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

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97

SIXTH REPORT AND ORDER IN CG DOCKET NO. 17-59, FIFTH REPORT AND ORDER IN WC DOCKET NO. 17-97, ORDER ON RECONSIDERATION IN WC DOCKET NO. 17-97, ORDER, SEVENTH FURTHER NOTICE OF PROPOSED RULEMAKING IN CG DOCKET NO. 17-59, AND FIFTH FURTHER NOTICE OF PROPOSED RULEMAKING IN WC DOCKET NO. 17-97

Adopted: May 19, 2022 **Released: May 20, 2022**

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

By the Commission: Chairwoman Rosenworcel and Commissioner Starks issuing separate statements

TABLE OF CONTENTS

I. INTRODUCTION

1. In this Gateway Provider Report and Order, Order on Reconsideration, Order, and Further Notice of Proposed Rulemaking, we take further steps to stem the tide of foreign-originated illegal robocalls and seek comment on additional ways to address all such calls. Because of the unique difficulties foreign-based robocallers present, reducing illegal robocalls that originate abroad is one of the most vexing challenges we face in tackling the problem of illegal robocalls. The rules we adopt today extend our protections against unlawful robocalls by placing new obligations on the gateway providers that are the entry point for foreign calls into the United States and requiring them to play a more active role in the fight.

2. Specifically, we require gateway providers to develop and submit traffic mitigation plans to the Robocall Mitigation Database. We also require gateway providers to apply STIR/SHAKEN caller ID authentication to all unauthenticated foreign-originated Session Initiation Protocol (SIP) calls with U.S. North American Numbering Plan (NANP) numbers. And we require gateway providers to respond to traceback requests in 24 hours, block calls where it is clear they are conduits for illegal traffic, and implement "know your upstream provider" obligations.

3. We next expand the requirement that voice service providers only accept calls carrying U.S. NANP numbers from foreign-originating providers listed in the Robocall Mitigation Database so that domestic providers may only accept calls carrying U.S. NANP numbers sent directly from providers that are listed in the Robocall Mitigation Database, regardless of whether they are originating or intermediate providers. We also end the stay of enforcement of the existing requirement and deny petitions for reconsideration of that requirement filed by CTIA and the Voice on the Net Coalition (VON).

4. Finally, we take the opportunity to seek comment on further steps we can take in our battle against illegal robocalls. Specifically, we seek comment on extending some of the new requirements we impose on gateway providers today to all domestic providers, including: expanding the STIR/SHAKEN authentication obligation to all intermediate providers;[1] applying certain existing mitigation obligations, including some adopted in this *Order*, to a broader range of providers; enhancing the enforcement of our rules; clarifying certain aspects of our STIR/SHAKEN regime; and placing limits on the use of U.S. NANP numbers for foreign-originated calls and indirect number access.

II. BACKGROUND

5. The Commission continues to receive more complaints about unwanted calls, which include illegal robocalls, than any other issue.[2] The Federal Trade Commission (FTC) reports a similarly high number of complaints.[3] While unwanted calls cause harm in the form of interruptions and irritation, illegal calls can lead to more serious harm, such as identity theft and financial loss. The FTC reports that 36% of the fraud reports it received in 2021 had a phone call as the contact method, with another 21% from contact via text message.[4] American consumers reported a total of $692 million lost to fraud via phone call, with a median loss of $1,200.[5] These losses are only a small fraction of the overall real cost of illegal robocalls.[6]

[1] We use the term "intermediate provider," consistent with 47 CFR § 64.6300(f), to mean "any entity that [carries] or processes traffic that traverses or will traverse the [public switched telephone network (PSTN)] at any point insofar as that entity neither originates nor terminates that traffic."

[2] The Commission received approximately 193,000 such complaints in 2019, 157,000 in 2020, 164,000 in 2021, and 32,000 in 2022 as of March 31st. FCC, *Consumer Complaint Data Center*, https://www.fcc.gov/consumer-help-center-data (last visited April 27, 2022). Multiple factors can affect these numbers, including outreach efforts and media coverage on how to avoid unwanted calls. Complaint numbers declined significantly during the first four months of the COVID-19 pandemic, reducing the total number of complaints the Commission received in 2020.

[3] The FTC reports it received over 300,000 complaints per month about illegal calls, especially robocalls, in the first three quarters of fiscal year 2021, in additional to approximately 175,000 complaints about unwanted calls that year. FTC, Biennial Report to Congress Under the Do Not Call Registry Fee Extension Act of 2007 at 3 (2021), https://www.ftc.gov/system/files/documents/reports/biennial-report-congress-under-do-not-call-registry-fee-extension-act-2007/p034305dncreport.pdf.

[4] FTC, Consumer Sentinel Network Data Book 2021 at 12 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/CSN%20Annual%20Data%20Book%202021%20Final%20PDF.pdf.

[5] *Id*.

[6] The Commission has previously estimated that illegal robocalls cost American consumers at least $13.5 billion annually, an amount that excludes the nonquantifiable harms caused by less reliable access to the emergency and healthcare communications and by the American public's loss of confidence in the U.S. telephone network. *Call Authentication Trust Anchor, Implementation of the TRACED Act Section 6(a) Knowledge of Customers by Entities with Access to Numbering Resources*, WC Docket Nos. 17-97, 20-67, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3241, 3263, paras. 47-48 (2020) (*First Caller ID Authentication Report and Order and Further Notice*).

6. While the most well-known type of illegal calls is fraudulent calls, where the caller is actively trying to obtain payment or personal information,[7] there are a number of other ways in which a call can be illegal and harm consumers. For example, robocalls may violate the Telephone Consumer Protection Act (TCPA) when made without the called party's prior express consent.[8] Calls with faked (i.e. spoofed) caller ID are also illegal when intended to defraud, cause harm, or wrongfully obtain something of value.[9] This ban extends to spoofing directed at consumers in the United States from foreign actors and applies to alternative voice and text message services.[10]

[7] Fraudulent calls may violate any of a number of state or federal statutes. *See, e.g.*, Telemarketing Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6101-6108; Credit Card Fraud Act of 1984, 18 U.S.C. § 1029; 18 U.S.C. §§ 1343, 1344.

[8] The TCPA prohibits initiating "any telephone call to any residential telephone line using an artificial or prerecorded voice to deliver a message without the prior express consent of the called party," with certain statutory exemptions. 47 U.S.C. § 227(b)(1)(B). Similarly, the TCPA prohibits, without the prior express consent of the called party, any call using an automatic telephone dialing system or an artificial or prerecorded voice to any telephone number "assigned to a . . . cellular telephone service, . . . or any service for which the called party is charged for the call" unless a statutory exemption applies. 47 U.S.C. § 227(b)(1)(A)(iii).

[9] 47 U.S.C. § 227(e)(1). In enforcement actions, the Commission has found that robocalling campaigns, regardless of the content of the robocalls, may violate the Truth in Caller ID Act and its implementing rules. Specifically, the Commission has found that when an entity spoofs a large number of calls in a robocall campaign, it causes harm to: (1) the subscribers of the numbers that are spoofed; (2) the consumers who receive the spoofed calls; and (3) the terminating carriers forced to deliver the calls to consumers and handle "consumers' ire," thereby increasing their costs, *see John C. Spiller et al*., File No.: EB-TCD-18-0027781, Notice of Apparent Liability for Forfeiture, 35 FCC Rcd 5948, 5957-61, paras. 23-33 (2020) (*Spiller NAL*), and it has assessed a record $225 million forfeiture in one instance. *See John C. Spiller et al*., File No.: EB-TCD-18-0027781, Forfeiture Order, 36 FCC Rcd 6225, para. 1 (2021). The Commission has held that the element of "harm" is broad and "encompasses financial, physical, and emotional harm" and that "intent" can be found when the harms can be shown to be "substantially certain" to result from the spoofing. *Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, WC Docket No. 11-39, Report and Order, 26 FCC Rcd 9114, 9122, para. 22 (2011); *see also Affordable Enterprises of Arizona, LLC*, Notice of Apparent Liability for Forfeiture, 33 FCC Rcd 9233, 9242-43, para. 26 n.70 (2018) (citing Restatement (Second) of Torts § 8A, comment b, p. 15 ("Intent is not . . . limited to consequences which are desired. If the actor knows that the consequences are certain, or substantially certain, to result from his act, and still goes ahead, he is treated by the law as if he had in fact desired to produce the result.")). *Cf. Burr v. Adam Eidemiller, Inc.*, 386 Pa. 416 (1956) (intentional invasion can occur when the actor knows that it is substantially certain to result from his conduct); *Garratt v. Dailey*, 13 Wash. 2d. 197 (1955) (finding defendant committed an intentional tort when he moved a chair if he knew with "substantial certainty" that the plaintiff was about to sit down). Affordable Enterprises was assessed a $37,525,000 forfeiture for its actions. *Affordable Enterprises of Arizona, LLC*, Forfeiture Order, 35 FCC Rcd 12142, 12143, para 3 (2020). In the case of high-volume calls, intent has been imputed where the caller knows it does not have a right to use the number. *See Spiller NAL*, 35 FCC Rcd at 5959, para. 25. Similarly, repeated spoofing of unassigned numbers is a strong indicator of harmful intent. *Best Insurance Contracts, Inc, and Philip Roesel et al.*, Forfeiture Order, 33 FCC Rcd 9204, 9215-16, n.85 (2018); *see also Best Insurance Contracts Inc., and Philip Roesel, et al*., Notice of Apparent Liability for Forfeiture, 32 FCC Rcd 6403, 6411, para. 23 (2017); *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 9706, 9713, para. 18 (2017) (*2017 Call Blocking Order*) ("Use of an unassigned number provides a strong indication that the calling party is spoofing the Caller ID to potentially defraud and harm a voice service subscriber. Such calls are therefore highly likely to be illegal.").

[10] *See* Consolidated Appropriations Act, 2018, Pub. L. No. 115-141, Div. P, Title V, § 503, 132 Stat. 348, 1091-94 (2018) (codified as amended in 47 U.S.C. § 227(e)) (RAY BAUM'S Act).

7. The Commission and Congress have long acknowledged that illegal robocalls that originate abroad are a significant part of the robocall problem.[11] Congress highlighted this problem in 2018 when it passed RAY BAUM'S Act, which prohibits spoofing calls or texts originating outside the U.S.[12] While these calls pose a significant problem, our jurisdiction does not directly apply to foreign entities. As the Michigan Attorney General recently noted, "[i]llegal robocalls continue to plague consumers nationwide, and when these calls originate from overseas, enforcement becomes increasingly difficult."[13] To help address these concerns, the Commission has now established partnerships between the Enforcement Bureau and Attorneys General in 29 states and the District of Columbia to collaborate to stop robocalls, including foreign-originated robocalls.[14]

8. *STIR/SHAKEN Caller ID Authentication.* The STIR/SHAKEN caller ID authentication framework[15] allows for the identification of call originators spoofing numbers by enabling authenticated caller ID information to securely travel with the call itself throughout the entire call path.[16] The Commission, consistent with Congress's direction in the Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act,[17] adopted rules requiring voice service providers[18] to

[11] For example, in a 2011 report to Congress, the Commission stated that "caller ID spoofing directed at the United States by people and entities operating outside the country can cause great harm." *Caller Identification Information in Successor or Replacement Technologies*, Report, 26 FCC Rcd 8643, 8655, para. 25 (2011). For more details, *see Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17-59 & Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17-97, FCC 21-105, at para. 5 (rel. Oct. 1, 2021) (*Gateway Provider Notice*).

[12] *See* RAY BAUM'S Act.

[13] Press Release, Department of Attorney General, Attorney General Nessel Works to Stop International Scam Calls (Jan. 14, 2022), https://www.michigan.gov/ag/0,4534,7-359-92297_47203-575599--,00 html.

[14] Press Release, FCC, Majority of U.S. States Have Joined FCC in Robocall Investigation Partnerships Chairwoman Rosenworcel Announces Latest Additions to State-Federal Partnerships to Combat Robocalls (Apr. 7 2022), https://docs.fcc.gov/public/attachments/DOC-382160A1.pdf; *see also* FCC, *FCC-State Robocall Investigation Partnerships*, https://www fcc.gov/fcc-state-robocall-investigation-partnerships (last visited Apr. 27 2022) (listing 28 federal-state partnerships). Two additional states have since signed MOUs with the Commission, Florida and South Carolina.

[15] More specifically, a working group of the Internet Engineering Task Force (IETF) called the Secure Telephony Identity Revisited (STIR) developed several protocols for authenticating caller ID information. *See Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, 36 FCC Rcd 1859, 1862-63, para. 7 (2020) (*Second Caller ID Authentication Report and Order*). And Alliance for Telecommunications Industry Solutions (ATIS), in conjunction with the SIP Forum, produced the Signature-based Handling of Asserted information using toKENs (SHAKEN) specification, which standardizes how the protocols produced by STIR are implemented across the industry. *Id.*

[16] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1862, para. 6.

[17] Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105 (2019) (codified in 47 U.S.C. § 227b) (TRACED Act).

[18] Because the TRACED Act defines "voice service" in a manner that excludes intermediate providers, our authentication and Robocall Mitigation Database rules use "voice service provider" in this manner. *See* 47 U.S.C. § 227b(a)(2)(A); 47 CFR § 64.6300(m) (defining voice service as "any service that is interconnected with the public switched telephone network and that furnishes voice communications to an end-user using resources from the North American Numbering Plan or any successor"). Our call blocking rules, many of which the Commission adopted prior to adoption of the TRACED Act, use a definition of "voice service provider" that includes intermediate providers. In that context, use of the TRACED Act definition of "voice service" would create inconsistency with our existing rules. *See, e.g.*, *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Fourth Report and Order, 35 FCC Rcd 15221, 1552 n.2 (2020) (*Fourth Call Blocking Order*). To avoid confusion,
(continued….)

implement STIR/SHAKEN in the IP portions of their voice networks by June 30, 2021,[19] subject to certain exceptions.[20]

9. 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.[21] The first component requires that the provider authenticating the call attach additional, encrypted information to the metadata that travels along with a call, as well as the provider's unique "certificate" which allows the terminating provider to verify that the caller ID is legitimate.[22] To maintain trust and accountability in the providers that vouch for the caller ID information, a neutral governance system issues these certificates.[23] Under the current Governance Authority rules, a provider must meet certain requirements to receive a certificate.[24]

10. The Commission requires voice service providers subject to a STIR/SHAKEN implementation extension—including smaller voice service providers and voice service providers with non-IP technology—to adopt and implement robocall mitigation practices in lieu of caller ID authentication.[25] These providers must commit to responding "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 robocalls that use its service to originate calls."[26] In adopting this requirement, the Commission explained that, if it determined that its

---

for purposes of this item, we use 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, we use "provider" and specify the type of provider as appropriate. Unless otherwise specified, we mean any provider, regardless of its position in the call path.

[19] 47 CFR § 64.6301; *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3252, para. 24.

[20] 47 CFR §§ 64.6304, 64.6306; *see also Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1876-83, 1897-907, paras. 36-51, 74-94.

[21] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1862-63, para. 7.

[22] *See id.* at 1863, para. 8.

[23] *See id.* at 1864, para 11.

[24] *See* STI Governance Authority, STI-GA Policy Decisions Binder, Version, 3.2 at 6 (Oct. 29, 2021), Policy Decision 001: SPC Token Access Policy, version 1.2 (May 18, 2021), https://sti-ga.atis.org/wp-content/uploads/sites/14/2021/10/211029-STIGA-Board-Policy-Decision-Binder-v3-2-Final.pdf (STI-GA Token Access Policy). To obtain a token, the Governance Authority policy requires that a provider must "(1) [h]ave a current FCC Form 499A on file with the Commission . . .; (2) [h]ave been assigned an Operating Company Number (OCN) . . . ; [and] (3) [h]ave certified with the FCC that they have implemented STIR/SHAKEN or comply with the [Commission's] Robocall Mitigation Program requirements and are listed in the FCC Robocall Mitigation Database, or have direct access to numbering resources." *Id*.

[25] 47 CFR §§ 64.6304, 64.6305; *see also Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1876-83, 1897-907, paras. 36-51, 74-94. We recently shortened the extension for "non-facilities-based" small voice service providers (100,000 or fewer voice access lines lines) by one year, so that they must implement STIR/SHAKEN in the IP portions of their networks by June 30, 2022. *See Call Authentication Trust Anchor,* WC Docket No. 17-97*,* Fourth Report and Order, FCC 21-122, at para. 23 (rel. Dec. 10, 2021) (*Small Provider Order*).

[26] 47 CFR § 64.6305(b)(2)(iii). Congress required the Commission to select a single consortium to "conduct[] private-led efforts to trace back the origin of suspected unlawful robocalls." TRACED Act § 13(d)(1), 133 Stat. at 3287. Pursuant to this directive, the Commission's Enforcement Bureau selected the Industry Traceback Group (ITG) as the industry traceback consortium. *See Implementing Section 13(d) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act)*, EB Docket No. 20-22, Report and Order, 35 FCC Rcd 7886 (EB 2020).

standards-based approach to mitigation was not sufficient, it would "not hesitate to revisit the obligations we impose through rulemaking at the Commission level."[27]

11. Voice service providers were required, by June 30, 2021, to submit a certification to the Robocall Mitigation Database, stating whether they had implemented STIR/SHAKEN on all or part of their networks and, if they had not fully implemented STIR/SHAKEN, describe their robocall mitigation program and "the specific reasonable steps the voice service provider has taken to avoid originating illegal robocall traffic."[28] The Commission prohibited intermediate providers and terminating providers from accepting calls directly from a voice service provider, including a foreign provider, that uses NANP resources that pertain to the United States in the caller ID field if the voice service provider has not filed in the Robocall Mitigation Database.[29] This prohibition became effective on September 28, 2021; however, the Commission held enforcement of that requirement with respect to foreign voice service providers in abeyance in the *Gateway Provider Notice* and sought comment on whether to expand or limit the foreign voice service provider prohibition.[30]

12. In addition to placing these obligations on voice service providers, the Commission required intermediate providers to implement STIR/SHAKEN in their IP networks. In the *Second Caller ID Authentication Report and Order*, the Commission required intermediate providers with IP networks to pass authenticated caller ID information unaltered to the next provider in the call path[31] and either authenticate caller ID information for all SIP calls it receives for which the caller ID information has not been authenticated[32] or, in the alternative, cooperatively participate with the industry traceback consortium and respond fully and in a timely manner to all traceback requests regarding calls for which it acts as an intermediate provider.[33]

13. *Call Blocking and Other Approaches to Mitigation.* Caller ID authentication is one important part of the Commission's attack on illegal robocalls. Another is robocall mitigation, especially empowering and encouraging domestic providers to voluntarily block unwanted and illegal calls.[34] At the

---

[27] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1902, para. 81.

[28] 47 CFR § 64.6305(b)(2)(ii). As of May 17, 2022, 6,285 voice service providers have filed in the Robocall Mitigation Database: 1,728 attest to full STIR/SHAKEN implementation, 1,495 state that they have implemented a mix of STIR/SHAKEN and robocall mitigation, and 3,062 state that they rely solely on robocall mitigation.

[29] *Id.* § 64.6305(c); *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1904, para. 87. The prohibition went into effect on September 28, 2021. *See Wireline Competition Bureau Announces Opening of Robocall Mitigation Database and Provides Filing Instructions and Deadlines*, WC Docket No. 17-97, Public Notice, 36 FCC Rcd 7394 (WCB 2021). The Commission emphasized that the rule did not constitute the exercise of jurisdiction over foreign voice service providers. Because the rule did not require foreign voice service providers to submit a certification into the Robocall Mitigation Database, it did not have an impermissible, direct effect on foreign voice service providers. *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1910, n.370. As discussed in the accompanying *Order on Reconsideration*, the Commission extended this rule to traffic sent directly by foreign voice service providers that use "North American Numbering Plan resources that pertain to the United States to send voice traffic to residential or business subscribers in the United States." 47 CFR § 64.6305(c).

[30] *Gateway Provider Notice* at para. 106.

[31] 47 CFR § 64.6302(a). The Commission created two exceptions from this rule under which an intermediate provider may remove the authenticated caller ID information: (1) where necessary for technical reasons to complete the call; and (2) where the intermediate provider reasonably believes the caller ID authentication information presents an imminent threat to its network security. *Id.* at (a)(1)-(2).

[32] *Id.* § 64.6302(b).

[33] *Id.* § 64.6302(b)(1)-(2).

[34] *See, e.g.*, *2017 Call Blocking Order*, 32 FCC Rcd at 9710-21, paras. 10-40 (establishing that certain calls may be blocked based on the number from which the call purports to originate); *Advanced Methods to Target and Eliminate* (continued….)

same time, the Commission has adopted affirmative obligations, which apply to all domestic providers in the call path where appropriate, to help eliminate illegal calls from the network and encourage providers to be good actors in the calling ecosystem.[35]

14. The Commission has taken several steps to encourage terminating providers and, in some instances, other providers in the call path, to block calls that are either unwanted or highly likely to be illegal, including adopting safe harbors to protect providers from liability for blocking errors.[36] In the *2017 Call Blocking Order*, Commission adopted clear, bright-line rules authorizing any provider in the call path to block certain calls based on the number in the caller ID field.[37] It also permits blocking based on a do-not-originate (DNO) list, which includes numbers that should never be used to originate calls.[38]

15. Since the *2017 Call Blocking Order*, the Commission has taken a flexible approach to respond to the ever-evolving tactics of bad actors. The Commission has primarily focused on permitting terminating providers to block based on reasonable analytics designed to identify either unwanted or illegal calls, and taken steps to ensure that those providers are protected from liability in doing so.[39] Along with this analytics-based approach, the Commission has established a safe harbor from liability for any provider in the call path to block calls from a bad-actor upstream provider that fails to effectively mitigate illegal traffic after being notified of such traffic by the Commission.[40]

16. In addition to blocking, the Commission has adopted three affirmative obligations for

---

Unlawful Robocalls, *Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, 34 FCC Rcd 4876, 4884-91, paras. 26-46 (2019) (*Call Blocking Declaratory Ruling and Further Notice*) (making clear that terminating providers may block calls in certain instances); *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Third Report and Order, Order on Reconsideration, and Fourth Further Notice of Proposed Rulemaking, 35 FCC Rcd 7614, 7625-31, 7633-37, paras. 51-60, 25-45 (2020) (*Third Call Blocking Order and Further Notice*) (establishing two safe harbors for blocking, as well as certain protections in case of erroneous blocking); *Fourth Call Blocking Order*, 35 FCC Rcd at 15234-47, paras. 39-78 (expanding the analytics-based safe harbor and establishing several transparency and redress requirements).

[35] *Fourth Call Blocking Order*, 35 FCC Rcd at 15227-33, paras. 14-36.

[36] *See, e.g.*, 47 CFR § 64.1200(k); *2017 Call Blocking Order*, 32 FCC Rcd at 9710-21, paras. 10-40; *Call Blocking Declaratory Ruling and Further Notice*, 34 FCC Rcd at 4884-91, paras. 26-46; *Third Call Blocking Order and Further Notice*, 35 FCC Rcd at 7625-31, 7633-37, paras. 25-45, 51-60; *Fourth Call Blocking Order*, 35 FCC Rcd at 15234-47, paras. 39-78.

[37] 47 CFR § 64.1200(k)(1), (2)(i)-(iii); *see also 2017 Call Blocking Order*, 32 FCC Rcd at 9710-21, paras. 10-40. Because there is no legitimate reason for a caller to use these numbers, the Commission reasoned that these calls are highly likely to be illegal and no reasonable consumer would want to receive such a call. *2017 Call Blocking Order* at 9709, 9722, paras. 9, 44.

[38] *2017 Call Blocking Order* at 9710-13, paras. 10-17.

