

■ 5. 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, 617, 620, 1401–1473, unless otherwise noted; Pub. L. 115–141, Div. P, sec. 503, 132 Stat. 348, 1091.

Subpart HH—Caller ID Authentication

■ 6. Amend § 64.6300 by redesignating paragraphs (i) through (n) as paragraphs (j) through (o) and adding new paragraph (i) to read as follows:

§ 64.6300 Definitions.

* * * * *

(i) *Non-gateway intermediate provider.* The term ''non-gateway intermediate provider'' means any entity that is an intermediate provider as that term is defined by paragraph (g) of this section that is not a gateway provider as that term is defined by paragraph (d) of this section.

* * * * *

■ 7. Amend § 64.6302 by adding paragraph (d) to read as follows:

§ 64.6302 Caller ID authentication by intermediate providers.

* * * * *

(d) Notwithstanding paragraph (b) of this section, a non-gateway intermediate provider must, not later than December 31, 2023, authenticate caller identification information for all calls it receives directly from an originating provider 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 non-gateway intermediate provider is subject to an applicable extension in § 64.6304.

§ 64.6303 [Amended]

■ 8. Amend § 63.6303 by adding reserved paragraph (c).

■ 9. Delayed indefinitely, further amend § 63.6303 by adding paragraph (c) to read as follows:

§ 64.6303 Caller ID authentication in non-IP networks.

* * * * *

(c) Except as provided in § 64.6304, not later than December 31, 2023, a non-gateway intermediate provider receiving a call directly from an originating 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(d) 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.

■ 10. Amend § 64.6304 by:
■ a. Removing the word ''and'' at the end of paragraph (a)(1)(i);
■ b. Revising paragraph (a)(1)(ii);
■ c. Adding paragraph (a)(1)(iii); and
■ d. Revising paragraphs (b) and (d).

The revisions and addition read as follows:

§ 64.6304 Extension of implementation deadline.

(a) * * *

(1) * * *

(ii) A small voice service provider notified by the Enforcement Bureau pursuant to § 0.111(a)(27) of this chapter that fails to respond in a timely manner, fails to respond with the information requested by the Enforcement Bureau, including credible evidence that the robocall traffic identified in the notification is not illegal, fails to demonstrate that it taken steps to effectively mitigate the traffic, or if the Enforcement Bureau determines the provider violates § 64.1200(n)(2), will no longer be exempt from the requirements of § 64.6301 beginning 90 days following the date of the Enforcement Bureau's determination, unless the extension would otherwise terminate earlier pursuant to paragraph (a)(1) introductory text or (a)(1)(i), in which case the earlier deadline applies; and

(iii) Small voice service providers that originate calls via satellite using North American Numbering Plan numbers are deemed subject to a continuing extension of § 64.6301.

* * * * *

(b) *Voice service providers, gateway providers, and non-gateway intermediate 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 an 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. Non-gateway intermediate providers that are incapable of obtaining an SPC token due to Governance Authority policy are exempt from the requirements of § 64.6302(d) regarding call authentication.

* * * * *

(d) *Non-IP networks.* Those portions of a voice service provider, gateway provider, or non-gateway intermediate 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, 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, and a non-gateway intermediate provider receiving calls directly from an originating provider subject to the foregoing extension shall comply with the requirements of § 64.6303(c) as to the portion of its network subject to the extension.

* * * * *

■ 11. Amend § 64.6305 by:
■ a. Revising paragraph (a)(1);
■ b. Redesignating paragraphs (c), (d), and (e) as paragraphs (d), (e), and (g) and adding new paragraph (c);
■ c. Revising newly redesignated paragraphs (d)(3) introductory text, (d)(5) introductory text, (e)(2) introductory text, (e)(3) introductory text, and (e)(5);
■ d. Adding reserved paragraph (f);
■ e. Revising newly redesignated paragraphs (g)(1) through (3);
■ f. Redesignating paragraph (g)(4) as paragraph (g)(5) and adding new reserved paragraph (g)(4); and
■ g. Revising newly redesignated paragraph (g)(5) introductory text.

The additions and revisions read as follows:

§ 64.6305 Robocall mitigation and certification.

(a) * * *

(1) Each voice service provider shall implement an appropriate robocall mitigation program.