[39] 47 CFR § 64.1200(k)(3), (11); *Call Blocking Declaratory Ruling and Further Notice*, 34 FCC Rcd at 4884-91, paras. 26-46 (making clear that terminating providers may block calls based on reasonable analytics so long as consumers are given the opportunity to opt out); *Third Call Blocking Order and Further Notice*, 35 FCC Rcd at 7625-27, paras. 25-34 (adopting a safe harbor from violations of the Act and the Commission's rules for terminating providers that block based on reasonable analytics designed to identify unwanted calls, so long as the analytics take into account caller ID authentication information and consumers are given the opportunity to opt out); *Fourth Call Blocking Order*, 35 FCC Rcd at 15234-38, paras. 39-47 (expanding the safe harbor for blocking based on reasonable analytics to include certain network-level blocking by terminating providers, without consumer opt out, designed to identify calls that are highly likely to be illegal).

[40] 47 CFR § 64.1200(k)(4); *Third Call Blocking Order and Further Notice*, 35 FCC Rcd at 7627-31, paras. 35-45 (discussing protections for lawful calls).

providers.[41] First, providers must respond to all traceback requests from the Commission, law enforcement, or the industry traceback consortium, in a full and timely manner.[42] Second, providers must take steps to effectively mitigate illegal traffic when notified of such traffic by the Commission.[43] Finally, providers must adopt affirmative, effective measures to prevent new and renewing customers from using the network to originate illegal calls.[44]

17. *Gateway Provider Notice*. On September 30, 2021, the Commission adopted the *Gateway Provider Notice*, proposing to address foreign-originated illegal calls by enlisting gateway providers in the fight to keep these calls off the U.S. network and consumers' phones. First, the *Gateway Provider Notice* sought comment on requiring gateway providers to authenticate caller ID information consistent with STIR/SHAKEN for SIP calls that are carrying a U.S. number in the caller ID field.[45] Second, it sought comment on several robocall mitigation requirements, including requiring response to traceback in 24 hours, mandatory blocking options for gateway providers and the providers immediately downstream in the call path, know-your-customer, contractual terms, and a general mitigation requirement.[46] Finally, it sought comment on requiring gateway providers to submit a certification to the Robocall Mitigation Database describing their robocall mitigation practices and stating that they are adhering to those practices regardless of whether they had implemented STIR/SHAKEN, as well as additional issues related to the Robocall Mitigation Database.[47]

18. In the *Gateway Provider Notice*, we explained that the Enforcement Bureau and Department of Justice have taken action against gateway providers serving as a conduit for illegal robocalls.[48] And the Commission, recognizing the problem gateway providers pose, has taken further action against gateway providers in the last several months.[49]

---

[41] *Fourth Call Blocking Order*, 35 FCC Rcd at 15227-34, paras. 14-38.

[42] 47 CFR § 64.1200(n)(1); *Fourth Call Blocking Order*, 35 FCC Rcd at 15227-29, paras. 15-21.

[43] 47 CFR § 64.1200(n)(2); *Fourth Call Blocking Order*, 35 FCC Rcd at 15229-32, paras. 22-31. The Commission noted that "blocking may be necessary for gateway providers to comply with these requirements." *Fourth Call Blocking Order*, 35 FCC Rcd at 15231, para. 26.

[44] 47 CFR § 64.1200(n)(3); *Fourth Call Blocking Order*, 35 FCC Rcd at 15232-33, paras. 32-36.

[45] *Gateway Provider Notice* at paras. 38-50.

[46] *Id.* at paras. 51-93.

[47] *Id.* at paras. 94-102.

[48] *See id.* at paras. 28-29.

[49] *See* Press Release, FCC, FCC Demands Three More Companies Immediately Stop Facilitating Illegal Robocall Campaigns (Oct. 21, 2021), https://docs fcc.gov/public/attachments/DOC-376789A1.pdf (announcing that the Commission sent cease-and-desist letters to Duratel, Primo Dialer, and PZ/Illium Telecommunication) (*Duratel et al. Press Release*). The Enforcement Bureau has now sent "more than a dozen" cease and desist letters to providers "suspected of facilitating illegal robocall traffic." Press Release, FCC, FCC Continues to Send Cease-And-Desist Letters to Voice Service Providers Suspected of Facilitating Illegal Robocalls (Feb. 17, 2022), https://docs.fcc.gov/public/attachments/DOC-380416A1.pdf; *see also* Press Release, FCC, FCC Warns Robocall Facilitators to Remove Illegal Robocall Traffic From Their Networks or Be Disconnected from Downstream Providers (Mar. 22, 2022), https://docs.fcc.gov/public/attachments/DOC-381603A1.pdf (announcing that the Commission sent cease-and-desist letters to Hello Miami, Airespring and ThinQ). These are only the most recent Commission actions. *See* Letter from Rosemary C. Harold, Chief, Enforcement Bureau, FCC, to Brick Kane, Pres., Globex Telecom, at 1-2 (Feb. 4, 2020) (https://docs.fcc.gov/public/attachments/DOC-362255A1.pdf); Press Release, FCC, FCC, FTC Demand Gateway Providers Cut Off Robocallers Perpetrating Coronavirus-Related Scams from United States Telephone Network (Apr. 3, 2020), https://docs fcc.gov/public/attachments/DOC-363522A1.pdf (noting that the FTC and FCC wrote to three gateway providers and demanded that they stop facilitating scam COVID-19-related robocalls from the Philippines and Pakistan); In May 2020, the FTC and FCC sent an additional

(continued….)

III. GATEWAY PROVIDER REPORT AND ORDER

19. In this *Gateway Provider Report and Order*, we take steps to protect consumers from foreign-originated illegal robocalls. Gateway providers' networks are the key entry point for foreign-originated robocalls, and the authentication and mitigation requirements we adopt today will ensure that American consumers are protected. We define the term "gateway provider," require such providers to authenticate all unauthenticated SIP calls in the IP portions of their networks, and adopt mitigation requirements specific to such providers, including requirements related to the Robocall Mitigation Database. As explained below, we find that the benefits of these new requirements, particularly to American consumers deluged by illegal calls originating in other countries, will far outweigh the short-term implementation costs imposed on gateway providers.

A. Need for Action

20. *Current Rules Addressing Foreign-Originated Robocalls Are Insufficient to Stop the Deluge of Illegal Robocalls Originating Abroad.* As proposed, we conclude that consumers will benefit from caller ID authentication and illegal robocall mitigation requirements applied to gateway providers to address the problem of foreign-originated illegal robocalls.

21. Commenters overwhelmingly support additional action to stop the flood of foreign-originated illegal calls.[50] For example, Comcast agrees with the Commission that the current rules "are not sufficient to resolve the problem of foreign-originated illegal robocalls" and that the robocall landscape "warrants consideration of further regulatory efforts targeting gateway providers."[51] The State Attorneys General also support steps to stop the "continued deluge of illegal foreign-based robocalls that use spoofed, U.S.-based phone numbers."[52]

22. Foreign robocallers use U.S. NANP numbers in myriad ways to reach U.S. end users. In some cases, the foreign robocallers utilize spoofed U.S. numbers,[53] while in other cases they have

---

three letters to three separate gateway providers regarding similar campaigns originating in the UK, Germany, and other destinations abroad. Press Release, FCC, FCC, FTC Demand Robocall-Enabling Service Providers Cut Off Covid-19-Related International Scammers (May 20, 2020), https://docs.fcc.gov/public/attachments/DOC-364482A1.pdf; Press Release, FCC, FCC Demands Two More Companies Immediately Stop Facilitating Illegal Robocall Campaigns (May 18, 2021), https://docs fcc.gov/public/attachments/DOC-372543A1.pdf; *see also* Press Release, FCC, FCC Calls on Carriers to Ensure Free Consumer Tools Are Available to Block Robocalls and Issues New Robocall Cease-and-Desist Letters (Apr. 13, 2021), https://docs.fcc.gov/public/attachments/DOC-371553A1.pdf; US Department of Justice, Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, 2020 Report to Congress at 3, https://www.justice.gov/opa/press-release/file/1331576/download; *see also United States of America v. Nicholas Palumbo, et al.*, Civil Action No. 20-CV-473, Complaint, para. 8, p.4 (filed Jan. 28, 2020 E.D.N.Y.); *see also* ZipDX Comments at 11 (stating that these cases are representative of the role gateway providers play in allowing foreign-originated calls into the U.S.).

[50] *See, e.g.*, AB Handshake Comments at 1 (asserting that "[t]o finally tame the scourge of illegal robocalls, the Commission must find a way to address calls that originate outside the United States"); i3forum Comments at 2 (stating that it "supports the Commission's goal of eliminating the scourge of illegal robocalling and agrees that gateway providers, which are a point of entry for foreign calls terminating in the United States, should lend a hand in the fight against illegal robocalls originating abroad") INCOMPAS Comments at 6; USTelecom Comments at 1 (asserting that "more action is necessary to address foreign-originated robocalls"); (internal citations omitted); 51 State AGs Reply at 3.

[51] Comcast Comments at 2.

[52] 51 State AGs Reply at 2; *see also id*. at 3 ("Like the Commission, many of our offices report that "unwanted calls, including illegal robocalls, are consistently . . . a top source of consumer complaints.").

[53] *See id*. ("Based upon consumer complaints received by our respective offices, these fraudulent, foreign-originated robocalls often involve caller ID spoofing of U.S.-based phone numbers."); Enterprise Communications Advocacy (continued….)

obtained U.S. NANP numbers from providers who have themselves obtained numbers on the secondary market or directly from the North American Numbering Plan Administrator (NANPA).[54]

23. Commenting parties agree that foreign-originated calls are a significant portion, if not the majority, of illegal robocalls.[55] The latest data from the Industry Traceback Group support the conclusion that many providers facilitating illegal robocalls are gateway providers and the upstream foreign originating and intermediate providers from whom they receive foreign-originating calls. Of the 347 providers identified in the Industry Traceback Group's 2021 report as responsible for transmitting illegal robocalls, 111 were gateway providers that brought the traffic into the U.S. network, and 115 were foreign providers originating illegal robocalls.[56] According to the Industry Traceback Group, 10% of all providers that are not responsive to traceback requests constitute 48% of all non-responsive traceback requests. Of that 10%, over two-thirds are foreign providers.[57] Recent action after the release of the *Gateway Provider Notice* by the Commission's Enforcement Bureau underscores the need for action against foreign-originated robocalls, including cease-and-desist letters the Enforcement Bureau sent to three companies for transmitting illegal robocalls, "many of which originate overseas."[58]

24. *Role of Gateway Providers*. We conclude that gateway providers serve as a critical choke-point for reducing the number of illegal robocalls received by American consumers, a conclusion confirmed by the record.[59] Gateway providers can stop illegal calls to customers before they reach terminating providers,[60] or, as the ITG data demonstrates, readily allow such calls into the U.S. market.[61] State Attorneys General argue that "in most cases" robocalling fraud results from "foreign actors gaining

---

Coalition Reply at 2 (noting that number spoofing is harmful to both the entity being spoofed and the call recipient); NCTA Comments at 1 (arguing that foreign providers are spoofing calls).

[54] *See* ZipDX Comments at 12 (noting that "[t]he primary approach we have observed is random spoofing" but that in other cases, illegal robocallers "obtain USA numbers" from "resellers"); USTelecom Reply at 4 (noting robocallers sometimes use properly assigned numbers).

[55] *See Gateway Provider Notice* at para. 26; AB Handshake Comments at 1 (noting that "foreign-originated calls using spoofed caller ID information continue to be a significant source of illegal robocalling and robocalling fraud"); Belgacom International Carrier Services Comments at 1 (asserting that there is a "large amount of robocalls generated outside" of the U.S.); Twilio Comments at 1-2 (stating that its "own traceback efforts show that fraudulent calls often originate from bad actors overseas"); YouMail Comments at 2-3 (stating that "foreign providers using NANP resources are a major (if not, the primary) source of robocalls"); Enterprise Communications Advocacy Coalition Reply at 1 (referencing a literary classic to argue that "[i]t is a truth universally acknowledged that an immense share of illegal calls . . . originate outside the United States"); NCTA Reply at 1 (noting that its "members' experiences show – a significant number of illegal robocalls originate abroad").

[56] *See* Letter from Joshua M. Bercu, Vice Pres., Policy and Advocacy, USTelecom, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 20-195 at 2 (filed Nov. 15, 2021) (ITG Nov. 15 *Ex Parte*).

[57] *See* Letter from Joshua M. Bercu, Vice Pres., Policy and Advocacy, USTelecom, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 17-97, CG Docket No. 17-59, Attach. at 11 (filed Mar. 29, 2022) (ITG Mar. 29 *Ex Parte*).

[58] *See Duratel et al. Press Release* at 1.

[59] *See, e.g.*, T-Mobile Comments at 2 (arguing that the Commission should focus its efforts on gateway providers); Verizon Reply at 12 (arguing that the Commission should go further, but that it is "appropriate for the Commission to look to address the foreign-originated robocall mitigation problem by protecting the edges of the PSTN").

[60] *See* Letter from Indra Sehdev Chalk, T-Mobile USA, Inc., to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59, WC Docket No. 17-97, at 2 (arguing that it is already mitigating calls as an intermediate provider) (T-Mobile Feb. 2 *Ex Parte*); Verizon Reply at 2 (same).

[61] *See* ITG Nov. 15 *Ex Parte* at 2; *see also* North American Numbering Council Call Authentication Trust Anchor Working Group, Best Practices for the Implementation of Call Authentication Frameworks at 14 (2020), https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf (2020 NANC Best Practices Report) (recognizing the key role that gateway providers play in facilitating illegal robocalls).

access to the U.S. phone network through international gateway providers."[62] State actions against gateway providers following the *Gateway Provider Notice* reinforce this conclusion.[63]

B. Scope of Requirements and Definitions

25. *Definition of Gateway Provider.* We define a "gateway provider" as a U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider, a slightly modified version of the definition we proposed in the *Gateway Provider Notice*.[64] By "U.S.-based," we mean that the provider has facilities located in the U.S., including a point of presence capable of processing the call.[65] By "receives a call directly" from a provider, we mean the foreign provider directly upstream of the gateway provider in the call path sent the call to the gateway provider, with no providers in-between. Commenters support our proposed definition,[66] with some suggesting minor modifications addressed below.[67]

26. In the *Gateway Provider Notice*, we initially proposed to define a gateway provider as "the first U.S.-based intermediate provider in the call path of a foreign-originated call that transmits the call directly to another intermediate provider or a terminating voice service provider in the United States."[68] We add "receives a call directly from a foreign originating provider or foreign intermediate provider" and drop "foreign-originated call" from our adopted definition for several reasons. First, as commenters note, a gateway provider may not know the identity or location of the entity that originated the call, but it will know the identity of the immediate upstream provider that sent the call to the gateway provider, including whether that provider has registered as a foreign provider in the Robocall Mitigation Database.[69] Our adopted definition ensures that a provider will be considered a gateway provider for any call it receives directly from a foreign provider that the provider does not itself terminate. Second, our

---

[62] *See* 51 State AGs Reply at 3.

[63] *See, e.g.*, *State of North Carolina, ex rel. Joshua H. Stein v. Articul8, LLC et al.*, Complaint for Injunctive Relief and Civil Penalties at 2, Case No. 1:22-cv-00058 (filed Jan. 25, 2022 M.D.N.C.) (stating in the complaint against Articul8, a gateway provider, that the company "allows scammers and fraudsters to access the U.S. telephone network and bombard U.S. consumers with fraudulent and illegal telemarketing calls and robocalls"); *State of Indiana v. Startel Communications et al.*, Complaint for Civil Penalties, Permanent Injunction, Other Equitable Relief, and Demand for Jury Trial at 16, Case No. 3:21-cv-00015-RLY-MPB (filed Oct. 14, 2021 S.D. Idaho) (stating in the complaint against Startel and other gateway providers that "[w]ithout Startel's support . . . foreign robocallers would not have been able to use telephone numbers beginning with a +1 to directly contact [Indiana consumers]" and that "robocallers needed Startel to be the point of entry into the United States").

[64] *See Gateway Provider Notice* at para. 33.

[65] *Id*.; Letter from Michael H. Pryor, Counsel, iBasis, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 17-97, CG Docket No. 17-59, at 2 (filed Sept. 22, 2021) (suggesting inclusion of a U.S.-based point-of-presence as part of the definition of "U.S.-based"); INCOMPAS Comments at 5 (same); *see also* Letter from David Frankel, CEO, ZipDX, to Marlene H. Dortch, Secretary FCC, CG Docket No. 17-59, WC Docket No. 17-97 at n.4 (filed May 2, 2022) (ZipDX May 2 *Ex Parte*).

[66] *See, e.g.*, iBasis Comments at 3-4 (agreeing with proposed definition); 51 State AGs Reply at 2 n.5.

[67] *See, e.g.*, INCOMPAS Comments at 5 (arguing for modifications to make clear that "affiliates of a U.S.-licensed provider or other U.S.-licensed entities that receive traffic in another country and transmit it to the United States would not qualify" as gateway providers); Twilio Comments at 2 (arguing for a definition that includes terminating providers).

[68] *Gateway Provider Notice* at para. 33.

[69] *See*, *e.g.*, Belgacom International Carrier Services Comments at 5; USTelecom Comments at 5; Twilio Comments; iconectiv Comments at 2. *But see* VON Reply at 2 (arguing it can be extremely difficult to know if a provider is a foreign provider); Verizon Reply at 12-13 (same). As explained below, we clarify foreign intermediate providers' traffic will be blocked unless they register in the Robocall Mitigation Database.

definition ensures that calls sent on a circuitous path out of and then back into the U.S. will be brought within the regime.[70] In that scenario, the U.S.-based provider acts as a gateway provider at the point in the call path when the foreign provider immediately upstream of the gateway provider sends the call to the gateway provider, even for calls originated within the United States. We agree with commenters that "U.S.-based facilities" for the purpose of our definition means that the provider has facilities in the U.S., including, at a minimum, a U.S.-located point of presence.[71]

27. We clarify that foreign affiliates of a U.S.-based provider or other U.S.-licensed entities that receive traffic in another country and transmit that traffic to another provider to bring across the boundary of the U.S. network are not gateway providers.[72] As proposed, we do not include in the definition providers that also terminate the call because they are then acting as terminating providers and are subject to the existing rules applicable to such providers.[73] In their capacity as terminating providers, these providers have existing obligations to prevent their own end users from receiving illegal robocalls.[74]

28. *Call-by-Call Basis*. Consistent with the proposal in the *Gateway Provider Notice*, we adopt the gateway provider classification on a call-by-call basis.[75] That is, a provider is a gateway provider and subject to the rules for gateway providers we adopt in this *Order* only for those calls for which it acts as a gateway provider unless otherwise noted.[76]

29. As we noted in the *Gateway Provider Notice*, we took this approach when classifying intermediate and voice service providers with respect to our caller ID authentication rules.[77] We adopt the call-by-call classification to ensure that gateway providers, due to their key role in the call path, are subject to the requirements we adopt today.[78] There is record support for this approach.[79] Concluding that the burdens are overstated, we reject concerns of commenters that assert that the call-by-call classification would not be administratively feasible, and would potentially impose two different sets of regulations on the same set of providers, causing confusion.[80] As we note, and a number of commenters agree, a gateway provider will know the identity of the immediate upstream provider from which it

---

[70] *See* ZipDX Comments at 14 (noting that "convoluted routing scenarios exist").

[71] *See* INCOMPAS Comments at 5 (arguing that "U.S.-based" would mean "a U.S. located point of presence"); VON Reply at 1-2 (supporting INCOMPAS proposed clarification).

[72] *See* INCOMPAS Comments at 5; *id*. at 6 ("The Commission has enforcement authority over domestic providers and, rather than attempt to adopt new requirements for U.S.-licensed affiliates operating outside the country, the definition would better clarify which U.S.-based providers would be subject to the Commission's rules.").

[73] *Gateway Provider Notice* at para. 33 n.100; Twilio Comments at 2 (arguing that gateway providers should include providers that also terminate the call, but noting that such providers are already voice service providers and subject to our rules).

[74] A terminating provider is a voice service provider for purposes of section 4 of the TRACED Act and our caller ID authentication rules. *See* TRACED Act § 4(a)(2), 133 Stat. at 3287; 47 CFR § 64.6300(m). A voice service provider is required to, among other things, verify caller ID information pursuant to STIR/SHAKEN for traffic it terminates, 47 CFR § 64.6301(a)(3), and submit a certification to the Robocall Mitigation Database. 47 CFR § 64.6305(b).

[75] *Gateway Provider Notice* at para. 35.

[76] *Id*.

[77] *Id*.; *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1930, para. 15.

[78] *Gateway Provider Notice* at para. 35.

[79] Twilio Comments at 2.

[80] *See, e.g.*, Belgacom International Carrier Services Comments at 2; ZipDX Comments at 16; T-Mobile Comments at 4-5.

receives a call.[81] The gateway provider will also know whether that provider has registered as a foreign provider in the Robocall Mitigation Database. Our approach ensures that a gateway provider is subject to the consumer protection requirements we adopt today whenever it receives a call directly from a foreign provider.

30. Moreover, a call-by-call approach will have a limited practical burden for several reasons. As an initial matter, several of the obligations we adopt today do not require a gateway provider or providers downstream from the gateway provider to determine, in real time, whether or not the relevant provider is acting as a gateway provider for a particular call. First, the 24-hour traceback requirement and know-your-upstream provider requirements do not involve any real-time action on the part of a gateway provider when it receives the call.[82] Second, the obligation to block traffic upon notification by the Commission applies only to those entities identified by the Commission, so that providers need not identify relevant traffic in real-time in the first instance.[83] Third, if a provider acts as a gateway provider for *any* calls, it must submit a robocall mitigation plan to the Robocall Mitigation Database describing how it mitigates calls in its role as a gateway provider *generally*.[84] Fourth, where a downstream provider needs to block traffic from an upstream provider that has not filed in the Robocall Mitigation Database, it is required to do so if it has reason to believe it is a gateway or voice service provider for *any* calls.[85] Additionally, while gateway providers must undertake call blocking on a call-by-call basis at the time of the call for numbers on a DNO list, all domestic providers in the call path are already permitted to engage in such blocking and can therefore elect to apply such blocking to all calls,[86] rather than simply the calls for which they act as a gateway provider.[87] Similarly, while gateway providers must take "reasonable steps" to mitigate calls received as a gateway provider on a call-by-call basis, the burden of identifying the relevant calls is likely low; gateway providers should know those calls they receive from foreign providers and send downstream to another domestic provider and can apply the appropriate mitigation procedures to those calls. Indeed, several stated that they already do so.[88] At a minimum, to the extent a provider receives a call directly from a provider listed as "foreign" in the Robocall Mitigation Database, it is acting as a gateway provider for that call.[89]

31. We note that many providers already operate under multiple sets of obligations—for example, as intermediate providers and voice service providers under our caller ID authentication rules[90]—and no party has indicated why a call-by-call approach for gateway providers would be more burdensome. Moreover, no commenter proposed an alternative approach for imposing unique obligations

[81] *See, e.g.*, Belgacom International Carrier Services Comments at 5; iconectiv Comments at 2; Twilio Comments; USTelecom Comments at 5. *But see* VON Reply at 2 (arguing it can be extremely difficult to know if a provider is a foreign provider); Verizon Reply at 12-13 (same). As explained below, we clarify foreign intermediate providers' traffic will be blocked unless they register in the Robocall Mitigation Database.

[82] *See infra* Sections III.E.1 and III.E.3.

[83] *See id*. Section III.E.2.

[84] *See id*. Sections III.C and III.E.4.

[85] *See id*. Section III.C.

[86] *Id*.

[87] *See id*.; *see also* 47 CFR § 64.1200(k)(1)-(2).

[88] Twilio Comments at 4; Verizon Reply at 6.

[89] *See* ZipDX May 2 *Ex Parte* at 4 (alleging ambiguity regarding whether a provider is "foreign" and suggesting that other providers should rely on provider's Robocall Mitigation Database designation as foreign).

[90] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1930, para. 15.

on gateway providers.[91] We thus conclude that the burden on gateway providers to identify the appropriate regulatory regime applicable to a particular call will be limited.

32. *U.S. NANP Numbers*. Consistent with our proposal, we limit the scope of the requirements we adopt today for gateway providers to those calls that are carrying a U.S. number in the caller ID field.[92] By a "U.S. number," we mean NANP resources that pertain to the United States.[93] We exclude from the scope of our rules those calls that carry a U.S. number in the ANI field but display a foreign number in the caller ID field.[94] Commenters uniformly support this approach,[95] which is consistent with the scope of the prohibition on receiving calls carrying U.S. NANP numbers from foreign voice service providers not listed in the Robocall Mitigation Database.[96] Foreign-originated robocalls are successful to the extent that end users believe they are calls from U.S. customers or businesses, and we therefore conclude it is appropriate to focus our efforts on such calls.[97]

33. *No Traffic Carve-Outs*. Finally, we decline to exclude certain types of traffic from the consumer protections we adopt today. We therefore reject iBasis's contention that we should exempt from the rules we adopt today cellular roaming calls sent from U.S. customers abroad.[98] We also decline, at this time, to draw a distinction between "conversational" and "non-conversational traffic" and to require it to be segregated at the gateway and subject to different levels of regulatory scrutiny.[99] The record does not reflect sufficient evidence to justify the utility of these carve-outs, or explain how they could be implemented in an administrable way and in a manner that avoids robocallers gaming whatever call-length definitions we adopt. For example, we are concerned that, if we set a threshold for

[91] Many commenters assert that we should not impose unique obligations on gateway providers. We address that argument in Section III.E.4 *infra*.

[92] *See Gateway Provider Notice* at para. 32.

[93] *See id*. at para. 33; *see also Administration of the North American Numbering Plan*, CC Docket No. 92-237, Report and Order, 11 FCC Rcd 2588, 2590-91, paras. 3-4 (1995) ("The [NANP] is the basic numbering scheme that permits interoperable communications in the United States, Canada, Bermuda and most of the Caribbean. . . . The NANP erects a framework for assigning the telephone numbers upon which these services depend and for permitting international calls between its member countries to be completed without the need to dial international access codes and international country codes. . . . These numbers are a public resource.").

[94] *See Gateway Provider Notice* at para. 36; *see also* 47 CFR § 64.1600(b) ("The term 'ANI' (automatic number identification) refers to the delivery of the calling party's billing number by a local exchange carrier to any interconnecting carrier for billing or routing purposes, and to the subsequent delivery of such number to end users.").

[95] *See, e.g.*, YouMail Comments at 2-3; ZipDX Comments at 17.

[96] 47 CFR § 64.6305(c) (limiting application of the prohibition on receiving calls carrying U.S. NANP numbers from foreign providers not listed in the Robocall Mitigation Database to foreign voice service providers that "use[] North American Numbering Plan resources that pertain to the United States").

[97] For this reason, we conclude that including "in the caller ID field" within our definition and elsewhere in our newly adopted rules will not encourage a deluge of illegal robocalls using non-US numbers as ZipDX argues. *See* ZipDX May 2 *Ex Parte* at 5.

[98] iBasis Comments at 4-5 (arguing that cellular roaming calls and conversation calls in general should be excluded from the rules).

[99] ZipDX Comments at 38 (arguing that conversational and non-conversational traffic should be segregated and that conversational traffic would be defined as traffic with an "average call duration of at least 120 seconds AND at least 20% of the calls are longer than 2 minutes"); *see also* i3forum Comments at 11 (arguing that the Commission's proposals should only apply to the origination of a "high volume of calls" and that such traffic should be subject to a surcharge"). We note that we seek comment on some of these ideas in the accompanying *Further Notice*.

conversational traffic at a particular call length,[100] robocallers would find a way to avoid crossing it while continuing to send robocalls. We find, at this time, that analytics providers, who can and do take call-length patterns into account in determining whether a call is likely to be an illegal robocall,[101] are in the best position to make these sorts of determinations. These entities have the incentive and ability to react quickly to robocallers' shifting tactics and can do so without disclosing to bad actors the specific thresholds on which they rely.

C. Robocall Mitigation Database

34. We adopt our proposal to require gateway providers to submit a certification and mitigation plan to the Robocall Mitigation Database. As explained below, we require gateway providers to take "reasonable steps" to mitigate robocall traffic regardless of whether they have fully implemented STIR/SHAKEN.[102] Gateway providers' robocall mitigation plans must describe their robocall mitigation practices and state that they are adhering to those practices, regardless of whether they have fully implemented STIR/SHAKEN.[103] We also adopt a modified version of our proposal for downstream domestic providers receiving traffic from gateway providers to block traffic from such a provider if the gateway provider has not submitted a certification in the Robocall Mitigation Database[104] or if the gateway provider has been de-listed from the Robocall Mitigation Database pursuant to enforcement action. The vast majority of commenters supported these proposals.

35. *Gateway Provider Robocall Mitigation Database Filing Obligations.* We conclude that requiring gateway providers to submit a certification to the Robocall Mitigation Database describing their robocall mitigation practices and stating that they are adhering to those practices, in conjunction with the new robocall mitigation obligations we adopt elsewhere in this *Order*, is an appropriate extension of similar obligations that currently apply to other providers.[105] We further conclude that requiring gateway provider certification will encourage compliance and facilitate enforcement efforts and industry cooperation. The record reflects significant support for this action.[106] For example, iBasis, a gateway provider, "believes that it is appropriate to require such a submission" along with a mitigation plan.[107] While INCOMPAS and T-Mobile argue that gateway providers that have implemented STIR/SHAKEN should not have to submit a mitigation plan,[108] we disagree because of the importance of gateway providers in the call path and our conclusion that STIR/SHAKEN, on its own, will not eliminate illegal robocalls, particularly traffic originating from outside the United States.

---

[100] ZipDX Comments at 38.

[101] YouMail Comments at 9.

[102] *See infra* Section III.E.4.

[103] *Gateway Provider Notice* at para. 94.

[104] *Id.* at para. 98.

[105] *See, e.g.*, USTelecom Comments at 8; ZipDX Comments at 31-32 (arguing for similar obligations on all providers); Verizon Reply at 2.

[106] *See* Comcast Comments at 10 (noting that this rule "would reasonably extend the database filing requirements to another class of providers—giving the Commission and other service providers broader visibility into the implementation status of gateway providers"); USTelecom Comments at 3; ZipDX Comments at 32 (arguing that "the public interest will best be served if ALL providers are required to register in the [Robocall Mitigation Database], regardless of their role(s)"); 51 State AGs Reply at 12 (supporting gateway provider certification, including filing of a robocall mitigation plan); Verizon Reply at 19 (urging that all providers file a certification in the database along with a mitigation plan).

[107] iBasis Comments at 13; *see also id.* (arguing that a requirement is necessary even for intermediate providers like iBasis that have been imported from the rural call completion database); iBasis Reply at 5-6.

[108] INCOMPAS Comments at 9; T-Mobile Comments at 9.

36. The rules we adopt today require gateway providers to submit the same information to the Robocall Mitigation Database that voice service providers must submit under existing Commission rules,[109] except for the limited areas described below. Specifically, gateway providers must certify to the status of STIR/SHAKEN implementation and robocall mitigation on their networks; submit contact information for a person responsible for addressing robocall mitigation-related issues; and describe in detail their robocall mitigation practices.[110] Gateway providers may make confidential submissions consistent with our existing confidentiality rules.[111] Gateway providers must also certify that they will comply with traceback requests within 24 hours, unlike the current "reasonable period of time" applicable for voice service providers, or that it has received a waiver of that rule.[112]

37. Consistent with voice service providers' current obligations, we do not require gateway providers to describe their mitigation program in a particular manner,[113] with the exception of clearly explaining how they are complying with the know-your-upstream-provider obligation adopted in this *Order*.[114] We conclude that the Commission and the public will benefit from understanding how each provider chooses to comply with the know-your-upstream provider duty, both because compliance is critical to stopping the illegal carrying or processing of robocalls[115] and because providers may choose to comply with this duty in different ways. As USTelecom argues, "providers' robocall mitigation programs should reflect at least a basic level of vetting of the providers from whom they directly accept traffic – beyond ensuring that they are registered in the [Robocall Mitigation Database]."[116]

38. We also clarify that, consistent with existing Commission filing requirements in other contexts, all mitigation plans must be submitted in English or with a certified English translation.[117] To

[109] *See* 47 CFR § 64.6305.

[110] *See infra* Appx. A, 47 CFR § 64.6305.

[111] *Wireline Competition Bureau Adopts Protective Order for Robocall Mitigation Program Descriptions*, WC Docket No. 17-97, Public Notice, DA 21-1288, Appx. A (Protective Order), para. 2 (WCB Oct. 14 2021) (*Protective Order PN*) (defining confidential information filed as part of a robocall mitigation plan as information filed consistent with the protective order or sections 0.459 or 0.461 of the Commission's rules). As USTelecom notes, providers may only redact filings to the extent appropriate under our confidentiality rules. *See* USTelecom Comments at 8-9; *see also Protective Order PN* at 2-3 ("filings which are overly redacted are not appropriate. . . . we will not hesitate should we identify improper confidentiality requests").

[112] *See infra* Appx. A, 47 CFR § 64.6305.

[113] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1899, para. 76.

[114] *See infra* Section III.E.3.

[115] In several legal settlements with gateway providers, the gateway providers were required to comply with extremely detailed, and public, know-your-customer obligations. *See, e.g.*, *In re: VC Dreams USA LLC d/b/a Strategic IT Partner*, Assurance of Discontinuance, at 10 (executed Apr. 19, 2021 Vt. Super. Ct.), https://ago.vermont.gov/wp-content/uploads/2021/04/Executed-AOD-SITP.pdf (requiring the gateway provider to "agree to require its [c]ustomers to," among other things, notify the gateway provider if it has been subject to traceback requests or deemed a "[n]on-[c]ooperative" provider); *id*. at 6 (requiring gateway provider to drop customer if customer does not agree to provide know-your-customer information).

[116] USTelecom Comments at 5; *see also* Twilio Comments at 4; USTelecom Reply at 4; Verizon Reply at 6 (arguing that all intermediate providers should "describe with particularity the processes they follow to know the identities of the upstream providers they accept traffic from and to monitor those service providers for illegal robocall traffic").

[117] *See* 47 CFR § 1.355 ("Every document, exhibit, or other paper written in a language other than English, which shall be filed in any proceeding, or in response to any order, shall be filed in the language in which it is written together with an English translation thereof duly verified under oath to be a true translation. Each copy of every such document, exhibit, or other paper filed shall be accompanied by a separate copy of the translation."); *cf.* 47 CFR § 63.53(c) ("Applications submitted under Section 214 of the Communications Act for international services and any related pleadings that are in a foreign language shall be accompanied by a certified translation in English."); *see also*

(continued….)

remove any ambiguity, we also codify that requirement with respect to our STIR/SHAKEN rules. Plans that were not submitted in English or with a certified English translation must be updated no later than 10 business days following the effective date of this *Order*, consistent with our existing requirement for updating information in the Robocall Mitigation Database.[118]

39. We delegate to the Wireline Competition Bureau the authority to specify the form and format of any submissions, and we direct the Wireline Competition Bureau to comply with any requirements under the Paperwork Reduction Act attendant upon such action.[119] This includes whether gateway providers that are also voice service providers may either submit a separate certification and plan as a gateway provider or amend their current certification and any plan.[120] A gateway provider that is also a voice service provider should explain the mitigation steps it undertakes as a gateway provider and the mitigation steps it undertakes as a voice service provider, to the extent those mitigation steps are different for each role.[121] And as with voice service providers, and consistent with our proposal, we require gateway providers to update their certifications within ten business days of "any change in the information" submitted, ensuring that the information is kept up to date.[122]

40. We also note that we may take the same enforcement actions against a gateway provider whose certification is deficient or who fails to meet the standards of its certifications as is the case for voice service providers. This includes, but is not limited to, delisting the gateway provider from the Robocall Mitigation Database.[123] In the *Second Caller ID Authentication Report and Order*, the Commission set forth consequences for providers that file a deficient robocall mitigation plan or that "knowingly or negligently" originate illegal robocall campaigns, including removal from the Robocall Mitigation Database.[124] To promote regulatory symmetry and close any loopholes in our regime, gateway providers will be subject to similar consequences. Specifically, if we find that a certification is deficient, such as if the certification describes an ineffective program, or if we determine that a provider knowingly or negligently carries or processes illegal robocalls, we will take appropriate enforcement action.[125] These actions may include, among others, removing a certification from the database after providing notice to the gateway provider and an opportunity to cure the filing, requiring the gateway provider to submit to more specific robocall mitigation requirements, and/or the imposition of a forfeiture. Should we remove a gateway provider from the Robocall Mitigation Database, downstream providers must block that gateway provider's traffic as described below.

U.S. v. Rivera-Rosario, 300 F.3d 1, 5 (1st Cir. 2002) ("It is clear, to the point of perfect transparency, that federal court proceedings must be conducted in English.").

[118] *See* 47 CFR § 64.6305(b)(5).

[119] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1902-03, para. 83; *Wireline Competition Bureau Announces Opening of Robocall Mitigation Database and Provides Filing Instructions and Deadlines*, WC Docket No. 17-97, Public Notice, 36 FCC Rcd 7394 (WCB 2021).

[120] USTelecom Comments at 6 ("[T]he Commission should not require new filings of providers that have already submitted [a] robocall mitigation program. Rather, the Commission should require those providers to update their plans as necessary.").

[121] *See id.* (arguing that the Commission should "require that providers indicate in the [Robocall Mitigation Database] the role or roles they play in the ecosystem").

[122] *See* 47 CFR § 64.6305(b)(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 (b)(1) through (4) of this section."); *Gateway Provider Notice* at para. 97.

[123] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1906, para. 93.

[124] *See id.* at 1903, para. 85.

[125] *See id.*

41. Gateway providers must submit a certification to the Robocall Mitigation Database by 30 days following publication in the Federal Register of notice of approval by Office of Management and Budget (OMB) of any associated Paperwork Reduction Act (PRA) obligations.[126] We conclude that the deadline we adopt today will give providers sufficient time to prepare their submission following notification of OMB approval. If a gateway provider has not fully implemented STIR/SHAKEN by the filing deadline, it must so indicate in its filing.[127] It must then later update the filing within 10 business days of STIR/SHAKEN implementation.[128]

42. We do not at this time adopt a requirement for gateway providers to inform the Commission through an update to the Robocall Mitigation Database filing if the gateway provider is subject to a Commission, law enforcement, or regulatory agency action, investigation, or inquiry due to its robocall mitigation plan being deemed insufficient or problematic, or due to suspected unlawful robocalling or spoofing.[129] Similarly, we do not at this time require all or a subset of Robocall Mitigation Database filers to include additional identifying information.[130] While we conclude that taking these steps may have merit, we find the record is insufficient to support taking action at this time.[131] Instead, we seek comment in the accompanying *Further Notice* on imposing these obligations on all domestic providers in the call path.[132]

43. We also do not at this time extend this certification obligation to domestic intermediate providers other than gateway providers or require voice service providers that have already implemented STIR/SHAKEN to meet the "reasonable steps" standard and submit a robocall mitigation plan. However, we seek comment on doing so in the accompanying *Further Notice*.

44. *Gateway Provider Call Blocking*. We also extend the prohibition on accepting traffic from unlisted voice service providers to gateway providers as proposed.[133] This proposal received significant record support and will close a loophole in our regime.[134] Under this rule, downstream

---

[126] In the *Gateway Provider Notice*, we proposed a filing deadline of 30 days after the publication of this Order, but that did not account for OMB approval of PRA obligations. *Gateway Provider Notice* at para. 99.

[127] Below, we require gateway providers to authenticate unauthenticated SIP traffic pursuant to STIR/SHAKEN by June 30, 2023. *See infra* Section III.D.

[128] Given the importance of tracking gateway providers' mitigation efforts, we conclude that the benefit of an earlier filing deadline outweighs the burden for some providers to subsequently update their filing with their STIR/SHAKEN compliance status. *But see* Letter from Michael Pryor, Counsel for the Cloud Communications Alliance and iBASIS, to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59, WC Docket No. 17-97 at 3-4 (filed May 11, 2020) (CCA May 11 *Ex Parte*) (arguing that the Robocall Mitigation Database filing and authentication compliance dates should be harmonized to the later of January 1, 2023 or 30 days following notice of OMB approval of the relevant information collection requirements).

[129] *Gateway Provider Notice* at para. 97.

[130] *Id.* at para. 100 (seeking comment on whether we should require filers to provide "additional identifying indicia, such as Carrier Identification Code, Operating Company Number, and/or Access Customer Name Abbreviation").

[131] *See, e.g.*, USTelecom Comments at 6 (arguing that such identifying information would be helpful); ZipDX Comments at 32 (asserting "[w]e are doubtful that misbehaving providers will comply with [] a rule" requiring reporting enforcement actions"), 33 (arguing that requiring the submission of additional identifying information "could be helpful, but making this information mandatory is problematic").

[132] *See infra* Section VI.B.4.

[133] *Gateway Provider Notice* at para. 98; 47 CFR § 64.6305(c).

[134] *See* USTelecom Comments at 3 (arguing for a database filing obligation for all intermediate providers); ZipDX Comments at 32 (arguing that all providers should be required to file in the Robocall Mitigation Database and have their traffic blocked if they are not listed); NCLC and EPIC Reply at 7; Verizon Reply at 5; T-Mobile Feb. 2 *Ex*

(continued….)

providers will be prohibited from accepting any traffic from a gateway provider not listed in the Robocall Mitigation Database, either because the provider did not file or their certification was removed from the Robocall Mitigation Database as part of an enforcement action. We conclude that a gateway provider Robocall Mitigation Database filing requirement and an associated prohibition against accepting traffic from gateway providers not in the Robocall Mitigation Database will ensure regulatory symmetry between voice service providers and gateway providers and underscore the key role gateway providers play in stemming foreign-originated illegal robocalls. Consistent with our proposal, and the parallel requirement adopted for voice service providers in the *Second Caller ID Authentication Report and Order*, this prohibition will go into effect 90 days following the deadline for gateway providers to submit a certification to the Robocall Mitigation Database.[135]

45. As a result of gateway providers' affirmative obligation to submit a certification in the Robocall Mitigation Database, we conclude that downstream providers will no longer be able to rely upon any gateway provider database registration imported from the intermediate provider registry when making blocking determinations.[136] In the *Second Caller ID Authentication Report and Order*, we imported intermediate providers into the Robocall Mitigation Database from the intermediate provider registry to ensure that downstream providers did not inadvertently block traffic sent from the intermediate providers' networks.[137] At that time, no intermediate providers were subject to a Robocall Mitigation Database filing or mitigation requirement.[138] To the extent a gateway provider was imported into the Robocall Mitigation Database via the intermediate provider registry, that Robocall Mitigation Database entry is not sufficient to meet the gateway provider's Robocall Mitigation Database filing obligation or to prevent downstream providers from blocking traffic upon the effective date of the obligation for downstream providers to block traffic from gateway providers. Therefore, gateway providers must submit a certification to the Robocall Mitigation Database by 30 days following Federal Register publication of OMB approval of the relevant information collection requirements, and the downstream provider must begin blocking traffic within 90 days of that certification deadline if the gateway provider has not submitted a certification to the Robocall Mitigation Database. We delegate to the Wireline Competition Bureau to make the necessary changes to the Robocall Mitigation Database to indicate whether a gateway provider has made an affirmative filing (as opposed to being imported as an intermediate provider) and whether any provider's filing has been de-listed as part of an enforcement action. The Bureau may, pursuant to an enforcement action, remove the record of a providers' filing or clearly mark it in a way so that downstream providers may not rely on it.

46. For the purpose of the downstream providers' call blocking duty, we do not require the downstream provider to determine if a specific call was sent from a provider acting as a voice service provider or gateway provider for that call. Nevertheless, we recognize that it may not always be possible for the downstream provider to know whether the upstream provider is (1) a voice service provider or gateway provider whose traffic must be blocked if the provider did not make an affirmative certification in the Robocall Mitigation Database and has not been de-listed; or (2) an intermediate provider that is not a gateway provider, whose traffic should not be blocked. We therefore only require the downstream

---

Parte at 5 (arguing that gateway providers should be prohibited from "accepting traffic from providers not listed in the [Robocall Mitigation Database], including foreign-originated traffic").

[135] *Gateway Provider Notice* at para. 98.

[136] Previously, all intermediate providers were imported into the Robocall Mitigation Database from the rural call completion database's Intermediate Provider Registry so that all intermediate providers would be represented therein, giving voice service providers "confidence that any provider not listed in the Robocall Mitigation Database" was not in compliance with the Commission's rules. *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1904, para. 88 & n.340.

[137] *See id.* at 1904, n.340.

[138] *See id.*

provider to block calls if they have a reasonable basis to believe that the upstream provider acts, *for some calls*, as a voice service provider or gateway provider and that the provider did not affirmatively file or in the Robocall Mitigation Database or has been de-listed. We note we are proposing in the *Further Notice* to expand the obligation to submit an affirmative certification to the Robocall Mitigation Database to all domestic intermediate providers.[139] Adoption of that proposal should eliminate any of these implementation concerns. In that case, the downstream provider would simply check to see if the upstream provider affirmatively filed in the Robocall Mitigation Database and has not been de-listed and would block the call if appropriate. Nevertheless, we conclude we must act now with respect to gateway providers to stem the tide of foreign-originated calls.

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

48. Commenters disagreed whether intermediate providers' imported data should be deleted from the database.[140] Consistent with our direction to the Wireline Competition Bureau to make the necessary changes to the portal to effectuate the rules we adopt today, we direct the Bureau to determine how to manage the imported data of gateway providers and to announce its determination as part of its guidance described in the paragraph above.

49. *Public Safety Calls.* In the *Gateway Provider Notice*, we clarified that: (1) even if a provider is not listed in the Robocall Mitigation Database, other voice service providers and intermediate providers in the call path must make all reasonable efforts to avoid blocking calls from PSAPs and government outbound emergency numbers; and (2) emergency calls to 911 from originating providers not in the Robocall Mitigation database must not be blocked "under any circumstances."[141] We now codify these requirements and apply them as well to the new blocking obligations we adopt in this Order.[142] Codifying these clarifications with respect to providers not listed in the Robocall Mitigation Database are

[139] *See infra* Section VI.B.4.

[140] *See* iBasis Reply at 6 n.27 ("The Commission should reject USTelecom's suggestion that the Commission remove from the [Robocall Mitigation Database] any provider currently in the database that was imported by the Commission as an intermediate provider. . . . Instead, intermediate providers, or at least those that are also gateway providers should supplement their filing with a mitigation plan.").

[141] These clarifications reflect our existing requirements. *See* TRACED Act § 10(b) (codified at 47 U.S.C. § 227(j)(1)(C)); *2017 Call Blocking Order*, 32 FCC Rcd at 9721, para. 41; *see also Third Call Blocking Order and Further Notice*, 35 FCC Rcd at 7633-34, paras. 52-53 ("Calls to PSAPs via 911 . . . should never be blocked unless the voice service provider knows without a doubt that the calls are unlawful."); *see also* Letter from Sarah Leggin, Director, Regulatory Affairs, CTIA, to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59, WC Docket No. 17-97, at 4 (filed May 10, 2022) (CTIA May 10 *Ex Parte*) (asking us to clarify that gateway providers may block calls to 911 or other emergency numbers where the provider is working with a public safety agency to mitigate harm to service); Letter from Joshua M. Bercu, Vice President, Policy & Advocacy, USTelecom, to Marlene Dortch, Secretary, FCC, CG Docket No. 17-59, WC Docket No. 17-97, at 3 (filed May 6, 2022) (INCOMPAS et al. May 6 *Ex Parte*) (asking that we clarify, consistent with the existing rules, that this restriction applies only to emergency calls to 911 and does not prevent a gateway provider from blocking calls that are intended to cause harm to public safety).