* * * * *

(c) *Robocall mitigation program requirements for non-gateway intermediate providers.* (1) Each non-gateway intermediate provider shall implement an appropriate robocall mitigation program.

(2) Any robocall mitigation program implemented pursuant to paragraph (c)(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 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 carry or process calls.

(d) * * *

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

* * * * *

(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 (d)(1) through (4) of this section.

* * * * *

(e) * * *

(2) A gateway provider shall include the following information in its certification made pursuant to paragraph (e)(1) of this section, in

English or with a certified English translation:

* * * * *

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

* * * * *

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

* * * * *

(f) [Reserved]

(g) * * *

(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 (d) of this section and that filing has not been de-listed pursuant to an enforcement action.

(2) *Accepting traffic from foreign providers.* Beginning April 11, 2023, 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 (d) of this section and that filing has not been de-listed pursuant to an enforcement action.

(3) *Accepting traffic from gateway providers.* Beginning April 11, 2023, 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 (e) 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) [Reserved]

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

* * * * *

■ 12. Delayed indefinitely, further amend § 64.6305 by:

■ a. Revising paragraphs (d)(1) introductory text, (d)(1)(ii) and (iii), (d)(2), and (d)(4)(iv) and (v) and adding paragraphs (d)(4)(vi) and (vii);

■ b. Revising paragraphs (e)(1) introductory text and (e)(2)(i) through (iii);

■ c. Adding paragraph (e)(2)(iv);

■ d. Revising paragraphs (e)(4)(iv) and (v) and adding paragraphs (e)(4)(vi) and (vii); and

■ e. Adding paragraphs (f) and (g)(4).

The additions and revisions read as follows:

§ 64.6305 Robocall mitigation and certification.

* * * * *

(d) * * *

(1) A voice service provider shall certify that all of the calls that it originates on its network are subject to a robocall mitigation program consistent with paragraph (a) of this section, that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and to one of the following:

* * * * *

(ii) It has implemented the STIR/SHAKEN authentication framework on a portion of its network and all calls it originates on that portion of its network are compliant with § 64.6301(a)(1) and (2); or

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

(2) A voice service provider 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, and the basis for the extension or extensions, or an explanation of why it is unable to implement STIR/SHAKEN due to a lack of control over the network infrastructure necessary to implement STIR/SHAKEN;

(ii) The specific reasonable steps the voice service provider has taken to avoid originating illegal robocall traffic as part of its robocall mitigation program, including a description of how it complies with its obligation to know its customers pursuant to § 64.1200(n)(3), any procedures in place to know its upstream providers, and the analytics system(s) it uses to identify and block illegal traffic, including whether it uses any third-party analytics vendor(s) and the name(s) of such vendor(s);

(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; and

(iv) State whether, at any time in the prior two years, the filing entity (and/or any entity for which the filing entity shares common ownership, management, directors, or control) has been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description; and, if so, provide a description of any such action or investigation, including all law enforcement or regulatory agencies involved, the date that any action or investigation was commenced, the current status of the action or investigation, a summary of the findings of wrongdoing made in connection with the action or investigation, and whether any final determinations have been issued.

* * * * *

(4) * * *

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

(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;

(vi) Whether the voice service provider is:

(A) A voice service provider with a STIR/SHAKEN implementation obligation directly serving end users;

(B) A voice service provider with a STIR/SHAKEN implementation obligation acting as a wholesale provider originating calls on behalf of another provider or providers; or

(C) A voice service provider without a STIR/SHAKEN implementation obligation; and

(vii) The voice service provider's OCN, if it has one.

* * * * *

(e) * * *

(1) A gateway provider shall certify that all of the calls that it carries or processes on its network are subject to a robocall mitigation program consistent with paragraph (b)(1) of this section, that any prior certification has not been removed by Commission action and it

has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and to one of the following:

* * * * *

(2) * * *

(i) Identification of the type of extension or extensions the gateway provider received under § 64.6304 and the basis for the extension or extensions, or an explanation of why it is unable to implement STIR/SHAKEN due to a lack of control over the network infrastructure necessary to implement STIR/SHAKEN;

(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 complies with its obligation to know its upstream providers pursuant to § 64.1200(n)(4), the analytics system(s) it uses to identify and block illegal traffic, and whether it uses any third-party analytics vendor(s) and the name(s) of such vendor(s);

(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; and

(iv) State whether, at any time in the prior two years, the filing entity (and/or any entity for which the filing entity shares common ownership, management, directors, or control) has been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description; and, if so, provide a description of any such action or investigation, including all law enforcement or regulatory agencies involved, the date that any action or investigation was commenced, the current status of the action or investigation, a summary of the findings of wrongdoing made in connection with the action or investigation, and whether any final determinations have been issued.