[142] *See infra* Appx. A § 64.6305(e)(4).

consistent with our action today to similarly codify these safeguards in our other blocking rules[143] and will ensure completion of emergency calls is subject to the same safeguards regardless of the rule under which the call would otherwise be blocked. There was record support for this approach.[144] We disagree with ZipDX that our clarification in the *Gateway Provider Notice* and its expansion to gateway providers would not be administratively feasible.[145] Providers have had to comply with our public safety exception to blocking for other purposes for several years, and ZipDX does not adequately explain why applying this exception to traffic sent from providers not in the Robocall Mitigation Database now would be different. Additionally, in balancing any implementation concerns against the critical importance of completing emergency calls, we conclude that adopting and expanding the public safety exception is in the public interest.

50. We also sought comment in the *Gateway Provider Notice* on whether we should expand these clarifications, including whether we should further define what constitutes "reasonable efforts" to prevent blocking of emergency calls.[146] In light of the limited comments in the record and the uncertain benefits to be gained,[147] we do not take any further action at this time.

D. Authentication

51. To combat foreign-originated robocalls, and to further the long-standing Commission goal and benefits of ubiquitous STIR/SHAKEN authentication,[148] we require gateway providers, consistent with our proposal, to implement STIR/SHAKEN to authenticate SIP calls that are carrying a U.S. number in the caller ID field.[149] We conclude based on the record that authentication, as well as the additional data sent to downstream providers along with the authentication, will reduce the incentive and ability of foreign providers to send illegal robocalls into the U.S. market, as well as provide downstream intermediate and terminating providers and their call analytics partners with additional data to protect their customers, and therefore will provide a significant benefit. Attestation information will facilitate analytics and promote traceback and enforcement efforts.[150] Speeding traceback efforts is also consistent

---

[143] *See* 47 CFR § 64.1200(k).

[144] *See* T-Mobile Comments at 10; 51 State AG Reply at 9.

[145] *See* ZipDX Comments at 34.

[146] *Gateway Provider Notice* at para. 102.

[147] *See* T-Mobile Comments at 10 (opposing more detailed requirements).

[148] *See, e.g.*, *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1928, para. 144 (adopting the requirement giving gateway providers the option to authenticate unauthenticated calls because "of the potential value of more ubiquitous authentication").

[149] *Gateway Provider Notice* at para. 38.

[150] *See, e.g.*, *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1926, para. 141; Enterprise Communications Advocacy Coalition Comments at 7 (agreeing with Commission on this point); iBasis Comments at 5-6 (opposing an authentication obligation, but acknowledging that it would assist in traceback efforts); INCOMPAS Comments at 7 (same); T-Mobile Comments at 7 (same); Letter from David Frankel, CEO, ZipDX, to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59, WC Docket No. 17-97, at 2 (filed May 9, 2022) (ZipDX May 9 *Ex Parte*) ("As terminating endpoints identify illegal calls…those signatures effectively give us instant tracebacks without doing traceback[,] enable[ing] immediate engagement with the gateway provider(s) to promptly investigate and take necessary action."); CEPT Electronics Communications Committee, Draft ECC Report 338, CLI Spoofing at 19 (2021), https://www.cept.org/files/9522/Draft%20ECC%20Report%20338.docx (last visited Apr. 27, 2022) (ECC Draft Report 338) ("Gateway attestation is useful for trace-back purposes since the 'origid' would point to the originating node or trunk."). *But see* USTelecom Comments at 11 (arguing that traceback is already sufficiently rapid); Verizon Reply at 15 (arguing that only some analytics providers use the origid and that the impact on traceback would be limited); Letter from Steven Augustino, Counsel, Transaction Network Services, to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59, WC Docket No. 17-97, at 2-4 (TNS May 11 *Ex*

(continued….)

with the underlying goal of our 24-hour traceback requirement.[151] We find those benefits outweigh the implementation costs. Additionally, certain commenters support requiring gateway providers to authenticate calls.[152]

52. As the Commission has previously explained, application of caller ID authentication by intermediate—including gateway—providers "will provide significant benefits in facilitating analytics, blocking, and traceback by offering all parties in the call ecosystem more information."[153] At the time the Commission reached this conclusion, given the concerns that an authentication requirement on all intermediate providers "was unduly burdensome in some cases," the Commission determined that intermediate providers could, instead of authenticating unauthenticated calls, "register and participate with the industry traceback consortium as an alternative means of complying with our rules."[154] Since that time, the Commission imposed on all domestic providers the requirement to respond to all traceback requests from the Commission, law enforcement, or the industry traceback consortium, fully and in a timely manner.[155] Because evidence shows that foreign-originated robocalls are a significant and increasing problem and that the benefits of a gateway authentication requirement outweigh the burdens, we thus adopt a gateway provider authentication obligation to address this problem. We believe gateway provider authentication will address a significant risk to American consumers and enhance their trust in this country's telecommunications network.

53. *Requirement.* To comply with the requirement to authenticate calls, consistent with our proposal, a gateway provider must authenticate caller ID information for all SIP calls it receives for which the caller ID information has not been authenticated and which it will exchange with another provider as a SIP call.[156] A gateway provider can satisfy its authentication requirement if it adheres to the three ATIS standards that are the foundation of STIR/SHAKEN—ATIS-1000074, ATIS-1000080, and ATIS-1000084—and all documents referenced therein.[157] Compliance with the most current versions of these standards as of the compliance deadline, including any errata to the standards as of that date or earlier,

---

Parte) (arguing that, in the near term, primarily C-level attestation from gateway providers will harm the ability of analytics providers and others to rely on attestation generally); Letter from Josh Bercu, Vice President, Policy & Advocacy, USTelecom, to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59, WC Docket No. 17-97, at 2 (USTelecom May 6 *Ex Parte*) (arguing that traceback benefits of gateway authentication have been "thoroughly disputed in the record").

[151] *See infra* Section III.E.1.

[152] *See, e.g.,* Comcast Comments at 4-5; INCOMPAS Comments at 7; T-Mobile Comments at 3; 51 State AGs Reply at 2; Enterprise Communications Advocacy Coalition Reply at 7. *But see* AB Handshake Comments at 4 (opposing gateway provider authentication obligations); Belgacom International Carrier Services Comments at 3 (same); CTIA Comments at 14 (same); i3forum Comments at 4 (same); iBasis Comments at 5-6 (same); SipNav Comments at 1-2; USTelecom Comments at 9-10 (same); Verizon Reply at 13-14 (same); TNS May 11 *Ex Parte* (same).

[153] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1928, para. 144.

[154] *Id*. at 1927, para. 144; 47 CFR § 64.6302(b).

[155] *Fourth Call Blocking Order*, 35 FCC Rcd at 15227-29, paras. 15-21.

[156] *See* 47 CFR § 64.6302(b); *Gateway Provider Notice* at para. 43. As noted, the call blocking rules have mooted this choice—all domestic providers now must cooperate with traceback efforts. 47 CFR § 64.1200(n)(1).

[157] *First Caller ID Authentication Report and Order and Further Notice*, 36 FCC Rcd at 3258, para. 36; *see also Gateway Provider Notice* at para. 44; Comcast Comments at 6 (agreeing that "gateway providers use the ATIS-1000074, ATIS-1000080, and ATIS-1000084 standards for this purpose" and "these standards are correct and appropriate for the Commission's envisioned use").

[157] *First Caller ID Authentication Report and Order and Further Notice*, 36 FCC Rcd at 3258-59, para. 36.

represents the minimum requirement to satisfy our rules.[158] ATIS and the SIP Forum conceptualized ATIS-1000074 as "provid[ing] a baseline that can evolve over time, incorporating more comprehensive functionality and a broader scope in a backward compatible and forward looking manner."[159] We intend for our rules to provide this same room for innovation, while maintaining an effective caller ID authentication ecosystem. Gateway providers may incorporate any improvements to these standards or additional standards into their respective STIR/SHAKEN authentication frameworks, so long as any changes or additions maintain the baseline call authentication functionality exemplified by ATIS-1000074, ATIS-1000080, and ATIS-1000084.

54. In addition, in line with the rule applicable to intermediate providers generally and the Commission's proposal, gateway providers have the flexibility in implementing call authentication to assign the level of attestation appropriate to the call based on the call information available to the gateway provider.[160] Gateway providers are not limited to assigning "gateway" (C-level) attestation, and one commenter notes that there are significant benefits to be gained from gateway providers appropriately applying higher attestation levels consistent with the standard.[161] Stakeholders support this approach.[162]

55. *Benefits Outweigh Burdens.* We conclude that the benefits of a gateway provider authentication obligation outweigh the burdens. Record evidence demonstrates that the benefits of gateway provider authentication are significant[163] and are likely to grow over time as more providers are brought within the STIR/SHAKEN regime.[164] Illegal robocalls cost Americans billions of dollars each year.[165] Even minimal deterrence arising from authenticating unauthenticated foreign-originated calls is likely to be highly beneficial.[166] To the extent "gateway providers already exchange traffic in SIP and

[158] *Id*. No commenters addressed this proposal.

[159] *Id*. (internal citations omitted).

[160] *Gateway Provider Notice* at para. 45 (proposing a flexible approach consistent with the rule applicable to intermediate providers); *see also Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1926-27, paras. 142-43 (adopting rule for intermediate providers).

[161] *See* i3forum Comments at 5 (noting that higher attestation levels provide "confidence to trust the validity of the calling identity").

[162] *See* Comcast Comments at 6 ("The Commission also is correct in declining to predetermine the attestation level that gateway providers may assign to a given call. . . . There is no reason to prohibit providers from assigning higher levels of attestation where they possess the information and confidence necessary to do so."); iconnectiv Comments at 2 ("A gateway provider who has established reliable mechanisms with their upstream partners that clearly indicate which traffic is attestation level A, B or C should be permitted to transmit that [information] downstream in order to be available to the terminating provider.").

[163] *See* INCOMPAS Comments at 7; T-Mobile Comments at 3; 51 State AGs Reply at 5-6; Enterprise Communications Advocacy Coalition Reply at 6; T-Mobile Feb. 2 *Ex Parte* at 2.

[164] *See* North American Numbering Council, Call Authentication Trust Anchor Working Group, Best Practices for Terminating Voice Service Providers using, Caller ID Authentication Information at 6 (Feb. 9, 2022), http://nanc-chair.org/docs/CATA_Report_Best_Practices_for_Terminating_VSPs_using_Caller_ID_Authentication_Information_Feb_2022.pdf (2022 NANC CATA Best Practices Report); INCOMPAS Comments at 7-8; 51 State AGs Reply at 4; T-Mobile Feb. 2 *Ex Parte* at 4; TNS May 11 *Ex Parte* at 2 (while opposing a gateway provider attestation obligation, acknowledging that "over the long term, the call attestation framework will be able to absorb and process such different attestation levels").

[165] *See Gateway Provider Notice* at para. 4; ZipDX Comments at 36-37; NCLC and EPIC Reply at 3 (millions per month).

[166] *First Caller ID Authentication Report and Order*, 35 FCC Rcd at 3263, paras. 47-48; Enterprise Communications Advocacy Coalition Comments at 7; T-Mobile Comments at 3.

therefore likely are ready to implement STIR/SHAKEN,"[167] the requirement will have a real, near-term benefit.

56. Those commenters asserting such a requirement will cost significant time and resources to implement[168] do not provide detailed support for their claims.[169] Indeed, to the extent a gateway provider also serves as a voice service provider, it will have already implemented STIR/SHAKEN in at least some portion of its network, likely lowering its compliance costs to meet the requirement we adopt today.[170] Given the real and significant benefits to providers and American consumers in the form of billions in savings and increased trust in the voice network that will flow from the reduction in foreign-originated illegal robocalls, we conclude that requiring authentication is in the public interest even if we credit those arguing that there are substantial implementation costs.

57. While gateway providers are likely to authenticate most calls with only C-level attestation at least initially, we disagree with those commenters who argue that the benefits of lower attestation levels, along with other information sent along with the attestation, are not worth the asserted cost.[171] While "C-level attestation is not as good as higher-level attestation . . . it is far more valuable, particularly in the case of foreign-originated illegal robocalls, than NO signature."[172] Terminating providers and their end users directly benefit from gateway provider authentication. As T-Mobile notes, "[r]eceiving *any* level of attestation can help carriers trace where unwanted or illegal calls enter the country so they can follow up and prevent additional traffic from the offending source.[173] The information passed along with the attestation can be valuable for analytics engines, enabling calls to be appropriately labeled or sent to voice mail" before reaching end users.[174] Indeed, the NANC recently

---

[167] Comcast Comments at 6.

[168] *See* USTelecom Reply at 8 (arguing that a gateway provider STIR/SHAKEN requirement would "fail any reasonable cost-benefit analysis"); Verizon Reply at 20 (arguing that requiring it to implement gateway provider authentication would "take multiple years and cost tens of millions of dollars" and that most calls would only be authenticated with "C-level" attestation); Letter from Joshua M. Bercu, Vice President, Policy & Advocacy, USTelecom, to Marlene Dortch, Secretary, FCC, CG Docket No. 17-59, WC Docket No. 17-97, at 1 (filed Mar. 3 2022) (USTelecom Mar. 3 *Ex Parte*); USTelecom May 6 *Ex Parte* at 1-2 (same); TNS May 11 *Ex Parte* at 3 (agreeing with Verizon's cost estimates and arguing that terminating providers will incur costs as well).

[169] *See* T-Mobile Feb. 2 *Ex Parte* at 4.

[170] *See* 51 State AGs Reply at 5.

[171] *See* i3forum Comments at 4 ("[G]ateway providers, which are several steps removed from the call originator, rarely have the ability to discern the identity of the call originator or to evaluate whether the calling number is legitimate."); iBasis Reply at 2-3; USTelecom May 6 *Ex Parte* at 2-3 (arguing that C-level attestations provide little benefit and gateway provider authentication will require significant time and money to implement); Letter from Stacey Hartman, Vice President, Public Policy and Compliance, Lumen, to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59, WC Docket No. 17-97, at 3 (filed May 12, 2022) (Lumen May 12 *Ex Parte*) (same).

[172] ZipDX May 9 *Ex Parte* at 2.

[173] T-Mobile Feb. 2 *Ex Parte* at 4; *see also Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1928, para. 144 ("We find that attestation of previously unauthenticated calls [even at lower levels of attestation by intermediate providers] will provide significant benefits in facilitating analytics, blocking and traceback by offering all parties in the call ecosystem more information.").

[174] T-Mobile Feb. 2 *Ex Parte* at 2; *see also* iBasis Comments at 5-6 (opposing attestation requirements but noting that it "may aid in more quickly identifying the signing provider and thus facilitate traceback efforts"); T-Mobile Comments at 3 (asserting "as a terminating provider, it is valuable to T-Mobile to receive the STIR/SHAKEN information that gateway providers are currently not required to provide"); Enterprise Communications Advocacy Coalition Reply at 7 (arguing that commenters are "wrong" to argue that "C-level attestation by gateway providers is not worthwhile" and asserting that C-level attestation is "valuable for traceback efforts" and "identify[ing] where potentially bad traffic is entering U.S. networks"); *cf*. ZipDX Comments at 18 (arguing that, for authentication to

(continued….)

recognized the value of this information.[175] Even if not all analytics providers currently use this information,[176] more could readily do so in the future.[177] And, while we agree with commenters that gateway provider authentication is not a "silver bullet," it "will have a significant impact on curtailing illegal robocalls which is critical to restoring trust in the voice network."[178] It also will make the traceback process more efficient and rapid,[179] consistent with the underlying goal of our newly adopted 24-hour traceback requirement.[180] Even if foreign-originated calls carrying U.S. numbers constitute a small portion of gateway providers' overall traffic,[181] such traffic represents a disproportionate share of illegal robocall traffic received by such providers,[182] underscoring the importance of authentication. We agree with USTelecom that our authentication regime would be harmed if gateway providers improperly sign calls with A-level attestations,[183] but that is not a problem unique to gateway provider authentication—all domestic providers authenticating calls are obligated to provide the appropriate attestation level.[184] Similarly, we disagree with Verizon that because some gateway providers still have

---

deter illegal robocalling, "it has to be more ubiquitous, and the authentication information has to be incorporated systemically into scaled mitigation practices"). *But see* Belgacom International Carrier Services Comments at 3 (arguing that C-level gateway attestation does not provide any benefits); i3forum Comments at 5 (asserting that C-level attestation "fails to provide any useful or meaningful assistance for blocking illegal robocalls"); USTelecom Comments at 11 (arguing that C-level attestation will not provide benefits for traceback).

[175] *See* 2022 NANC CATA Best Practices Report at 6-7; *see also Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1928, para. 144.

[176] *See* Verizon Reply at 14-16.

[177] YouMail Comments at 7 (noting that it is continually improving its analytics based on the information it gathers); 2022 NANC CATA Best Practices Report at 7 ("Typical anti-robocalling analytics products can provide call labeling, support blocking, and generate reports. It is not difficult to imagine that call analytics integrated with input from SHAKEN informational elements could identify the Subject and the Issuer of certificates associated with illegal robocall campaigns."). *But see* USTelecom May 6 *Ex Parte* at 2 (arguing that the "Draft Order relies on the unproven notion that 'more' analytics providers '*could*' use C-level attestations in the future") (emphasis in original).

[178] INCOMPAS Comments at 7; *see id*. at 7-8 ("Broad adoption of the STIR/SHAKEN framework will arm consumers with the knowledge they need to make informed choices about which calls to accept while simultaneously equipping voice service providers with the information to make responsible and non-discriminatory call blocking decisions."); Comcast Comments at 4-5 ("While call authentication may not be a panacea, it is a critical step in reestablishing Americans' trust in the telephone system."); 51 State AGs Reply at 4 ("[U]niversal implementation of STIR/SHAKEN by all voice service providers in the call path is an important step that will provide increased protection for consumers against illegal spoofing.").

[179] 2022 NANC CATA Best Practices Report at 7 (noting that information sent along with the authentication allows the traceback process to quickly identify who signed the call, regardless of the attestation level).

[180] *See infra* Section III.E.1.

[181] *See, e.g.*, iBasis Comments at 6.

[182] *See* AB Handshake Comments at 1; Belgacom International Carrier Services Comments at 2; Twilio Comments at 2; YouMail Comments at 2-3; Enterprise Communications Advocacy Coalition Reply at 1; NCTA Reply at 1.

[183] *See* USTelecom Comments at 11 n.21; *see also* TNS May 11 *Ex Parte* at 4 (arguing that providers are signing calls with A-level attestation "inconsistent with ATIS standards" and raising concerns that the same problems could arise if gateway providers sign calls).

[184] *See* ATIS-1000088, A Framework for SHAKEN Attestation and origination Identifier, Section 5.4 (defining what information is necessary to provide A, B and, C attestations), https://access.atis.org/apps/group_public/download.php/51435/ATIS-1000088,%20A%20Framework%20for%20SHAKEN%20Attestation%20and%20Origination%20Identifier.pdf (last visited Apr. 27, 2022); STI Governance Authority, STI-GA Policy Decisions Binder, Version, 3.2 at 72 (Oct. 29, (continued….)

some TDM facilities, which fall "out of the scope" of the attestation mandate, we should not require gateway providers to authenticate SIP calls.[185] The Commission continuously has required voice service providers to implement authentication on the IP portions of their networks, as we do for gateway providers today, despite the presence of TDM facilities on their networks subject to a continuing extension.[186]

58. Expanding the scope of providers subject to the STIR/SHAKEN regime will increase the overall benefits of the standard and its future reach. As many parties and the NANC note, STIR/SHAKEN has beneficial network effects, and the more steps we take to increase its use, the greater the overall benefit for those providers that have already implemented the standard and those providers' customers.[187] Indeed, our expansion of the STIR/SHAKEN regime today may spur other countries and regulators to also develop and adopt STIR/SHAKEN, further increasing the standards' benefit.[188] In the interim, gateway provider authentication is the only way to ensure that all foreign-originated calls with U.S. numbers in the caller ID field are authenticated. We acknowledge that at least some of the benefits that will flow from gateway provider authentication are based on our reasoned predictions arising from disputed record evidence.[189] Nevertheless, in adopting our rule, we are persuaded by the available evidence that the benefits will be significant, and the sooner we act, the sooner the public will obtain these benefits.[190] For these reasons, we disagree with CTIA that it would be "premature" for the Commission to

---

2021) (noting that a provider's token can be revoked if it violates its agreement "not to sign any telephone calls that do not meet the levels of attestation in the relevant ATIS SHAKEN Specifications").

[185] *See* Christopher D. Oatway, Associate General Counsel, Federal Regulatory and Legislative Affairs, Verizon, to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59, WC Docket No. 17-97, at 3-4 n.12 (filed May 11, 2022) (Verizon May 11 *Ex Parte*).

[186] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1893, para. 67 (interpreting the TRACED Act to require an extension only for "those portions of a voice service provider's network that rely on technology that cannot initiate, maintain, and terminate SIP calls"); *id*. at 1881, n.167 (requiring small voice service providers to implement STIR/SHAKEN notwithstanding IP-interconnection issues raised by commenters).

[187] *See* 2022 NANC CATA Best Practices Report at 6 (describing how the value of information sent along with attestation will increase as STIR/SHAKEN deployment spreads); INCOMPAS Comments at 7-8; 51 State AGs Reply at 4; T-Mobile Feb. 2 *Ex Parte* at 4 ("[A]s T-Mobile has pointed out in the past, the greater the number of providers that employ STIR/SHAKEN, the better for the entire calling ecosystem."); ZipDX May 9 *Ex Parte* at 2 (asserting that "SHAKEN will become increasingly useful as it gets more broadly deployed"). For the same reasons, we do not adopt USTelecom's alternative proposal to only impose a gateway provider authentication obligation on smaller, non-facilities-based providers. *See* USTelecom Mar. 3 *Ex Parte* at 3-4 (supporting acting now with respect to small, non-facilities-based providers or seeking further comment in the FNPRM); *see also* TNS May 11 *Ex Parte* at 4 (supporting USTelecom proposal to act now against small, non-facilities-based providers); Letter from Linda S. Vandeloop, Asst. Vice Pres., Federal Regulatory, AT&T, to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59, WC Docket No. 17-97, at 2 (filed May 11, 2022) (AT&T May 11 *Ex Parte*) (same); Verizon May 11 *Ex Parte* at 5 (same).

[188] *See* ECC Draft Report 338 at 32 (noting that Europe will likely move to implement STIR/SHAKEN because of its "first mover advantage"). While the i3forum opposes an attestation obligation, it notes that cross-border adoption of STIR/SHAKEN and voluntary agreements can lead to "situations in which [the gateway provider] has access to information that would enable it to provide an A-level or B-level attestation." i3forum Comments at 5.

[189] *See* USTelecom May 6 *Ex Parte* at 2 (arguing that the claimed benefits of gateway provider authentication are "speculative"). *But see* ZipDX May 9 *Ex Parte* at 2 (disagreeing with USTelecom that "the claimed benefits of a plethora of C-level attestations are speculative").

[190] *American Family Assoc. v. FCC*, 365 F.3d 1156, 1166 (D.C. Cir. 2004) (quoting *Bechtel v. FCC*, 10 F.3d 875, 880 (D.C. Cir. 1993)) (holding that the Commission more generally has "wide latitude to make policy based on predictive judgments deriving from its general expertise"); *BellSouth Corp. v. FCC*, 162 F.3d 1215, 1221 (D.C. Cir. (continued….)

require gateway authentication while foreign regulators consider mandating STIR/SHAKEN[191] or that we should wait for the recommendations of outside third parties, or possible future rule changes, before acting.[192]

59. *Compliance Deadline*. We require that gateway providers authenticate unauthenticated foreign-originated SIP calls carrying U.S. NANP numbers by June 30, 2023, a longer period than we proposed in the *Gateway Provider Notice*.[193] One commenter supported a December 2023 deadline,[194] while others supported either a longer or shorter deadline.[195] We conclude that this deadline appropriately balances the relevant burdens and benefits of implementation; it will give gateway providers less time than the 18 months voice service providers had to implement STIR/SHAKEN, but more time than the shorter deadline of the effective date of the order proposed by the 51 state attorneys general.[196] This deadline also coincides with the extension for STIR/SHAKEN implementation for facilities-based small voice service providers.[197]

60. We also believe that a June 30, 2023 deadline is reasonable because the industry has much more experience with implementation than when we originally required voice service providers to implement STIR/SHAKEN, there is evidence that STIR/SHAKEN implementation costs have dropped since we first adopted the requirement for voice service providers[198] and because the authentication requirement applies only to the IP portions of the gateway providers' networks. Finally, to facilitate uniformity, simplify compliance, and consistent with comments in the record, we do not adopt an earlier deadline for those providers that have, in their role as voice service providers, already implemented STIR/SHAKEN, nor do we adopt a longer deadline for certain providers or classes of provider, or a specific process for the grant of extensions or exemptions from this requirement,[199] with the exception of

---

1999) ("When . . . an agency is obliged to make policy judgments where no factual certainties exist or where facts alone do not provide the answer, our role is more limited; we require only that the agency so state and go on to identify the considerations it found persuasive.").

[191] *See* CTIA Comments at 14.

[192] *See* USTelecom May 6 *Ex Parte* at 3 (arguing that the Commission should wait for a June 15, 2022 NANC CATA report on related issues before considering broad action on gateway provider authentication); AT&T May 11 *Ex Parte* at 3 (same); Lumen May 12 *Ex Parte* at 3-4; Verizon May 11 *Ex Parte* at 5 (arguing that the Commission should wait for the NANC report and consideration of a gateway provider attestation obligation should "be part of the Commissions' follow-on work via the Further Notice of Proposed Rulemaking"); TNS May 11 *Ex Parte* at 4 (same*)*; *see also* USTelecom May 6 *Ex Parte* at 3 n.15 (arguing the Commission should wait to clarify third-party authentication practices).

[193] *Gateway Provider Notice* at para. 48.

[194] *See* Belgacom International Carrier Services Comments at 3.

[195] *See* INCOMPAS Comments at 8 (suggesting a March 1, 2023 deadline); 51 State AGs Reply at 5 (arguing that the obligation should become effective within 30 days of the publication of the order in the Federal Register); USTelecom May 6 *Ex Parte* at 2 (asserting that it would take "years" to implement gateway provider authentication).

[196] *See* 51 State AGs Reply at 5.

[197] *See Small Provider Order* at para. 1.

[198] *See* Deployment of STIR/SHAKEN by Small Voice Service Providers, NANC Call Authentication Working Group at 4 (Oct. 13, 2021) (2021 NANC CATA Report) ("In general, there are no significant barriers which prevent universal STIR/SHAKEN implementation for interconnected and non-interconnected VoIP providers (regardless of size)."), http://nanc-chair.org/docs/October_13_2021_CATA_Working_Group_Report_to_NANC.pdf.

[199] *Gateway Provider Notice* at paras. 49-50; Belgacom International Carrier Services Comments at 3 ("[W]e believe that the conditions and deadlines should be the same across the market to avoid negative discrimination of any party."); 51 State AGs Reply at 6 (urging the Commission to not adopt a waiver process). *But see* ZipDX May 9 *Ex*

(continued….)

two extensions regarding token access and non-IP networks described below.[200] As noted above, once a gateway provider has fully implemented STIR/SHAKEN, it must update its filing in the Robocall Mitigation Database.[201]

61. *Token Access.* We sought comment on whether the STI-GA's token access policy serves as a barrier for all or a subset of gateway providers from obtaining a token and, if so, what if any actions we should take to address that barrier,[202] but we received limited response.[203] We conclude that the current token access policy will likely not present a material barrier to gateway providers meeting their authentication obligation, and we anticipate that the STI-GA can address any concerns before gateway providers are required to authenticate calls by June 30, 2023. Nevertheless, to ensure that gateway providers are not unfairly penalized, we provide a STIR/SHAKEN extension to gateway providers that are unable to obtain a token due to the STI-GA token access policy. The extension will run until the gateway provider is able to obtain a token as long as the gateway provider "diligently pursues" doing so.[204]

62. *Non-IP Networks and Authentication.* We conclude that gateway providers should have the same duty as voice service providers to either upgrade their non-IP networks to IP and implement STIR/SHAKEN or work with a working group, standards group, or consortium to develop a non-IP caller ID authentication solution.[205] Such an obligation is appropriate in light of gateway providers' key role in serving as the entry point for foreign-originated voice traffic into the U.S. marketplace and the limited burden gateway providers would experience in working with a standards group. No party commented on this issue, and this approach is consistent with those commenters arguing that all domestic providers in the call path should have similar obligations.[206] As with voice service providers, gateway providers that choose to work with a working group are subject to an extension to implement STIR/SHAKEN in the non-IP portions of their networks.[207]

63. We asked in the *Gateway Provider Notice* whether we should require gateway providers to adopt a non-IP caller ID authentication solution, an obligation that voice service providers currently do

---

Parte at 1 (proposing the creation of an "exception process" where providers must show that the authentication obligation would be "unduly burdensome"). Parties are, of course, free to file a request for waiver. The Commission may grant such requests where the particular facts at issue make strict compliance with the rule at issue inconsistent with the public interest. *Northeast Cellular Tel. Co. v. FCC*, 897 F.2d 1164, 1166 (D.C. Cir. 1990). In considering whether to grant a waiver, the Commission may take into account factors such as hardship, equity, or more effective implementation of overall policy. *WAIT Radio v. FCC*, 418 F.2d 1153, 1159 (D.C. Cir. 1969).

[200] This extension will be similar to the one already in place for voice service providers. *See* 47 CFR § 64.6304(b) ("[V]oice service providers that are incapable of obtaining a SPC token due to Governance Authority policy are exempt from the requirements of § 64.6301 until they are capable of obtaining a SPC token.").

[201] *See supra* Section III.C.

[202] *Gateway Provider Notice* at para. 47.

[203] USTelecom and iconectiv assert that the policy should not be changed. *See* iconectiv Comments at 2; USTelecom Reply at 8. iBasis argues that the OCN criteria should be eliminated. *See* iBasis Reply at 3.

[204] *Cf. Caller ID Authentication Governance Framework Revised to Enable Earlier Participation by Providers Without Direct Access To Telephone Numbers*, WC Docket Nos. 13-97, 17-97, Public Notice, 36 FCC Rcd 8318, at 2 (WCB 2021) ("As a result of the Governance Authority's [token access] policy change, voice service providers that previously were unable to obtain a certificate due to lack of direct access to numbers must now diligently pursue a certificate by registering in the Robocall Mitigation Database and then seeking a certificate from the Secure Telephone Identity Certification Authority.") (internal citations omitted).

[205] *See Gateway Provider Notice* at para. 46; 47 CFR § 64.6303.

[206] *See, e.g.*, USTelecom Comments at 8; ZipDX Comments at 29; Verizon Reply at 2.

[207] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1870-75, paras. 24-35.

not have.[208] A number of commenters filed specific proposals in the record for authentication on IP and non-IP networks for gateway providers as well as voice service providers.[209] We do not adopt these proposals, in part because many are outside of the scope of the *Gateway Provider Notice.*[210] However, we seek comment on some of these alternatives in the accompanying *Further Notice*, as well as their applicability to all domestic providers in the call path, and do not foreclose the possibility of seeking comment on the remainder of these proposals in a future notice.

E. Robocall Mitigation

64. We adopt several of our robocall mitigation proposals from the *Gateway Provider Notice*. First, we adopt our proposal to require gateway providers to respond to traceback requests within 24 hours, with one modification. Second, we require gateway providers and the providers immediately downstream from the gateway provider to comply with blocking mandates in certain instances. Third, we require gateway providers to "know" the provider immediately upstream from the gateway provider. Finally, we adopt a general mitigation standard.

1. 24-Hour Traceback Requirement

65. We adopt our proposal to require gateway providers to fully respond to traceback requests from the Commission, civil and criminal law enforcement, and the industry traceback consortium within 24 hours of receipt of such a request.[211] This is an enhancement of our existing rule, which requires all domestic providers, including gateway providers, to respond to traceback requests "fully and in a timely manner."[212] We take this step recognizing the critical role that gateway providers play in stopping the deluge of illegal foreign-originated robocalls, which continue to increase despite our previous efforts to stem the tide.

66. We find that a mandatory 24-hour response requirement best serves to protect consumers from foreign-originated illegal robocalls, which are a prevalent source of illegal robocalls aimed at U.S.

---

[208] *Gateway Provider Notice* at para. 46.

[209] *See, e.g.*, AB Handshake Comments at 5 (urging the Commission to allow providers to adopt its or a similar non-IP based technology as an alternative to STIR/SHAKEN); SipNav Comments at 2 (asserting that the Commission should allow providers to examine the "media IP address" in lieu of STIR/SHAKEN authentication); TransNexus Comments at 1-2 (arguing that we should take action on the non-IP extension generally); GSMA Reply at 4 (noting that it "is currently working on a platform solution that would facilitate information sharing and analytics from around the world to identify and prevent fraudulent traffic by focusing on network identification rather than numbers"); Letter from Mitchell N. Roth, Roth Jackson Gibbons Condlin PLC, counsel to SipNav to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59, WC Docket No. 17-97, at 1-2 (filed Feb. 11, 2022).

[210] *See, e.g.*, USTelecom Reply at 9 n.29 (arguing that it would not be "appropriate for the Commission to address the non-IP extension here, as it is not directly germane to addressing foreign-originated robocalls").

[211] To be clear, the 24-hour clock does not start outside of the business hours of the local time for the responding office. Requests received outside of business hours as defined in our rules are deemed received at 8:00 a.m. on the next business day. Similarly, if the 24-hour response period would end on a non-business day, either a weekend or a federal legal holiday, the 24-hour clock does not run for the weekend or holiday in question, and restarts at 12:01 a.m. on the next business day following when the request would otherwise be due. "Business day" for these purposes is Monday through Friday, excluding federal legal holidays, and "business hours" are 8:00 a.m. to 5:30 p.m. on a business day, consistent with the definition of office hours in the Commission's rules. 47 CFR § 0.403. By way of example, a request received at 3:00 p m. on a Friday will be due at 3:00 p m. on the following Monday, assuming that Monday is not a federal legal holiday. We believe that this clarification resolves concerns raised by some parties about the burden of a strict 24-hour requirement. *See* CTIA May 10 *Ex Parte* at 3-4; Letter from Steven Morris, Vice President & Deputy General Counsel, NCTA, to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59, WC Docket No. 17-97, at 2 (filed May 11, 2022) (NCTA May 11 *Ex Parte*); INCOMPAS et al. May 6 *Ex Parte* at 3.

[212] 47 CFR § 64.1200(n)(1).

consumers.[213] As the Commission has repeatedly made clear, traceback is an essential part of both identifying and stopping illegal calls, and rapid traceback is key to its success. The process used by the Industry Traceback Group, which is the currently designated industry traceback consortium, is semi-automated, allowing the process to continue very quickly when a provider responds to a traceback request.[214] While time is always of the essence in traceback, time is particularly important in the case of foreign-originated calls. In such cases, reaching the origination point of the call may require working with foreign providers and foreign governments, which could significantly increase the total time for the traceback process. As the 51 State AGs have argued, time is of the essence for traceback of foreign-originated calls because law enforcement may need to work with international regulators to obtain information from providers outside of U.S. jurisdiction.[215] As a result, any unnecessary delay increases the risk that this essential information may become impossible to obtain.

67. We therefore disagree with commenters that do not support our enhanced 24-hour requirement.[216] First, we disagree with commenters that argue that a stricter requirement is not warranted here.[217] We acknowledge the work industry has done on improving the traceback process, and recognize that many, if not most, providers that receive traceback requests already respond in under 24 hours.[218] However, we find that it is important to act aggressively in the international calling context. The gateway provider's response to a traceback request is often the first step in a process where the entity conducting the traceback must work with multiple foreign providers to trace a call back to the originating foreign provider and caller. The longer this process takes, the higher the risk that a foreign provider will no longer have the information necessary to respond—if they are even willing to do so—or that other factors will change, reducing the ability to fully trace the call. Therefore, this process must both begin and be completed as soon as possible. Many, if not most, providers that receive traceback requests are already responding within 24 hours, and we believe this enhanced obligation presents no additional burden. For providers that do not already meet this standard, the additional burden is justified by the need to quickly obtain this information. The record does not support the contention that this requirement presents a significant burden for providers.[219] We emphasize again, as we stated in the *Fourth Call Blocking Order*, that we generally expect *all* domestic providers to respond to traceback within 24 hours in most instances.[220] The rule we adopt today simply makes that expectation a requirement in the gateway context.[221]

---

[213] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1906, para. 91.

[214] Industry Traceback Group, Policies and Procedures at 8 (2022), https://tracebacks.org/wp-content/uploads/2022/04/ITG-Policies-and-Procedures-Updated-Apr-2022.pdf.

[215] 51 State AGs Reply at 7 (*citing Fourth Call Blocking Order*, 35 FCC Rcd at 15228, n.52).

[216] *See, e.g.*, Belgacom International Carrier Services Comments at 4; CTIA Comments at 11; i3forum Comments at 8; iBasis Comments at 7-8; INCOMPAS Comments at 9-10; T-Mobile Comments at 7; ZipDX Comments at 20.

[217] *See, e.g.*, CTIA Comments at 11; INCOMPAS Comments at 9-10; T-Mobile Comments at 7; ZipDX Comments at 19-20.

[218] *See, e.g.*, Verizon Reply at 17; Industry Traceback Group, Combating Illegal Robocalls at 3 (2021), https://tracebacks.org/wp-content/uploads/2021/08/ITG-Report-Combatting-Illegal-Robocalls.pdf (ITG Robocall Report).

[219] Some commenters did raise specific concerns about this requirement. *See, e.g.*, Belgacom International Carrier Services Comments at 4; i3forum Comments at 8; iBasis Comments at 7-8. However, as discussed further below, these comments appear to either misunderstand the current expectations or to misunderstand the scope of the requirement.

[220] *Fourth Call Blocking Order*, 35 FCC Rcd at 15228, n.52.

[221] While we require response to all traceback requests within 24 hours, we retain our right to exercise discretion in enforcement or consider limited waivers where a provider that normally responds within the 24-hour time frame has (continued….)

68. We also disagree with commenters who argue that 24 hours is too short a time frame.[222] We note that, in the *Fourth Call Blocking Order*, we made clear that, in most cases, we expect responses within 24 hours under our existing rule.[223] Further, according to a report by the ITG, the average time to complete a single hop in the traceback process is less than one day, with many providers responding in less than 30 minutes.[224] Many, if not most, providers that receive traceback requests already respond in under 24 hours.[225] We therefore see no reason to believe that rule we adopt today would unduly burden any gateway providers, nor would the burden of such a requirement outweigh the significant benefits to law enforcement from such a requirement.[226]

69. We make clear that we do not require the gateway provider to identify the caller or originating provider within this 24-hour response period except in the case where the originating provider is the provider from which the gateway provider received the call. Some commenters appear concerned that this rule would require them to trace a call back to the point of origination, or, at least, through several hops.[227] One commenter points to the "need to obtain information from several other carriers located in foreign countries,"[228] while another mentions the need for "detailed investigations."[229] We require the gateway provider to respond with information only about the provider from which it directly received the call.[230]

70. We also encourage gateway providers to determine whether their relationship with upstream providers should change to better facilitate traceback.[231] We see no reason that a gateway provider should not be able to identify the immediate upstream provider from its records and respond to the traceback request without further investigation. In fact, one commenter indicated that it currently

---

an truly unexpected or unpredictable issue that leads to a delayed response in a particular case or for a short period of time.

[222] *See, e.g.*, Belgacom International Carrier Services Comments at 4; i3forum Comments at 8. One commenter incorrectly indicated that the "current deadline" is 36 hours, without indicating the source of that figure. Belgacom International Carrier Services Comments at 4.

[223] *Fourth Call Blocking Order*, 35 FCC Rcd at 15228, n.52.

[224] ITG Robocall Report at 3; ITG Mar. 29 *Ex Parte*, Attach at 3-4. While the ITG Mar. 29 *Ex Parte* notes that overall response time is reduced by certain providers responding more quickly, it also notes that "[t]racebacks that end with non-responsive providers tend to have slower response times, even in completed hops before the non-responsive provider" and that providers closer to the origination point tend to respond more slowly. ITG Mar. 29 *Ex Parte* Attach. at 6. Speeding up these responses can only benefit the traceback process.

[225] *See, e.g.*, Verizon Reply at 17; ITG Mar. 29 *Ex Parte* Attach. at 3-4; ITG Robocall Report at 3.

[226] Gateway providers for which this requirement poses a unique and significant burden may apply for a waiver of this rule under the "good cause" standard of section 1.3 of our rules. Under that standard, for example, waivers may be available in the event of sudden unforeseen circumstances that prevent compliance for a limited period or for a limited number of calls. We note that any applicant for waiver "faces a high hurdle even at the starting gate" and would need to "plead with particularity" the "special circumstances" that warrant a waiver and explain how granting a waiver would serve the public interest. *WAIT Radio v. FCC*, 418 F.2d 1153, 1159 (D.C. Cir. 1969); *see also Northeast Cellular Tel. Co. v. FCC*, 897 F.2d 1164, 1166 (D.C. Cir. 1990).

[227] *See, e.g.*, i3forum Comments at 8; iBasis Comments at 7-8.

[228] i3forum Comments at 8.

[229] iBasis Comments at 7-8.

[230] An appropriate response would include the identity of the upstream provider, as well as, for example, the country, a complete address, contact information for the provider, and a link to that provider's Robocall Mitigation Database filing. *See* ITG Mar. 29 *Ex Parte* Attach. at 15.

[231] For example, a gateway provider may conduct such an investigation as part of compliance with the "know your upstream provider" obligation discussed below, which does not have a 24-hour requirement. *See infra* Part III.E.3.

automates response to traceback.[232]

71. *Compliance Deadline.* We require gateway providers to comply with this requirement no later than 30 days after publication of notice of OMB approval under the Paperwork Reduction Act. This allows gateway providers sufficient time to update their processes and come into compliance with the rule.

2. Mandatory Blocking

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

73. We find that the mandatory blocking requirements we adopt today, along with the appropriate procedural safeguards described herein, strike an appropriate balance between the benefit of blocking calls likely to be illegal with the risk of blocking lawful calls. We acknowledge that this represents a shift, at least in part, from our previous approach of permitting, rather than mandating, blocking.[233] We agree that "[b]locking calls is a serious and complicated action that must be precisely and judiciously applied to avoid blocking lawful traffic."[234] However, we disagree with commenters that argue mandatory blocking requirements are generally inappropriate.[235] Our existing permissive blocking rules are still in effect; we encourage providers to make use of permissive blocking, where available, to protect American consumers from unwanted and illegal calls. The rules we adopt today narrowly target the most obvious foreign-originated illegal calls, including those calls that have already been determined to be illegal, and enlist gateway providers into the fight to block these calls before they enter the U.S. telephone network.

a. Blocking Following Commission Notification

74. We adopt two of our proposals from the *Gateway Provider Notice*. First, we require gateway providers to block, rather than effectively mitigate, illegal traffic when notified of such traffic by the Commission.[236] Second, we require providers immediately downstream from a gateway provider to block all traffic from the identified provider when notified by the Commission that the gateway provider failed meet its obligation to block illegal traffic.[237] To ensure that gateway providers are afforded sufficient due process prior to downstream providers blocking all traffic from them, we adopt a clear process that allows ample time for the notified gateway provider to remedy the problem and demonstrate that it can be a good actor in the calling ecosystem before the Commission directs downstream providers to begin blocking. This process, laid out in greater detail below, includes the following steps: 1) the Enforcement Bureau shall provide the gateway provider with an initial Notification of Suspected Illegal Traffic; 2) the gateway provider shall be granted time to investigate and act upon that notice; 3) if the

[232] Verizon Reply at 3.

[233] *See* CTIA Comments at 12.

[234] i3forum Comments at 6.

[235] *See, e.g.*, CTIA Comments at 12; i3forum Comments at 6; INCOMPAS Comments at 10-14; T-Mobile Comments at 5; USTelecom Comments at 12; Enterprise Communications Advocacy Coalition Reply at 3; iBasis Reply at 4; NCTA Reply at 2; USTelecom Reply at 5-6.

[236] *See Gateway Provider Notice* at paras. 57-59.

[237] *See Id*. at paras. 60-65.

gateway provider fails to respond or its response is deemed insufficient, the Enforcement Bureau shall issue an Initial Determination Order, providing a final opportunity for the gateway provider to respond and; 4) if the gateway provider fails to respond or that response is deemed insufficient, the Enforcement Bureau shall issue a Final Determination Order, directing downstream providers to block all traffic from the identified provider.

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

76. We agree with commenters that this blocking will help protect American consumers by ensuring less illegal traffic reaches their phones.[238] An affirmative obligation for gateway providers to block upon Commission notification ensures greater protection than an "effective mitigation" requirement. This is particularly true because gateway providers, by definition, are intermediate providers and are thus a step removed from the caller, limiting their available effective mitigation options.

77. We therefore disagree with commenters that urge us to rely on the existing requirement to effectively mitigate this traffic rather than to adopt this enhanced requirement.[239] We also disagree with providers that a separate set of obligations when acting as a gateway provider complicates or increases the burden of compliance because providers cannot easily determine if they are acting as a gateway provider for a particular call.[240] Here, per the process described below, the Enforcement Bureau makes the initial determination of whether the provider is acting as a gateway provider.[241] If the gateway provider is not directed to comply with 47 CFR § 64.1200(n)(5), but rather with 47 CFR § 64.1200(n)(2), then that provider will not be in violation of our rules for effectively mitigating, rather than blocking, illegal traffic, regardless of its position in the call path for a particular call.

78. *Downstream Provider Blocking When Gateway Provider Fails to Comply with Blocking Requirement.* We adopt our proposal requiring providers immediately downstream from a gateway provider to block all traffic from the identified provider when notified by the Commission that the gateway provider failed to block.[242] If the Enforcement Bureau determines a gateway provider fails to satisfy 47 CFR § 64.1200(n)(5), it shall publish and release an Initial Determination Order as described below giving the provider a final opportunity to respond to the Enforcement Bureau's initial determination. If the Enforcement Bureau determines that the identified gateway provider continues to violate its obligations, the Enforcement Bureau shall release and publish a Final Determination Order in EB Docket No. 22-174 to direct downstream providers to both block and cease accepting all traffic they receive directly from the identified gateway provider starting 30 days from the release date of the Final

[238] *See* 51 State AGs Reply at 8.

[239] *See, e.g.*, iBasis Comments at 9; T-Mobile Comments at 6.

[240] *See, e.g.*, T-Mobile Comments at 4; USTelecom Comments at 7; NCTA Reply at 2; USTelecom Reply at 2.

[241] A provider determines whether it is a "gateway provider" on a call-by-call basis. A provider may be a gateway provider for some of the calls in the identified traffic and a non-gateway originating provider, non-gateway intermediate provider, or non-gateway terminating provider for other calls in the identified traffic. If the provider is the gateway provider for any of the calls in the traffic identified in the Notification of Suspected Illegal Traffic, the provider must block all traffic that is substantially similar to the identified traffic, regardless of whether the provider is a gateway provider for any particular call.

[242] *See Gateway Provider Notice* at paras. 60-65; 47 CFR § 64.1200(n)(5).

Determination Order.[243]

79. We agree with several commenters that support this requirement[244] and disagree with the lone commenter that objects to this mandate.[245] We find that this requirement is an appropriate and proportional response where a gateway provider actively and willfully refuses to be a good actor in the calling ecosystem. Blocking all traffic from a particular provider is a dramatic step that will likely also block some lawful traffic[246] but is justified by the need to protect consumers from foreign-originated illegal robocalls. Lawful traffic can then be routed through other gateway providers that comply with the Commission's rules.