* * * * *

(4) * * *

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

(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;

(vi) Whether the gateway provider is:

(A) A gateway provider with a STIR/SHAKEN implementation obligation; or

(B) A gateway provider without a STIR/SHAKEN implementation obligation; and

(vii) The gateway provider's OCN, if it has one.

* * * * *

(f) *Certification by non-gateway intermediate providers in the Robocall Mitigation Database.* (1) A non-gateway intermediate provider shall certify that all of the calls that it carries or processes on its network are subject to a robocall mitigation program consistent with paragraph (c) of this section, that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and 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 non-gateway intermediate provider shall include the following information in its certification made pursuant to paragraph (f)(1) of this section in English or with a certified English translation:

(i) Identification of the type of extension or extensions the non-gateway intermediate provider received under § 64.6304, if the non-gateway intermediate provider is not a foreign provider, and the basis for the extension or extensions, or an explanation of why it is unable to implement STIR/SHAKEN due to a lack of control over the network infrastructure necessary to implement STIR/SHAKEN;

(ii) The specific reasonable steps the non-gateway intermediate provider has taken to avoid carrying or processing illegal robocall traffic as part of its robocall mitigation program, including a description of any procedures in place to know its upstream providers and the analytics system(s) it uses to identify and block illegal traffic, including whether it uses any third-party analytics vendor(s) and the name of such vendor(s);

(iii) A statement of the non-gateway intermediate 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 carry or process calls; and

(iv) State whether, at any time in the prior two years, the filing entity (and/or any entity for which the filing entity shares common ownership, management, directors, or control) has been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description; and, if so, provide a description of any such action or investigation, including all law enforcement or regulatory agencies involved, the date that any action or investigation was commenced, the current status of the action or investigation, a summary of the findings of wrongdoing made in connection with the action or investigation, and whether any final determinations have been issued.

(3) All certifications made pursuant to paragraphs (f)(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 non-gateway intermediate provider filing a certification shall submit the following information in the appropriate portal on the Commission's website:

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

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

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

(iv) Whether the non-gateway intermediate provider or any affiliate is also foreign voice service provider;

(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;

(vi) Whether the non-gateway intermediate provider is:

(A) A non-gateway intermediate provider with a STIR/SHAKEN implementation obligation; or

(B) A non-gateway intermediate provider without a STIR/SHAKEN implementation obligation; and

(vii) The non-gateway intermediate service provider's OCN, if it has one.

(5) A non-gateway intermediate provider shall update its filings within 10 business days of any change to the information it must provide pursuant to this paragraph (f) subject to the conditions set forth in paragraphs (d)(5)(i) and (ii) of this section.

(g) * * *

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

* * * * *

[FR Doc. 2023–12142 Filed 6–20–23; 8:45 am]

BILLING CODE 6712–01–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

50 CFR Part 622

[Docket No. 1206013412–2517–02]

RTID 0648–XD065

Fisheries of the Caribbean, Gulf of Mexico, and South Atlantic; 2023 Commercial Closure for Gulf of Mexico Greater Amberjack

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Temporary rule; closure.

SUMMARY: NMFS implements an accountability measure for commercial greater amberjack in the Gulf of Mexico (Gulf) reef fish fishery for the 2023 fishing year through this temporary rule. NMFS has determined that Gulf greater amberjack landings have exceeded the commercial annual catch target (ACT). Therefore, the commercial fishing season for greater amberjack in the Gulf exclusive economic zone (EEZ) will close on June 18, 2023, and the sector will remain closed until the start of the next commercial fishing season on January 1, 2024. This closure is necessary to protect the Gulf greater amberjack resource.

DATES: This rule is effective 12:01 a.m., local time, June 18, 2023, until 12:01 a.m., local time, January 1, 2024.