80. *Process for Issuing a Notification of Suspected Illegal Traffic*. The Enforcement Bureau shall make an initial determination that the provider is a gateway provider for suspected illegal traffic and notify the provider by issuing a written Notification of Suspected Illegal Traffic. The Notification of Suspected Illegal Traffic shall: (1) identify with as much particularity as possible the suspected illegal traffic; (2) provide the basis for the Enforcement Bureau's reasonable belief that the identified traffic is unlawful;[247] (3) cite the statutory or regulatory provisions the suspected illegal traffic appears to violate; and (4) direct the provider receiving the notice that it must comply with section 64.1200(n)(5) of the Commission's rules.

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

82. We make clear that the requirement to block on an ongoing basis is not tied to the number in the caller ID field or any other single criterion. Instead, we require the identified provider to block on a continuing basis any traffic that is substantially similar to the identified traffic and provide the Enforcement Bureau with a plan as to how it expects to do so. We do not define "substantially similar traffic" in any detail here because that will be a case-specific determination based on the traffic at issue. We decline to limit the scope of "substantially similar traffic" to only "traffic sent by the upstream entity that was responsible for sending the illegal robocall traffic that triggered the Commission's notification."[248] While gateway providers may propose such a limitation in the blocking plan they submit to the Enforcement Bureau, we do not find that such a limitation is appropriate in all instances. In particular, such a limitation could make it easy for a bad actor to circumvent blocking by simply routing their traffic through multiple upstream providers. We are also concerned that a detailed definition could allow bad actors to circumvent this blocking by providing a roadmap as to how to avoid detection. Additionally, we note that each calling campaign will have unique qualities that are better addressed on a case-by-case basis, where the analytics used can be tailored to the particular campaign at issue. We nevertheless encourage gateway providers to consider common indicia of illegal calls such as call duration; call completion ratios; large bursts of calls in a short time frame; neighbor spoofing patterns;

---

[243] Ignorance of a Final Determination Order's release is not sufficient reason for a downstream provider to fail to block all traffic from the gateway provider unless such Order is not posted in EB 22-174.

[244] *See, e.g.*, Comcast Comments at 8; ZipDX Comments at 23; 51 State AGs Reply at 9; NCLC and EPIC Reply at 7.

[245] iBasis Comments at 9-10.

[246] *See* Comcast Comments at 8 ("[T]he Commission should account for the fact that blocking all traffic from such a gateway provider could result in the blocking of some domestic and otherwise lawful traffic.").

[247] The notice should include any relevant nonconfidential evidence from credible sources such as the industry traceback consortium or law enforcement agencies.

[248] CCA May 11 *Ex Parte* at 2.

and sequential dialing patterns. We make clear that these are not the only criteria that the gateway provider may consider in developing its plan, and that not all criteria may be relevant in all situations. Gateway providers will have flexibility to determine the correct approach for each particular case, but a gateway provider must provide a detailed plan in its response to the Enforcement Bureau so that the Bureau can assess the plan's sufficiency. If the Enforcement Bureau determines that the plan is insufficient, it shall provide the gateway provider an opportunity to remedy the deficiencies prior to taking further action. We will consider the identified provider to be in compliance with our mandatory blocking rule if it blocks traffic in accordance with its approved plan. However, we make clear that the Enforcement Bureau may require the identified provider to modify its approved plan if it determines that the identified provider is not blocking substantially similar traffic. Additionally, if the Enforcement Bureau finds, based on the evidence, that the identified provider continues to allow suspected illegal traffic onto the U.S. network, it may proceed to an Initial Determination Order or Final Determination Order, as appropriate. Finally, we adopt a limited safe harbor from liability under the Communications Act or our rules for gateway providers that inadvertently block lawful traffic as part of the requirement to block substantially similar traffic in accordance with the gateway provider's approved plan.[249] While we agree that a safe harbor for inadvertent over-blocking is warranted, we decline to provide a safe harbor for under-blocking within this rule. A gateway provider that is under-blocking and not fully cooperating with the Enforcement Bureau to address the issue should not be granted protection from liability under the very rule with which it fails to comply.

83. *Gateway Provider Investigation.* Each notified provider must investigate the identified traffic and report the results of its investigation to the Enforcement Bureau in the timeframe specified in the Notification of Suspected Illegal Traffic. If the provider's investigation determines that it served as the gateway provider for the identified traffic, it must block the identified traffic within the timeframe specified in the Notification of Suspected Illegal Traffic (unless its investigation determines that the traffic is not illegal) and include in its report to the Enforcement Bureau: (1) a certification that it is blocking the identified traffic and will continue to do so; and (2) a description of its plan to identify and block substantially similar traffic on an ongoing basis. If the provider's investigation determines that the identified traffic is not illegal, it shall provide an explanation as to why the provider reasonably concluded that the identified traffic is not illegal and what steps it took to reach that conclusion. Absent such a showing, or the Enforcement Bureau determines based on the evidence that the traffic is illegal despite the provider's assertions, the identified traffic will be deemed illegal. If a provider's investigation determines it did not serve as a gateway provider for any of the identified traffic, its report shall provide an explanation as to how it reached that conclusion and, if it is a non-gateway intermediate or terminating provider for the identified traffic, the provider must identify the upstream provider(s) from which it received the identified traffic and, if possible, take lawful steps to mitigate this traffic.[250] If the notified provider determines that it is the originating provider for the identified traffic, or the traffic otherwise comes from a source that does not have direct access to the U.S. public switched telephone network, the notified provider must comply with 47 CFR § 64.1200(n)(2) by effectively mitigating the identified traffic and report to the Enforcement Bureau any steps the provider has taken to effectively mitigate the identified traffic. If the gateway provider determines that the traffic is not illegal, it must inform the Enforcement Bureau and explain its conclusion within the specified timeframe.

84. *Process for Issuing an Initial Determination Order*. If the gateway provider fails to respond to the notice within the specified timeframe, the Enforcement Bureau determines that the response is insufficient, the Enforcement Bureau determines that the gateway provider is continuing to allow substantially similar traffic onto the U.S. network, or the Enforcement Bureau determines based on

[249] CCA May 11 *Ex Parte* at 3 (seeking a safe harbor when blocking substantially similar traffic); *see also* CTIA May 10 *Ex Parte* at 1-2 (seeking a safe harbor consistent with the blocking mandates).

[250] Such steps could include, for example, enforcing contract terms, or blocking the calls from bad actor providers consistent with the safe harbor found in 47 CFR § 64.1200(k)(4).

the evidence that the traffic is illegal despite the provider's assertions, the Enforcement Bureau shall issue an Initial Determination Order to the gateway provider stating its determination that the gateway provider is not in compliance with 47 CFR § 64.1200(n)(5). This Initial Determination Order must include the Enforcement Bureau's reasoning for its determination and give the gateway provider a minimum of 14 days to provide a final response prior to the Enforcement Bureau's final determination as to whether the gateway provider is in compliance with 47 CFR § 64.1200(n)(5).

85. *Process for Issuing a Final Determination Order.* If the gateway provider does not provide an adequate response to the Initial Determination Order or continues to allow substantially similar traffic onto the U.S. network, or the Enforcement Bureau determines based on the evidence that the traffic is illegal despite the provider's assertions, the Enforcement Bureau shall issue a Final Determination Order. The Enforcement Bureau shall publish the Final Determination Order in EB Docket No. 22-174 to direct downstream providers to both block and cease accepting all traffic they receive directly from the identified gateway provider starting 14 days from the release date of the Final Determination Order. This Final Determination Order may be adopted up to one year after the release date of the Initial Determination Order and may be based on either an immediate failure to comply with 47 CFR § 64.1200(n)(5) or a determination that the gateway provider has failed to meet its ongoing obligation to block substantially similar traffic under that rule.

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

b. Do-Not-Originate

87. We further require gateway providers to block calls based on a reasonable DNO list.[251] A "DNO list" is a list of numbers that should never be used to originate calls, and therefore any calls that include a listed number in the caller ID field can be blocked. We decline to mandate the use of a specific list, but allow gateway providers to use any DNO list so long as the list is reasonable. We decline to mandate the use of a specific list, but gateway providers must use at least one DNO list, so long as the list is reasonable. Such a list may include only invalid, unallocated, and unused numbers, as well as numbers for which the subscriber to the number has requested blocking.[252]

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

89. In the *2017 Call Blocking Order,* we specifically found that, where the subscriber to the originating number requests blocking, calls purporting to be from that number are "highly likely to be illegal and to violate the Commission's anti-spoofing rule, with the potential to cause harm defraud, or wrongfully obtain something of value."[253] Spoofing of this sort is particularly damaging as it can be used to foster consumer trust and bolster imposter scams. Therefore, we find that a reasonable list would need to include, at a minimum, any inbound-only government numbers where the government entity has requested the number be included. It must additionally include private inbound-only numbers that have

[251] *Gateway Provider Notice* at paras. 71-73.

[252] 47 CFR § 64.1200(k)(1), (2)(i)-(iii); *2017 Call Blocking Order*, 32 FCC Rcd at 9709-21, paras. 9-40.

[253] *2017 Call Blocking Order*, 32 FCC Rcd at 9710, para. 10.

been used in imposter scams, when a request is made by the private entity assigned such a number.[254] In either scenario, the provider or the third party that manages the DNO list may impose reasonable requirements on including the numbers, such as requiring that the number is currently being spoofed at a substantial volume.[255] Gateway providers, or those managing such a list on behalf of gateway providers, should ensure that entities can reasonably request inclusion on the list.

90. We agree with commenters that support a DNO mandate.[256] We further agree with one commenter that urged the Commission to look to existing DNO lists for this purpose.[257] While we do not endorse a specific list, we encourage industry to either make use of existing tools or develop new ones to serve this purpose. Gateway providers may choose the list that works best for their networks so long as that list is reasonable. Because we find that a single, centralized list is not the correct approach, we decline to develop a "high availability application or online tool" as one commenter suggests.[258] We are concerned that a centralized list could present security concerns and allow bad actors to circumvent blocking by providing a clear list of numbers to avoid spoofing.[259]

91. We disagree with the commenter that argued the mandate is unnecessary because many providers already use a DNO list to block calls.[260] We recognize that providers have used DNO lists to reduce the number of illegal calls that reach consumers, and we applaud these industry efforts.[261] We find that enlisting all gateway providers in this effort will further reduce the risk of illegal calls reaching consumers. There is no legitimate reason for the caller to use numbers that appear on a DNO list. Therefore, these calls, if they reach even a single consumer, cause harm. We also decline to deem gateway providers in compliance with this requirement if they have implemented a reasonable DNO in some parts of their network but not at the gateway.[262] The intent of this rule is to stop foreign-originated illegal calls from entering the U.S. network at all. If these calls are not stopped at the gateway, there is a risk that they will not be blocked at all and will therefore reach consumers.

c. No Analytics-Based Blocking Mandate

92. We decline at this time to require gateway providers to block calls that are highly likely to be illegal based on reasonable analytics.[263] We agree with commenters' concerns regarding mandating

---

[254] The current list maintained by the Industry Traceback Group is reasonable. We decline, however, to deem that list "presumptively reasonable" as NCTA suggests. NCTA May 11 *Ex Parte* at 1-2. While we agree that the list, as it currently stands "would advance the Commission's goal of reducing harmful spoofing and imposter scams," we are concerned that deeming it "presumptively reasonable" does not account for the fact that the list is not under Commission control and could be modified, or no longer updated, at any time without Commission input. *Id.*

[255] Multiple parties requested this or a similar clarification, to address concerns that some switches may have limits on the total amount of numbers that can be blocked. *See* CTIA May 10 *Ex Parte* at 2-3; INCOMPAS et al. May 6 *Ex Parte* at 1-2; Lumen May 12 *Ex Parte* at 2-3.

[256] *See, e.g.*, Somos Comments at 1-4; 51 State AGs Reply at 10; Enterprise Communications Advocacy Coalition Reply at 5.

[257] Somos Comments at 1.

[258] *See* Belgacom International Carrier Services Comments at 5.

[259] In some instances, there is still value in a DNO list even when bad actors know what numbers are included. For example, consumer trust may increase when the caller cannot spoof a known number associated with the caller the bad actor is attempting to impersonate. A non-public list, at a minimum, slows bad actors in their efforts to switch numbers and prevents some calls from reaching consumers.

[260] *See* USTelecom Comments 12-14.

[261] *See Id*.

[262] *See* CTIA May 11 *Ex Parte* at 3; Lumen May 12 *Ex Parte* at 2; INCOMPAS et al. May 6 *Ex Parte* at 2.

[263] *Gateway Provider Notice* at paras. 66-70.

such blocking.[264] Additionally, we find that many of the arguments against mandatory blocking generally, while not persuasive in the context of other rules we adopt today, are persuasive in this context.[265] An analytics-based blocking mandate would require us to more strictly define "reasonable analytics" in order for gateway providers to be certain that they are in compliance with a mandatory blocking rule.[266] To do so may be counter-productive and prevent providers from responding to evolving threats.[267] We are also concerned that providing a strict definition, while certainly valuable to lawful callers, could potentially provide a road map bad actors could use to circumvent blocking.[268] These concerns, coupled with the need for truly robust redress mechanisms for callers when the blocking is not initiated by the consumer and therefore cannot be corrected by the consumer, support our decision not to require such blocking at this time.[269]

d. No Blocking Safe Harbor

93. Except as described above, we decline to adopt a safe harbor for providers that block consistent with the rules we adopt today.[270] Several comments addressing safe harbors focused on blocking based on reasonable analytics, and in some cases on extending our existing safe harbor instead of mandating blocking.[271] We do not adopt a reasonable analytics blocking mandate, and extending the existing safe harbor is outside of the scope of this *Order*. Other comments did support a safe harbor more

[264] *See, e.g.*, i3forum Comments at 7; iBasis Comments at 10; T-Mobile Comments at 5; Enterprise Communications Advocacy Coalition Reply at 4.

[265] *See, e.g.*, CTIA Comments at 12 ("The Commission should not deviate from this carefully crafted and long-standing approach for permissive blocking of illegal robocalls, as doing so would upend the Commission's careful balance and would have serious call completion implications for legitimate calls that originate outside of the United States."); i3forum Comments at 6 ("Blocking calls is a serious and complicated action that must be precisely and judiciously applied to avoid blocking lawful traffic. The risk of over-blocking must be minimized to prevent unintentional harm and serious consequences that can result if lawful calls relaying emergency or urgent information erroneously are blocked."); INCOMPAS Comments at 10-14 (objecting to mandatory blocking and raising concerns about transparency and redress); Enterprise Communications Advocacy Coalition Reply at 3 ("Other than blocking unallocated, unassigned, and invalid numbers, subjective blocking should be done by terminating carriers with customer consent and opt-in. Implementing a blocking requirement for gateway providers in the middle of a call path without clear objective criteria and a means for call originators to know who blocked calls and a redress for unjustified blocking is a major obstacle for legal call originators."); Voice on the Net Reply at 3 ("[T]he Commission should not mandate any additional blocking requirements until the analytics and the redress process have been adequately tested to ensure lawful calls will be completed").

[266] *See, e.g.*, Belgacom International Carrier Services Comments at 5; iBasis Comments at 11; Twilio Comments at 6; Enterprise Communications Advocacy Coalition Reply at 6.

[267] *See, e.g.*, TNS Comments at 5-6; YouMail Reply at 5.

[268] *See, e.g.*, Belgacom International Carrier Services Comments at 5; iBasis Comments at 11; Twilio Comments at 6; Enterprise Communications Advocacy Coalition Reply at 6.

[269] Several commenters, while objecting to a blocking mandate, urged us to extend our safe harbor for blocking based on reasonable analytics to all providers in the call path, either in conjunction with a mandate or as an alternative. *See, e.g.*, Comcast Comments at 8-9; i3forum Comments at 7; INCOMPAS Comments at 12-13; T-Mobile Comments at 6; TNS Comments at 1, 3-5; iBasis Reply at 4-5; NCTA Reply at 1-2. Because we do not adopt such a mandate, we decline to reach the question of whether a safe harbor would be a necessary part of such a requirement. At this time, we also decline to consider further extending the safe harbor absent such a mandate, as such an extension would be outside the scope of this *Order*.

[270] *See Gateway Provider Notice* at paras. 77-78.

[271] *See, e.g.*, i3forum Comments at 7; iBasis Comments at 10; TNS Comments at 3-5; iBasis Reply at 4-5.

broadly, without tying the request to reasonable analytics.[272] However, we find that the rules we adopt today remove the need for such a safe harbor. In the case of blocking based on Commission notification, there is no need for a safe harbor where there is a clear Commission directive to block particular traffic directed at an individual provider. Nor is a safe harbor necessary for the downstream provider blocking requirement[273] because the immediate downstream provider is required to block all traffic from the identified provider, regardless of whether that provider is a gateway provider for the particular traffic. There is no judgment call for a provider to make that could require a safe harbor. We decline CTIA's request to establish a safe harbor is necessary for blocking based on a reasonable DNO list.[274] First, providers have been permitted to engage in this type of blocking since 2017, and no commenter has pointed to any liability issues regarding over-blocking in this context. A gateway provider that is concerned about the possibility that they may not be able to keep a list containing unallocated or unused numbers fully up to date is not required to include those numbers on the list; while these numbers may be included, they are not mandatory.[275] Providers that are concerned about possible under-blocking should take steps to ensure they are making use of a reasonable DNO list, and we see no reason to provide additional protection.

e. Protections for Lawful Calls

94. Consistent with our existing blocking rules, gateway providers must never block emergency calls to 911[276] and must make all reasonable efforts to ensure that calls from public safety answering points (PSAPs) and government emergency numbers are not blocked.[277] We decline to adopt additional transparency and redress requirements at this time or extend any other existing requirements that would not already apply to the blocking mandates we adopt today. The new mandatory blocking rules either require the Commission to direct blocking, in which case the blocking provider is not in a position to provide redress, or target categories of calls that have been permissible to block since 2017. Some commenters expressed concerns about transparency and redress.[278] We recognize some concerns regarding the potential for lawful calls to be blocked are valid, such as when a provider relies on analytics to make blocking decisions. These concerns do not apply here, however, where blocking is either at the direction of the Commission or based on a reasonable DNO list.

f. Compliance Deadline

95. We require gateway and downstream providers to comply with the requirements to block upon Commission notification no later than 60 days after publication of this *Order* in the Federal Register. Additionally, we require gateway providers to comply with the DNO blocking requirement no later than 30 days after publication of notice of OMB approval under PRA. We find that requiring gateway providers to comply with these rules quickly imposes a minimal burden. In the case of blocking upon Commission notification, gateway providers need not make any changes to their processes prior to receipt of such a notification, and we allow time for a gateway provider to comply following that

---

[272] *See, e.g.*, Comcast Comments at 8-9; INCOMPAS Comments at 12-13; T-Mobile Comments at 6; NCTA Reply at 1-2.

[273] *See, e.g.*, Comcast Comments at 8-9; NCTA Reply at 1-2.

[274] CTIA May 10 *Ex Parte* at 1-2

[275] *See supra* paras. 88-89 (discussing the scope of a reasonable DNO list).

[276] 47 CFR § 64.1200(k)(5). *See also* CTIA May 10 *Ex Parte* at 4 (asking us to clarify that gateway providers may block calls to 911 or other emergency numbers where the provider is working with a public safety agency to mitigate harm to service); INCOMPAS et al. May 6 *Ex Parte* at 3 (asking that we clarify, consistent with the existing rules, that this restriction applies only to emergency calls to 911 and does not prevent a gateway provider from blocking calls that are intended to cause harm to public safety).

[277] 47 CFR § 64.1200(k)(6).

[278] *See, e.g.*, INCOMPAS Comments at 10-14; Twilio Comments at 7; Voice on the Net Reply at 3.

notification. We acknowledge that gateway providers that do not already block based on a DNO list may need to identify or develop such a list in order to comply with that particular requirement. However, the PRA approval process gives providers ample time to do so, and providers may use one of the existing DNO lists to meet this requirement with minimal burden.

3. "Know Your Upstream Provider"

96. We adopt a modified version of our proposal to require gateway providers to "know the customer."[279] Recognizing the difficulty posed by a requirement for gateway providers to know information about the caller, who is likely not their customer and with whom they have no relationship, we instead require gateway providers to "know" the immediate upstream foreign provider from which they receive traffic with U.S. numbers in the caller ID field. Specifically, we require gateway providers to take reasonable and effective steps to ensure that the immediate upstream foreign provider is not using the gateway provider to carry or process a high volume of illegal traffic onto the U.S. network.

97. The record supports deeming the immediate upstream foreign provider as "customer" for these purposes, rather than the caller.[280] Though one commenter favored adopting our original proposal,[281] we agree with other commenters that it would be difficult, if not impossible, for gateway providers to routinely confirm that a particular caller is authorized to use a U.S. number.[282] By definition, a gateway provider is an intermediate provider and is thus at least one step removed from the caller.[283] By contrast, the gateway provider must have a direct relationship with the upstream foreign provider from which it accepts traffic, which allows the gateway provider to "know" that upstream provider. This approach best balances the benefit of holding gateway providers responsible for calls they allow into the U.S. network with the difficulty of determining information about a caller that may be several hops away from the gateway.

98. We agree with the commenter that argues that our existing, flexible approach to know-your-customer requirements, rather than specific mandates, is appropriate in the gateway context.[284] We do not mandate the steps gateway providers must take in order to "know" the upstream foreign provider. Instead, we allow gateway providers the flexibility to determine the exact measures to take, including whether to adopt contractual provisions with their upstream providers to meet this obligation, and the contours of any such provisions.[285] This approach is consistent with our existing requirement for originating providers to implement effective measures to prevent new and renewing customers from originating illegal calls, and allows each gateway provider to determine the best approach for its network and customers.[286] We make clear, however, that gateway providers must take effective steps. If a

---

[279] *Gateway Provider Notice* at paras. 80-86.

[280] *See, e.g.*, Comcast Comments at 9-10; INCOMPAS Comments at 10; Twilio Comments at 3-4.

[281] 51 State AGs Reply at 11.

[282] *See, e.g.*, Comcast Comments at 9; i3forum Comments at 9-10; iBasis Comments at 12; iconectiv Comments at 3; T-Mobile Comments at 7-8; Twilio Comments at 3-4; Enterprise Communications Advocacy Coalition Reply at 7.

[283] *See supra* paras. 25-27.

[284] *See* CTIA Comments at 12-13.

[285] *Fourth Call Blocking Order*, 35 FCC Rcd at 15232-33, paras. 32, 35 (noting that originating providers may meet the requirement to "know their customers and exercise due diligence in ensuring that their services are not used to originate illegal traffic" by "impos[ing] and enforce[ing] relevant contract terms."). We note that several commenters argued contract terms can be a valuable way of meeting a know-your-customer obligation and mitigating robocalls. *See* Twilio Comments at 4; Verizon Reply at 7-8.

[286] *See* 47 CFR § 64.1200(n)(3); *Fourth Call Blocking Order*, 35 FCC Rcd at 15232-33, paras. 32-36. For the same reason, we do not require gateway providers to enter into contractual provisions with their upstream provider to

(continued….)

gateway provider repeatedly allows a high volume of illegal traffic onto the U.S. network, the steps that provider has taken are not effective and must be modified for that provider to be in compliance with our rules.

99. We recognize concerns about the effectiveness of such a requirement, since the foreign provider upstream of the gateway may not be the source of the calls.[287] We agree that the ideal approach would be for any obligation to fall to the originating provider, as in our existing rules.[288] Unfortunately, in the case of foreign-originated calls, we face substantial difficulties in enforcing such an obligation on the foreign originating provider.[289] We recognize that gateway providers cannot prevent all instances of illegal calls from entering the U.S. network. In particular, a gateway provider's previously effective steps may become unexpectedly ineffective due to changes in factors outside of the gateway provider's control, particularly when the gateway provider is multiple hops from the call originator.[290] We therefore reiterate that, as with our existing rule, we do not expect perfection.[291] We do require gateway providers to take reasonable steps, and we encourage gateway providers to regularly evaluate and adjust their approach so that they remain reasonable and effective.[292]

100. Because we do not adopt the exact proposal in the *Gateway Provider Notice*, we decline to address roaming or adopt a carve-out for emergency calls.[293] The rule we adopt today does not require gateway providers to block calls when they cannot confirm that the caller is authorized to use a particular U.S. number in the caller ID field, and therefore is unlikely to have detrimental effect on roaming or emergency traffic. We also decline to adopt alternative proposals in the record that fall outside the scope of this *Order*, including YouMail's proposal for post-contracting know-your-customer,[294] i3forum's

---

meet this know-your-upstream-provider requirement or any other requirements we adopt today. *See Gateway Provider Notice* at paras. 87-89 (seeking comment on mandating contractual protections); iconectiv Comments at 2 (arguing that a gateway provider is unlikely to have contractual relationship with the call originator); Comcast Comments at 9 (any contractual obligations should only run to its upstream customer); CTIA Comments at 15 (providers should have flexibility to choose whatever safeguards, including contract terms, that have the effect of mitigating robocalls). However, gateway providers must explain the steps they have taken to meet their know-your-upstream-provider obligation in their Robocall Mitigation Database certification. *See infra* Section III.C.

[287] *See* T-Mobile Comments at 7-8.

[288] *See id*.

[289] Due to this jurisdictional issue, we impose this obligation on the gateway provider as the first U.S.-based provider in the call path.

[290] We further acknowledge that, no matter how effective a gateway provider's methods are, some illegal calls may make up a portion of the traffic that it originates onto the U.S. network, and make clear that the fact that some illegal calls evade detection does not necessarily make a gateway provider's methods ineffective. We therefore agree with parties that asked us to clarify that "occasionally serving as a gateway provider for illegal robocalls, particularly where those illegal calls are an insignificant fraction of that provider's traffic, does not inherently make the provider's practices ineffective." *See* INCOMPAS et al. May 6 *Ex Parte* at 2-3; *see also* CTIA May 10 *Ex Parte* at 3. We decline, however, to adopt the specific language proposed in the INCOMPAS et al. May 6 *Ex Parte*. INCOMPAS et al. May 6 *Ex Parte* at 3. We make clear, however, that a "high volume of illegal traffic" is a relative measure that is determined, in part, by what percentage of the traffic for which the provider is a gateway provider is illegal.

[291] *Fourth Call Blocking Order* 35 FCC Rcd at 15233, para. 36.

[292] Reasonable steps may include, but are not limited to, investigation of the practices of the upstream provider, modification of contracts to allow termination where issues arise, and/or monitoring incoming traffic for issues on an ongoing, proactive, basis.

[293] *Gateway Provider Notice* at para. 83. We further address roaming traffic in the attached Further Notice. *See infra* Section VI.H.

[294] YouMail Comments at 5-6.

"know your traffic" proposal,[295] or ZipDX's proposal to expand the requirement to cover all high-volume, non-conversational traffic even when such traffic is not foreign originated.[296]

101. *Compliance Deadline*. We require gateway providers to comply with this rule no later than 180 days after publication of this *Order* in the Federal Register. We agree with the commenter that argued that requiring compliance 30 days after publication may be insufficient for such a requirement.[297] Allowing 180 days after publication ensures that gateway providers have sufficient time to develop effective systems and make any modifications to their networks or practices to implement these measures.

4. General Mitigation Standard

102. In addition to the specific mitigation requirements that we adopt above, we also require gateway providers to meet a general obligation to mitigate illegal robocalls regardless of whether they have fully implemented STIR/SHAKEN on the IP portions of their network. We take this step now because of the unique and key role that gateway providers play in the call path.[298] Specifically, we now require all gateway providers to take "reasonable steps to avoid carrying or processing illegal robocall traffic."[299] We do not require that the gateway provider take specific steps to meet this standard, in line with the existing requirement for voice service providers.[300] The majority of commenters support the adoption of a general mitigation standard for gateway providers.

103. As with voice service providers subject to the "reasonable steps" standard, gateway providers must also implement a robocall mitigation program and, as explained above, file that plan along with a certification in the Robocall Mitigation Database.[301] The record reflects significant support for adopting, at a minimum, a mitigation duty for gateway providers in addition to requiring them to submit a certification to the Robocall Mitigation Database.[302] We therefore adopt, consistent with our proposal, a mitigation duty for gateway providers that closely tracks the analogous rule for voice service providers.[303] Specifically, a gateway provider's plan is "sufficient if it includes detailed practices that can reasonably

---

[295] i3forum Comments at 10-12.

[296] ZipDX Comments at 26.

[297] *See* Belgacom International Carrier Service Comments at 6.

[298] *See* NCLC and EPIC Reply at 4-5 ("Gateway providers . . . are in a unique position to arrest the flow of harmful scam calls and illegal robocalls. . . . To this end, we strongly support the Commission's proposal to impose a general duty on gateway providers to mitigate illegal robocalls.").

[299] *Infra*, Appx. A, 47 CFR § 64.6305(b)(2); *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1899, para. 76 (parallel obligation for voice service providers); 47 CFR § 64.6305(a)(2) (parallel rule for voice service providers that have not implemented STIR/SHAKEN).

[300] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1900, para. 78.

[301] *Gateway Provider Notice* at paras. 91-96; *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1899-903, paras. 76-85; *see also supra* Section III.C.

[302] *See Gateway Provider Notice* at para. 91; Comcast Comments at 10; CTIA Comments at 6-7 ("[B]y clarifying intermediate providers . . . are expected to implement robocall mitigation programs . . . the Commission can make its [Robocall Mitigation Database] more effective."); iBasis Comments at 13 ("iBasis agrees with the Commission's proposal to require gateway providers to submit a certification to the Robocall Mitigation Database describing their mitigation practices and stating that they are adhering to those practices."); USTelecom Comments at 4 (proposing that all providers should implement a robocall mitigation plan); *cf.* Twilio Comments at 3 ("[I]ntermediate providers, including gateway providers, must certify in the Robocall Mitigation Database [] that they have implemented a robocall mitigation program or implemented STIR/SHAKEN technology."); USTelecom Mar. 3 *Ex Parte* at 2-3.

[303] *Gateway Provider Notice* at para. 91.

be expected to significantly reduce the [carrying or processing] of illegal robocalls."[304] Moreover, a gateway provider "must comply with the practices" that its plan requires,[305] and its program is insufficient if the gateway provider "knowingly or through negligence [carries or processes calls] for unlawful robocall campaigns."[306]

104. We require gateway providers to mitigate traffic under the "reasonable steps" standard even if they have implemented STIR/SHAKEN for several reasons. First, we note the strong support in the record for requiring gateway provider mitigation, regardless of their STIR/SHAKEN status,[307] with certain commenters explicitly advocating for both gateway provider authentication and mitigation.[308] Commenters agree that gateway providers are uniquely positioned to stop the entry of robocalls into this country, increasing the importance of strong mitigation.[309]

105. Second, both the current record and the experience since the *Second Caller ID Authentication Report and Order* have shown that while STIR/SHAKEN is an effective tool to stop illegal robocalls, it is not a "silver bullet,"[310] particularly in those cases where a robocaller is using a properly assigned telephone number.[311] Providers, especially gateway providers serving as the entry point to the U.S. marketplace, can and must do more to stop robocalls. This is particularly the case while STIR/SHAKEN mandates by foreign governments and implementation by foreign providers remain

[304] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1900, para. 78 (obligation for voice service providers).

[305] *Id.*

[306] *Id.*

[307] CTIA Comments at 3 (supporting a requirement that all intermediate providers implement robocall mitigation programs, but not an authentication obligation); USTelecom Comments at 2-3 (arguing that all providers should "have robocall mitigation programs, regardless of their STIR/SHAKEN implementation status"); ZipDX Comments at 32; NCLC and EPIC Reply at 6 (supporting mitigation obligation for all providers); Twilio Comments at 3 (supporting mitigation measures and a database filing); USTelecom Reply at 3; Verizon Reply at 20 ("[T]he worst possible outcome . . . would be T-Mobile's proposal to mandate STIR/SHAKEN for 'gateway' providers but do nothing to require them – or any other intermediate service providers in the call path – to take any action to disrupt the chain of illegal robocalls destined for consumers."). *But see* INCOMPAS Comments at 8 (opposing a gateway provider mitigation obligation); T-Mobile Comments at 3 (opposing mitigation duty on gateway providers that are also voice service providers).

[308] Comcast Comments at 3, 10; Enterprise Communications Advocacy Coalition Comments at 1; 51 State AGs Reply at 2.

[309] *See, e.g.*, T-Mobile Comments at 2 (arguing that the Commission should focus its efforts on gateway providers); Verizon Reply at 6 (describing its mitigation practices as an intermediate provider), *id.* at 12 (arguing that the Commission should go further, but that it is "appropriate for the Commission, to look to address the foreign-originated robocall problem by protecting the edges, the PSTN"); T-Mobile Feb. 2 *Ex Parte* at 2 (arguing that it is already mitigating calls as an intermediate provider); *see also* 2020 NANC Best Practices Report at 14 (recognizing the key role that gateway providers play in facilitating illegal robocalls).

[310] *See* Press Release, FCC, STIR/SHAKEN Broadly Implemented Starting Today (Jun. 30, 2021), https://docs.fcc.gov/public/attachments/DOC-373714A1.pdf (Chairwoman Rosenworcel noting that "[w]hile there is no silver bullet" in stopping illegal robocalls, STIR/SHAKEN will "turbo-charge many of the tools we use in our fight against robocalls"); INCOMPAS Comments at 7 (supporting gateway provider authentication even though it is not a "silver bullet" but opposing mitigation obligations); Twilio Comments at 1 (supporting gateway provider mitigation obligations because STIR/SHAKEN is "not a silver bullet.").

[311] USTelecom Reply at 4 (noting that "STIR/SHAKEN alone cannot address the issue" where scammers are using "legitimately-assigned numbers," while a mitigation program can).

limited.[312]

106. Finally, we anticipate that a general mitigation duty applicable to all gateway providers regardless of whether they have implemented STIR/SHAKEN will "provide a valuable backstop" to the other obligations we adopt today[313] because call blocking, and traceback based on notice "cannot take the place of the *proactive* dut[y] to mitigate harmful traffic."[314] For all these reasons, we disagree with INCOMPAS and T-Mobile that we should not impose mitigation obligations on gateway providers that have implemented STIR/SHAKEN[315] and find that requiring gateway providers that have implemented STIR/SHAKEN to also meet our "reasonable steps" mitigation standard "would be an efficient use of their resources."[316] We do not adopt an alternative mitigation standard for gateway providers including a requirement proposed in the *Gateway Provider Notice* based on the existing duty for providers to take "affirmative, effective measures to prevent new and renewing customers from using their network to originate illegal calls."[317] We note, however, that under the rules we adopt today, gateway providers must also comply with the "know-your-upstream-provider standard,[318] and steps a gateway provider takes to meet one standard could meet the other, and *vice versa*.

107. We conclude that gateway providers' key role in facilitating the transmission of foreign-originated robocalls to U.S. consumers warrants imposing the "reasonable steps" mitigation duty on these providers without delay. While several commenters argue in the record for adopting more specific and broader duties on all domestic providers, we leave open for consideration such an expansion in the accompanying *Further Notice*.[319] For example, we do not at this time require gateway providers to take specific actions to meet the "reasonable steps" standard. Nor do we require voice service providers or other intermediate providers to comply with the unique requirements we adopt today for gateway providers, including the obligation to meet a general mitigation obligation even if they have fully implemented STIR/SHAKEN.[320] Given the scope of the *Gateway Provider Notice* and the limited record evidence submitted regarding specific proposals, we do not take these additional steps at this time.

108. *Compliance Deadline*. We require gateway providers to comply with the "reasonable steps" standard within 30 days of the effective date of this *Order*. We conclude that this is an appropriate period because we do not mandate specific steps that gateway providers must take to meet this

---

[312] *See* AB Handshake Comments at 1 (noting that the "origination of many illegal robocalls outside of the United States has limited STIR/SHAKEN's effectiveness despite its implementation across IP networks across the United States"); ECC Draft Report 338 at 32 (arguing that while European operators have not implemented STIR/SHAKEN, they are likely to do so "in due course").

[313] *Gateway Provider Notice* at para. 91; *see also* 51 State AGs Reply at 12 (agreeing that a mitigation obligation "can serve as an effective backstop").

[314] NCLC and EPIC Reply at 7 (italics in original); *see also* USTelecom Reply at 4 ("A robocall mitigation program can help to ensure that providers take proactive steps to prevent illegal robocalls.").

[315] INCOMPAS Comments at 9 ("It is unclear why a gateway provider would need to implement a robocall mitigation plan for the portions of its network in which it has implemented STIR/SHAKEN."); T-Mobile Comments at 9.

[316] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1899, para. 75 (determining that a dual obligation on voice service providers was not appropriate at that time, but noting that "[w]e will revisit this conclusion if we determine that additional robocall mitigation efforts are necessary in addition to STIR/SHAKEN after the caller ID authentication technology is more widespread").

[317] *Gateway Provider Notice* at para. 92.

[318] *See supra* Section III.E.3.

[319] *See, e.g.*, USTelecom Comments at 8; ZipDX Comments at 29; Verizon Reply at 2.

[320] *See, e.g.*, CTIA Comments at 7 (urging that the Commission require domestic intermediate providers to mitigate traffic and file in the Robocall Mitigation Database).

requirement other than submitting a certification to the Robocall Mitigation Database, and many gateway providers are already mitigating illegal call traffic.[321] The compliance date for the requirement to submit a certification and mitigation plan to the Robocall Mitigation Database is 30 days following Federal Register notice of OMB approval of the relevant information collection requirements,[322] and we expect providers to refine their "reasonable steps" in light of additional time and marketplace developments prior to submission into the Robocall Mitigation Database.[323]

F. Summary of Cost Benefit Analysis

109. We find that the benefits of the rules we adopt today will greatly outweigh the costs imposed on gateway providers. We sought comment on our belief that the proposed rules, viewed collectively, would account for a large share of the annual $13.5 billion minimum benefit we originally estimated in the *First Caller ID Authentication Report and Order and Further Notice* because of the large share of illegal calls originating outside of the United States.[324] While some commenters argue that the individual requirements may not provide substantial benefit taken individually[325] or that there is no benefit to imposing obligations solely on gateway providers,[326] others agree that the requirements we adopt today will benefit consumers and the calling ecosystem.[327] We find that these requirements, taken together, will achieve a large share of the annual $13.5 billion minimum benefit. In addition, we find that there are many additional, non-quantifiable benefits from these rules, including restoring confidence in the U.S. telephone network and reliable access to the emergency and healthcare communications that save lives, reduce human suffering, and prevent the loss of property.

110. We find that the costs imposed on gateway providers are, in many instances, minimal and in all cases do not exceed the benefits. For example, a number of gateway providers are already required to implement STIR/SHAKEN in some portions of their networks because they do not solely act as gateway or intermediate providers, but may also serve as originating or terminating providers for some calls.[328] In these cases, the additional burden to implement STIR/SHAKEN where a provider is acting as

---

[321] *Gateway Provider Notice* at para. 93 (arguing that any deadline balances the benefits and burdens).

[322] *See supra* Section III.C.

[323] *Cf. Wireless E911 Location Accuracy Requirements*, PS Docket No. 07-114, Sixth Report and Order and Order on Reconsideration, 35 FCC Rcd 7752, 7775-76, paras. 51-53 (2020) (adopting a requirement for CMRS providers to provide, by January 6, 2022, dispatchable location with wireless E911 calls if it is technically feasible and cost effective for them to do so).

[324] *Gateway Provider Notice* at paras. 107-09.

[325] *See, e.g.*, Belgacom International Carrier Services Comments at 4 (discussing the 24-hour traceback requirement); iBasis Comments at 5-6 (discussing authentication); USTelecom Comments at 11, 13-14 (discussing authentication and mandatory DNO blocking); USTelecom Reply at 7 (discussing authentication); Verizon Reply at 13-14 (discussing authentication).

[326] *See, e.g.*, T-Mobile Comments at 4, 7-8; Verizon Reply at 12-13.

[327] *See, e.g.*, Comcast Comments at 4-5 ("Comcast agrees with the Commission that expanding STIR/SHAKEN obligations across the voice service ecosystem will benefit all parties and call recipients."); T-Mobile Comments at 3 ("[A]s a terminating provider, it is valuable to T-Mobile to receive the STIR/SHAKEN information that gateway providers are currently not required to provide. Imposing those obligations on more providers will promote fewer spoofed calls overall."); ZipDX Comments at 36-37 ("We agree that significant benefits can come from the outcome of this proceeding providing that it is timely enforced.").

[328] *See, e.g.*, T-Mobile Comments at 2 (noting that it acts in both roles); USTelecom Reply at 2 (noting that providers act in different roles in different situations); Verizon Reply at 6-7 (noting that it has separate know-your-upstream provider practices in its role as an intermediate provider).

a gateway provider may be limited and has declined over time.[329] Similarly, requiring gateway providers to block, rather than effectively mitigate, illegal traffic when notified by the Commission does not represent a burden increase, and in some cases may even be a burden decrease by eliminating the need to determine what mitigation is effective in a particular instance. As explained, we disagree with the burden estimates proffered by some commenters.[330] However, even if we do credit those claims, the expected minimum benefit is, as explained, so large that it will greatly outweigh the expected burden.[331]

111. Moreover, although the rules we adopt today will impose higher short-term costs on gateway providers for implementation, we find that they will lead to lower long-term costs. Specifically, we find that an overall reduction in illegal robocalls will greatly lower network costs for the gateway providers and other domestic service providers by eliminating both the unwanted traffic congestion and labor costs of handling numerous customer complaints,[332] and by enabling those providers to trace calls back to the originator more quickly and efficiently.

G. Legal Authority

112. Consistent with our proposals, we adopt the foregoing obligations pursuant to the legal authority we relied on in prior caller ID authentication and call blocking orders. We note that no commenter questioned our proposed legal authority.[333]

113. *Caller ID Authentication.* We find authority to impose caller ID authentication obligations on gateway providers under section 251(e) of the Act and the Truth in Caller ID Act.[334] In the *Second Caller ID Authentication Report and Order*, the Commission found it had the authority to impose

[329] *See* 51 State AGs Reply at 5 (arguing that implementation costs for voice service providers that are also gateway providers are likely to be less than such providers' initial cost of implementation as a voice service provider); 2021 NANC CATA Report at 4 ("In general, there are no significant barriers which prevent universal STIR/SHAKEN implementation for interconnected and non-interconnected VoIP providers (regardless of size).").

[330] *See, e.g.*, USTelecom Reply at 9-11 (arguing that a gateway provider STIR/SHAKEN requirement would "fail any reasonable cost-benefit analysis"); Verizon Reply at 18 (arguing that requiring it to implement gateway provider authentication would "take multiple years and cost tens of millions of dollars" and that most calls would only be authenticated with "C-level" attestation); USTelecom Mar. 3 *Ex Parte* at 1; AT&T May 11 *Ex Parte* at 2 (arguing that gateway provider authentication will "not provide a material benefit" and estimating that the "costs will exceed ten million dollars" and "take more than two years").

[331] Contrary to USTelecom's assertion, we do not take the position that we "can adopt any individual regulation to fight illegal robocalls, no matter the cost or benefit of that particular regulation, as long as the aggregate cost of requirements is less than $13.5 billion." USTelecom May 6 *Ex Parte* at 2. Rather, we conclude that the requirements we adopt here will result in a "large share" of the $13.5 billion annual projected benefits from eliminating illegal robocalls, and no party has asserted that the purported costs of any or all of these regulations would cost either in one year or over several years a "large share" of $13.5 billion.

[332] *See Spiller NAL*, 35 FCC Rcd at 5651, para. 33 ("Spoofed robocalls harm carriers by (1) burdening the carriers' networks with illegal calls, and (2) inducing enraged recipients of the illegal robocalls to complain, thereby adding to the workload of customer service agents, decreasing the perceived value of the service, and increasing carrier costs.").

[333] *See* YouMail Comments at 10-13 (proposing for the Commission to utilize Section 205(a) to adopt an "index-based" safe harbor); NCLC & EPIC Reply at 5-6 (supporting our proposed legal authority). USTelecom suggests that because C-level attestations are "untethered to the call authentication goal," the TRACED Act does not provide authority to adopt a gateway provider authentication requirement. *See* USTelecom May 6 *Ex Parte* at 3, n.12 (internal citations omitted). But USTelecom's argument is inapposite because we do not rely on the TRACED Act for our authority to impose this obligation, and USTelecom does not assert that we otherwise lack authority to impose a gateway provider authentication obligation.

[334] *See* 47 U.S.C. §§ 227(e), 251(e).

caller ID authentication obligations on intermediate providers under these provisions.[335] It reasoned that "[c]alls that transit the networks of intermediate providers with illegally spoofed caller ID are exploiting numbering resources" and so found authority under section 251(e).[336] It found "additional, independent authority under the Truth in Caller ID Act" on the basis that such rules were necessary to "prevent . . . unlawful acts and to protect voice service subscribers from scammers and bad actors," stressing that intermediate providers "play an integral role in the success of STIR/SHAKEN across the voice network."[337] While the *Second Caller ID Authentication Report and Order* did not specifically discuss gateway providers, we use the same legal authority to impose an authentication obligation on gateway providers because we define gateway providers as a subset of intermediate providers.

114. *Robocall Mitigation and Call Blocking.* We adopt our robocall mitigation and call blocking provisions for gateway providers pursuant to sections 201(b), 202(a), 251(e), the Truth in Caller ID Act, and our ancillary authority, consistent with the authority we invoked to adopt analogous rules in the *Second Caller ID Authentication Report and Order* and our *Call Blocking Orders*.

115. We conclude that section 251(e) and the Truth in Caller ID Act authorize us to prohibit intermediate providers and voice service providers from accepting traffic from gateway providers that do not appear in the Robocall Mitigation Database. In the *Second Caller ID Authentication Report and Order*, the Commission concluded, "section 251(e) gives us authority to prohibit intermediate providers and voice service providers from accepting traffic from both domestic and foreign voice service providers that do not appear in [the Robocall Mitigation Database]," noting that its "exclusive jurisdiction over numbering policy provides authority to take action to prevent the fraudulent abuse of NANP resources."[338] The Commission observed that "[i]llegally spoofed calls exploit numbering resources whenever they transit any portion of the voice network—including the networks of intermediate providers" and that "preventing such calls from entering an intermediate provider's or terminating voice service provider's network is designed to protect consumers from illegally spoofed calls."[339] The Commission found that the Truth in Caller ID Act provided additional authority for our actions to protect voice service subscribers from illegally spoofed calls.[340]

116. We also conclude that sections 201(b), 202(a), and 251(e) of the Act, as well as the Truth in Caller ID Act and its ancillary authority, support the mandatory mitigation and blocking obligations we impose on gateway providers here. In the *Fourth Call Blocking Order*, the Commission required providers "to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls," which includes a duty to "know" their customers.[341] Additionally, the Commission required providers, to "take steps to effectively mitigate illegal traffic when notified by the Commission,"[342] which may require blocking when applied to gateway providers. The Commission also adopted traceback obligations.[343]

117. The Commission concluded that it had the authority to adopt these requirements pursuant

---

[335] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1931-32, paras. 153-55.

[336] *Id.* at 1931, para. 153.

[337] *Id.* at 1931, para. 154 (quoting *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3262, para. 44).

[338] *Id.* at 1910, para. 99.

[339] *Id*.

[340] *Id*. at 1910, para. 100.

[341] *Fourth Call Blocking Order*, 35 FCC Rcd at 15232-33, paras. 32-36.

[342] *Id.* at 15229-30, para. 22.

[343] *Id.* at 15227-29, paras. 15-19 (describing traceback obligations).