FOR FURTHER INFORMATION CONTACT: Kelli O'Donnell, NMFS Southeast Regional Office, telephone: 727–824–5305, or email: *Kelli.ODonnell@noaa.gov.*

SUPPLEMENTARY INFORMATION: NMFS manages the reef fish fishery of the Gulf, which includes greater amberjack, under the Fishery Management Plan for the Reef Fish Resources of the Gulf (FMP). The Gulf of Mexico Fishery Management Council (Council) prepared the FMP and NMFS implements the FMP under the authority of the Magnuson-Stevens Fishery Conservation and Management Act (Magnuson-Stevens Act) by regulations at 50 CFR part 622. All greater amberjack weights discussed in this temporary rule are in round weight.

On June 15, 2023, NMFS published the final rule implementing Amendment 54 to the FMP (88 FR 39193). Among other measures, that final rule decreased the commercial annual catch limit (ACL) and quota (commercial ACT) for Gulf greater amberjack. Effective on the date of publication of the Amendment 54 final rule, the commercial greater amberjack ACL and ACT for the 2023 fishing year are 101,000 lb (45,813 kg) and 93,930 lb (42,606 kg), respectively (50 CFR 622.41(a)(1)(iii) and 622.39(a)(1)(v)).

Under 50 CFR 622.41(a)(1)(i), NMFS is required to close the greater amberjack commercial sector when the commercial ACT is reached, or is projected to be reached, by filing a notification to that effect with the Office of the Federal Register. NMFS has determined that the commercial ACT of 93,930 lb (42,606 kg) has been exceeded. Accordingly, NMFS closes commercial harvest of greater amberjack from the Gulf EEZ effective 12:01 a.m., local time, June 18, 2023, until 12:01 a.m., local time, January 1, 2024.

During the commercial closure, the sale or purchase of greater amberjack taken from the EEZ is prohibited. The prohibition on sale or purchase does not apply to the sale or purchase of greater amberjack that were harvested, landed ashore, and sold prior to 12:01 a.m., local time, June 18, 2023, and were held in cold storage by a dealer or processor. The commercial sector for greater amberjack will re-open on January 1, 2024, the beginning of the 2024 greater amberjack commercial fishing season.

During the commercial closure, the bag and possession limits specified in 50 CFR 622.38(b)(1) apply to all harvest or possession of greater amberjack in or from the Gulf EEZ. However, for the current 2022–2023 recreational fishing year of August 1, 2022, through July 31, 2023, the recreational fishing season is closed for the remainder of the current fishing year, or through July 31, 2023. Therefore, through July 31, 2023, the bag and possession limits for greater amberjack in or from the Gulf EEZ are zero. The recreational season will reopen on August 1, 2023, the start of the next recreational fishing year.

Classification

NMFS issues this action pursuant to section 305(d) of the Magnuson-Stevens Act. This action is required by 50 CFR 622.41(a)(1), which was issued pursuant to section 304(b) of the Magnuson-Stevens Act, and is exempt from review under Executive Order 12866.

Pursuant to 5 U.S.C. 553(b)(B), there is good cause to waive prior notice and an opportunity for public comment on this action, as notice and comment is unnecessary and contrary to the public interest. Such procedures are unnecessary because the regulations associated with the closure of the greater amberjack commercial sector 50 CFR 622.41(a)(1) have already been subject to notice and public comment, and all that remains is to notify the public of the closure. Prior notice and opportunity for public comment are contrary to the public interest because there is a need to immediately implement this action to protect the greater amberjack stock. Prior notice and opportunity for public comment would require time and could result in a harvest well in excess of the commercial ACL. NMFS is required to reduce the 2024 ACT and ACL by the amount of any overage of the 2023 commercial ACL, which would reduce the 2024 fishing season.

For the aforementioned reasons, the AA also finds good cause to waive the 30-day delay in the effectiveness of this action under 5 U.S.C. 553(d)(3).

Authority: 16 U.S.C. 1801 *et seq.*

Dated: June 15, 2023.

Jennifer M. Wallace,

Acting Director, Office of Sustainable Fisheries, National Marine Fisheries Service.

[FR Doc. 2023–13189 Filed 6–15–23; 4:15 pm]

BILLING CODE 3510–22–P