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.[344] Sections 201(b) and 202(a) provide the Commission with "broad authority to adopt rules governing just and reasonable practices of common carriers."[345] Accordingly, the Commission found that the new blocking rules were "clearly within the scope of our section 201(b) and 202(a) authority" and "that it is essential that the rules apply to all voice service providers," applying its ancillary authority in section 4(i).[346] 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,"[347] a category that includes Voice over Internet Protocol (VoIP) providers and, in the context of our call blocking orders, gateway providers.[348] We conclude that the same authority provides a basis to adopt the mitigation and blocking obligations on gateway providers we adopt in this *Order* to the extent that gateway providers are acting as common carriers.

118. While we conclude that our direct sources of authority provide an ample basis to adopt our proposed rules on all gateway providers, our ancillary authority in section 4(i)[349] provides an independent basis to do so with respect to gateway providers that have not been classified as common carriers. We conclude that the regulations adopted in this *Report and Order* are "reasonably ancillary to the Commission's effective performance of its . . . responsibilities"[350] because gateway providers that interconnect with the public switched telephone network and exchange IP traffic clearly offer "communication by wire and radio."[351]

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

120. *Indirect Effect on Foreign Service Providers.* We confirm our conclusion in the *Gateway Provider Notice* that, to the extent any of the rules we adopt today have an effect on foreign service providers, that effect is only indirect and therefore consistent with the Commission's authority,[352] and we find that it does not conflict with any of our international treaty obligations.[353] No commenter argues otherwise. In the *Second Caller ID Authentication Report and Order*, the Commission acknowledged an indirect effect on foreign providers but concluded that it was permissible under Commission precedent

[344] *Id.* at 15233-34, paras. 37-38.

[345] *Id.* 15233, para. 37.

[346] *Id.* at 15233-34, para. 37; *see also* 47 U.S.C. § 154(i).

[347] *Fourth Call Blocking Order*, 35 FCC Rcd at 15234, para. 37.

[348] *Id*. at 15222, n.2 (defining voice service provider to include intermediate provider).

[349] 47 U.S.C. § 154(i).

[350] *United States v. Southwestern Cable Co.*, 392 U.S. 157, 178 (1968); *see also, e.g.*, *Rural Call Completion*, WC Docket No. 13-39, Report and Order and Further Notice of Proposed Rulemaking, 28 FCC Rcd 16154, 16562, para. 35 (2013) ("Ancillary authority may be employed, at the Commission's discretion, when the Act 'covers the regulated subject' and the assertion of jurisdiction is 'reasonably ancillary to the effective performance of [the Commission's] various responsibilities.'") (footnotes omitted).

[351] 47 U.S.C. § 152(a).

[352] *See Gateway Provider Notice* at para. 119.

[353] The Commission expressly sought comment on "whether any of our proposed rules would be contrary to any of our international treaty obligations." *See id*. No commenter identified any international treaty obligations that would be contravened by our new requirement, nor is the Commission aware of any.

affirmed by the courts.[354] This includes the authority, pursuant to section 201, for the Commission to require that U.S. providers modify their contracts with foreign providers with respect to "foreign communication" to ensure that the charges and practices are "just and reasonable," as we do here.[355] The obligations we adopt today only impose such an indirect effect.

121. Several parties argue that foreign providers may not be able to file in the Robocall Mitigation Database because foreign legal obligations may prevent them from satisfying the traceback obligations imposed on all such filers.[356] To the extent that foreign providers face *bona fide* domestic legal constraints that conflict with any of the certifications or attestations required of Robocall Mitigation Database filers, we clarify that they may still submit a certification to the Robocall Mitigation Database. We recommend that foreign providers explain any such domestic legal constraints as part of their certification. We direct the Wireline Competition Bureau to make any limited, necessary changes to the Robocall Mitigation Database to ensure that foreign providers are able to provide any necessary explanations.

IV. ORDER ON RECONSIDERATION

122. In this *Order on Reconsideration*, we expand the requirement that voice service providers only accept calls carrying U.S. NANP numbers from foreign-originating providers listed in the Robocall Mitigation Database so that domestic providers may only accept calls carrying U.S. NANP numbers sent directly from foreign-originating or intermediate providers that are listed in the Robocall Mitigation Database, including those that have not been de-listed through enforcement action.[357] In doing so, we

[354] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1910 n.370 ("An indirect effect on foreign voice providers, however, 'does not militate against the validity of rules that only operate directly on voice service providers within the United States.'") (quoting *International Settlement Rate Benchmarks*, IB Docket No. 96-261, Report and Order, 12 FCC Rcd 19806, 19819, para. 27 (1997)); *see also Cable & Wireless P.L.C. v. FCC*, 166 F.3d 1224, 1230 (D.C. Cir. 1999) (finding that "the Commission does not exceed its authority simply because a regulatory action has extraterritorial consequences"); 47 CFR §§ 1.767(g)(5), 63.14 (prohibiting carriers from agreeing to access special concessions from a foreign carrier with respect to any U.S. international route where the foreign carrier possesses sufficient market power to adversely affect competition in the U.S. market); *Petition of AT&T for Settlements Stop Payment Order on the U.S.-Tonga Route*, IB Docket No. 09-10, Memorandum Opinion and Order, 29 FCC Rcd 4186, 4196, para. 24 (2014) (concluding that "Commission review and interpretation of contracts entered into by U.S. carriers for delivery of traffic to foreign destinations may, as here, be necessary and relevant to the Commission's policy goals of protecting U.S. ratepayers from the effects of anticompetitive actions. . . . Thus, the existence of extraterritorial consequences stemming from the Bureau's review of this case does not render the Bureau's actions impermissible.").

[355] *See* 47 U.S.C. § 201(a)-(b); *International Settlement Rates*, IB Docket No. 96-61, Report and Order, 12 FCC Rcd 19806, 19818, para. 26 (1997) ("We . . . find that the plain language of Section 201 gives us jurisdiction over settlement rates. To the extent that the above-cost portion of settlement rates paid by U.S. carriers to their foreign correspondents leads to those settlement rates being 'unjust or unreasonable,' Section 201 requires us to declare such 'charges' or 'practices' unlawful.").

[356] *See* Belgacom International Carrier Services Comments at 2; GSMA Reply at 3. We note that these obligations arise out of the prohibition established in the *Second Caller ID Authentication Report and Order* on receiving calls carrying U.S. NANP numbers from foreign providers not listed in the Robocall Mitigation Database. *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1904, para. 86; 47 CFR § 64.6305(c).

[357] We adopt this change in response to both CTIA's and VON's Petitions, as well as the *Gateway Provider Notice*, which sought comment on whether to eliminate, retain, or enhance the requirement that voice service providers only accept calls carrying U.S. NANP numbers from foreign providers listed in the Robocall Mitigation Database. *See* Petition for Partial Reconsideration of CTIA, WC Docket No. 17-97, at 2 (filed Dec. 17, 2020), https://www.fcc.gov/ecfs/file/download/DOC-5d9cb85236c00000-A.pdf?file_name=201217%20CTIA%20Petition%20for%20Partial%20Reconsideration%20-%20FINAL.pdf (CTIA Petition); Petition For Reconsideration of the VON Coalition, WC Docket No. 17-97 (filed Dec. 17, 2020), https://www.fcc.gov/ecfs/file/download/DOC-5d9c8c6266800000-

(continued….)

resolve the petitions of CTIA and VON seeking reconsideration of the existing requirement,[358] and end the stay of enforcement of that requirement in the *Gateway Provider Notice*.[359]

A. Background

123. In October 2020, the Commission adopted a rule that required U.S.-based providers to only accept traffic carrying U.S. NANP numbers that was received directly from voice service providers, including foreign voice service providers, that are listed in the Robocall Mitigation Database.[360] By its terms, the rule does not require U.S.-based providers to reject foreign-originated traffic carrying U.S. NANP numbers that is received by a U.S. provider directly from a foreign intermediate provider, but only applies to traffic received directly from the originating foreign provider.[361]

124. CTIA sought reconsideration of the requirement, arguing that it risked causing harmful consequences to mobile wireless consumers due to issues related to international mobile wireless roaming.[362] In particular, CTIA claims that reconsideration of the requirement and its effect on international mobile wireless traffic was necessary and appropriate to protect American mobile wireless customers living or travelling outside the United States.[363]

125. VON's Petition echoed CTIA's objection to the requirement, though objecting on procedural grounds. VON claimed that the requirement violates the Administrative Procedure Act (APA) because the Commission had failed to provide adequate notice that such a requirement might be adopted.[364]

126. In the *Gateway Provider Notice*, the Commission sought comment on whether the requirement as written allowed a significant portion of foreign-originated robocall traffic carrying U.S. NANP numbers to reach the U.S. outside of the requirement, and on whether the requirement should be expanded to require U.S.-based providers to only accept traffic carrying U.S. NANP numbers directly from any foreign provider registered in the Robocall Mitigation Database.[365] In light of (1) the "unique difficulties" foreign service providers were likely to face in timely registering with the Robocall Mitigation Database, (2) the fact that the requirement "can be evaded by transmitting traffic via one or more foreign intermediate providers," and (3) the goal to avoid the potential disruption associated with such delays and to permit the Commission time to explore potentially more effective measures, the Commission concluded that the public interest would not be served by enforcing the requirement that voice service providers only accept calls carrying U.S. NANP numbers from foreign voice service providers listed in the Robocall Mitigation Database during the pendency of the proceeding.[366] Thus, the

---

A.pdf?file_name=VON%20PFR%20Docket%2017-97%20FINAL%2012%2017%2020.pdf (VON Petition), 5; *Gateway Provider Notice* at paras. 104-06.

[358] *See generally* CTIA Petition; VON Petition. The VON Petition also seeks reconsideration of "the requirement in Section 64.6305(b)(4) that voice service providers filing certifications provide the name, telephone number and email address of a central point of contact within the company responsible for addressing robocall-mitigation-related issues." VON Petition at 1. We do not address that issue at this time, but may do so at a later date.

[359] *See Gateway Provider Notice* at para. 106.

[360] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1904-07, paras. 86-94; 47 CFR § 64.6305(c).

[361] 47 CFR § 64.6305(c).

[362] *See* CTIA Petition at 2.

[363] *See id.*

[364] *See* VON Petition at 3-5.

[365] *See Gateway Provider Notice* at para. 104.

[366] *Id.* at para. 106.

Commission held that, until a final decision was made regarding whether to eliminate, retain, or enhance the requirement, domestic voice service providers and intermediate providers could accept traffic carrying U.S. NANP numbers sent directly from foreign voice service providers not listed in the Robocall Mitigation Database.[367]

127. Once this *Order on Reconsideration* and the rules we adopt in the *Gateway Provider Report and Order* become effective and expand the rule, domestic providers may only accept, with limited exceptions,[368] calls sent directly from a provider that has affirmatively filed and is listed in the Robocall Mitigation Database; all gateway providers and all foreign-originating and intermediate providers sending calls directly to providers in the United States must at that point be registered in the Robocall Mitigation Database.

B. Ending the Stay of Enforcement and Extending the Requirement to Include Calls Received Directly from Intermediate Foreign Providers

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

129. Several commenters support this approach, including CTIA.[369] In its comments, CTIA notes that industry stakeholders have made significant strides in encouraging their foreign partners to implement robocall mitigation programs so that they can register in the Robocall Mitigation Database, with many reporting that "all, or nearly all, of their foreign partners that originate traffic have now registered," even absent enforcement of the requirement.[370] Indeed, as of May 17, 2022, 875 foreign voice service providers have filed in the Robocall Mitigation Database, out of a total 6,285 voice service provider filings. To further enhance the effectiveness of the Robocall Mitigation Database in protecting against foreign-originated robocalls, CTIA argues that the Commission should clarify that foreign intermediate providers must also implement robocall mitigation programs and certify to such in the database in order for their traffic to be accepted by domestic providers.[371] CTIA notes that promoting

---

[367] *Id.*

[368] Domestic intermediate providers that are not also voice service providers or gateway providers are not yet required to affirmatively file in the Robocall Mitigation Database, and downstream providers are not required to block calls from such providers not in the Robocall Mitigation Database. We propose in the accompanying *Further Notice* to require these providers to file. *See infra* Section VI.B.4.

[369] *See, e.g.*, CTIA Comments at 7; ZipDX Comments at 35; *see also* INCOMPAS and The Cloud Communications Alliance Reply, WC Docket No. 17-97, at 7-9 (filed Feb. 8, 2021) (INCOMPAS & CCA Recon Reply).

[370] CTIA Comments at 6-7. *But see* iBasis Comments at 13 (noting that it "has experienced difficulty in informing and assisting foreign providers in registering and has encountered some that have resisted registering "); INCOMPAS Comments at 14 (noting that it raised concerns regarding "the difficulties associated with educating and registering foreign providers in a U.S. database" in supporting the CTIA and VON Petitions).

[371] CTIA Comments at 7; *see also* ZipDX Comments at 35; INCOMPAS & CCA Recon Reply at 7-9.

robocall mitigation by foreign intermediate providers in this fashion will promote use of the techniques by all entities in the call path and will help protect U.S. networks from illegal traffic.[372]

130. We agree with CTIA's conclusions. Given the number of different entities that are typically involved in originating, carrying, processing, and terminating a call, a requirement that applies only to calls received directly from the foreign provider that originated them will capture only a small fraction of the total number of calls that domestic providers accept from foreign providers on a daily basis.[373] To increase the effectiveness of the requirement and to better protect American consumers from foreign-originated illegal robocalls, it is necessary to expand the scope of the requirement to include all calls received directly from a foreign provider that originates, carries, or processes the call in question. This approach obviates the concerns of commenters that a gateway provider likely does not know which provider originated a particular call or where it was originated; it only knows the upstream foreign provider that handed off the call.[374] Indeed, this is one of the reasons we define "gateway provider" in the accompanying *Gateway Provider Report and Order* as the U.S.-based intermediate provider that receives a call directly from a foreign originating or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider.

131. To ensure that foreign providers have sufficient time to take steps in light of this expanded rule and to facilitate consistent obligations, we will begin enforcing the requirement that providers accept only traffic received directly from foreign providers that originate, carry, or process calls that have filed a certification in the database on the deadline for gateway providers to block traffic sent from foreign providers that originate, carry, or process calls established in the accompanying *Gateway Provider Report and Order*. That is, enforcement will begin 90 days following the deadline for gateway providers to submit a certification to the Robocall Mitigation Database.[375] This same blocking deadline will also apply to providers to block traffic from foreign *intermediate* providers that were not subject to the prior blocking rule. The date of this deadline is subject to OMB approval for any new information collection requirements.[376] We conclude that this extended period will provide sufficient time for all affected foreign providers to submit a certification to the Robocall Mitigation Database in order to remain on the Database. For similar reasons, we add "in the caller ID field" to the expanded rule to clarify the scope of the requirement and make it consistent with the newly adopted blocking obligation for providers receiving calls from gateway providers.

132. Contrary to the dire outcomes contemplated in CTIA and VON's Petitions discussed below, the requirement that voice service providers only accept calls carrying U.S. NANP numbers from foreign voice service providers listed in the Robocall Mitigation Database has not resulted in mass confusion or a widespread failure on the part of foreign voice service providers to register in the Robocall Mitigation Database. In reality, a significant number of foreign voice service providers have been made aware of the requirement and have registered in the Robocall Mitigation Database.[377] Now that we have taken the time to ensure that the requirement can be implemented without causing significant disruptions to legitimate, legal traffic, it is time to ensure that the requirement adequately protects American

[372] CTIA Comments at 7.

[373] *See* INCOMPAS & CCA Recon Reply at 7-9.

[374] *See*, *e.g.*, Belgacom International Carrier Services Comments at 6; USTelecom Comments at 5; Twilio Comments at 3-4; iconectiv Comments at 3. *But see* VON Reply at 2 (arguing it can be extremely difficult to know if a provider is a foreign provider); Verizon Reply at 12-13 (same).

[375] *See supra* Section III.C.

[376] *See id*.

[377] CTIA Comments at 5-7; GSMA Comments at 2-3; *see also* Letter from Linda S. Vandeloop, Asst. Vice Pres., Federal Regulatory, AT&T Services, Inc., to Marlene H. Dortch, Secretary, FCC, WC Docket No. 17-97, at 1 (filed Sept. 24, 2021) (AT&T Sept. 24, 2021 *Ex Parte*).

consumers from as many foreign-originated illegal robocalls as possible, and not merely a tiny fraction of such calls. We know the requirement can work on a practical level, and we find that the expected benefits will far outweigh any minimal costs that may be imposed on gateway providers. While the rules we adopt in the *Gateway Provider Report and Order* provide some additional tools to domestic providers to combat illegal robocalls originating outside the U.S.,[378] we must give domestic providers as many tools as we can to protect their customers from as wide a swathe of foreign-originated illegal robocalls as possible.

133. Several commenters have urged the Commission to reach out to our counterparts in foreign governments and inform them of our latest efforts to protect consumers from illegal robocalls while also encouraging regulators abroad to promote foreign provider participation in robocall mitigation and the Robocall Mitigation Database.[379] We take this opportunity to reiterate our commitment to continue engaging actively with our international partners abroad to inform them of our latest efforts to combat illegal robocalls and to encourage robocall mitigation efforts on their part as well as participation in the Robocall Mitigation Database among their domestic providers. We recognize that it is only through active dialogue and cooperation with our international counterparts that we will be able to fully address the scourge of illegal robocalls here at home.

134. *Legal Authority*. We conclude that section 251(e) gives us authority to require intermediate providers and voice service providers to accept traffic only from foreign intermediate providers using U.S. NANP numbering resources in the caller ID field that appear in the Robocall Mitigation Database.[380] As we concluded in the *First Caller ID Authentication Report and Order and Further Notice* and affirmed in the *Second Caller ID Authentication Report and Order*, our exclusive jurisdiction over numbering policy provides authority to take action to prevent the fraudulent abuse of U.S. NANP resources.[381] Illegally spoofed calls exploit numbering resources whenever they transit any portion of the voice network—including the networks of intermediate and terminating providers. Our action preventing such calls from entering an intermediate provider's or terminating provider's network is designed to protect consumers from illegally spoofed calls, even while STIR/SHAKEN is not yet ubiquitous. No commenters have challenged our authority to require voice service providers to accept traffic only from foreign providers that do appear in the Robocall Mitigation Database.[382] One of the only

[378] *See* INCOMPAS Comments at 15 ("Given the potential scope of the new requirements on gateway providers, including application of caller ID authentication implementation and robocall mitigation provisions intended for intermediate providers, the Commission should be confident that these measures will be effective in stopping illegal robocall traffic from entering the U.S. market. These new requirements alone would appear to obviate the need for the foreign provider prohibition or for foreign providers to register in the Commission's RMD. As such, INCOMPAS urges the Commission to eliminate the foreign provider prohibition from its rules."). To quote T-Mobile, the tools the new gateway provider rules represent "may not be foolproof." T-Mobile Reply, WC Docket No. 17-97, at 2 (filed Feb. 8, 2021) (T-Mobile Recon Reply).

[379] CTIA Comments at 8; GSMA Comments at 2-3; INCOMPAS Comments at 15; CTIA Reply to Opposition, WC Docket No. 17-97, at 9-10 (filed Feb. 8, 2021) (CTIA Recon Reply); Verizon Reply at 10-11; *see also* T-Mobile Recon Reply at 7.

[380] *See* 47 U.S.C. § 251(e).

[381] *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3260-61, para. 42; *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1910, para. 99.

[382] T-Mobile does not challenge our authority to require intermediate providers and voice service providers to only accept traffic directly from foreign providers that appear in the Robocall Mitigation Database, but it asserts that "the FCC has no authority over foreign voice service providers." T-Mobile Recon Reply at 7. The revised rule we adopt today does not constitute the exercise of jurisdiction over foreign voice service providers. We acknowledge that this rule will have an indirect effect on foreign voice service providers by incentivizing them to certify to be listed in the database. An indirect effect on foreign voice service providers, however, "does not militate against the validity of rules that only operate directly on voice service providers within the United States." *International Settlement Rate*

(continued….)

parties to even touch upon the subject in response to the *First Caller ID Authentication Report and Order and Further Notice*, Verizon, agrees that section 251(e) gives us ample authority to ensure foreign VoIP providers "submit to the proposed registration and certification regime by prohibiting regulated U.S. carriers from accepting their traffic if they do not."[383]

135. We additionally find authority in the Truth in Caller ID Act.[384] We find that the rule we adopt today is necessary to enable voice service providers and intermediate providers to help prevent illegal spoofed robocalls and to protect voice service subscribers from scammers and bad actors that spoof caller ID numbers, and that section 227(e) thus provides additional independent authority for the revised rule we adopt today.[385]

C. Petitions for Reconsideration

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

1. CTIA Petition

137. We deny CTIA's Petition because the evidence in the record demonstrates that the requirement is unlikely to have the negative consequences CTIA fears, and the Commission has already followed CTIA's recommendations to focus on other mitigation efforts and to delay enforcement of the requirement while developing a more substantial record. In its Petition, CTIA raises three primary arguments against the requirement that domestic providers only accept calls carrying U.S. NANP

Benchmarks, IB Docket No. 96-261, Report and Order, 12 FCC Rcd 19806, 19819 (1997); *see also supra* Section III.G; *Cable & Wireless P.L.C. v. FCC*, 166 F.3d 1224, 1230 (D.C. Cir. 1999) (finding that "the Commission does not exceed its authority simply because a regulatory action has extraterritorial consequences"). In addition, several commenters raise concerns about whether registering in the Robocall Mitigation Database would have U.S. tax implications for foreign providers, whether registration would subject foreign providers to universal service contributions, and whether such providers would be subject to the Commission's enforcement authority regarding certifications or other matters, such as compliance with traceback requests. *See* CTIA Petition at 7 n.16; BT Americas Comments, WC Docket No. 17-97, at 4 (filed Jan. 29, 2021) (BT Americas Recon Comments); INCOMPAS & CCA Recon Reply at 4-5; T-Mobile Recon Reply at 7-8. In the absence of any showing of any significant tax consequences for foreign providers, and in light of the overwhelming pace at which they have already registered, we conclude that the benefits obtained by our new rules substantially outweigh any such possible consequences. We clarify that the act of registration in the Robocall Mitigation Database, by itself, would not create a universal service contribution obligation for a foreign provider. *See* 47 CFR § 54.706(a) (requiring contributions from providers of interstate telecommunications); 47 CFR § 54.706(c) (limiting contribution obligations for entities providing predominantly international services). Finally, we confirm that the Commission has authority to enforce our rules by ensuring that the Robocall Mitigation Database includes only accurate certifications.

[383] Verizon Comments, WC Docket No. 17-97 et al., at 8 (filed May 15, 2020) (Verizon 2020 Comments); *see also* T-Mobile Comments, WC Docket No. 17-97 et al., at 6-8 (filed May 15, 2020) (arguing that a foreign voice service provider "should be required to certify to the Commission that it uses an appropriate robocall mitigation program to prevent unlawful robocalls from originating on its network," and concurring that our numbering authority allows us "to impose numbering-related requirements - including the rights and obligations associated with using telephone numbers") (T-Mobile 2020 Comments).

[384] *See* 47 U.S.C. § 227(e)(1); 47 CFR § 64.1604(a).

[385] *See* 47 U.S.C. § 227(e)(1); *see also* 47 U.S.C. § 154(i) ("The Commission may perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as may be necessary in the execution of its functions.").

numbers from foreign voice service providers listed in the Robocall Mitigation Database: (1) the requirement will cause issues with international roaming that will harm American mobile wireless consumers in the U.S. and abroad; (2) the Commission's other efforts enable providers to protect consumers from illegal and unwanted robocalls from overseas without the need for a requirement that domestic providers only accept calls carrying U.S. NANP numbers from foreign voice service providers listed in the Robocall Mitigation Database; and (3) reconsideration is necessary because evidence of the requirement's impact on American wireless consumers is now available.[386] We address each of these arguments in turn.

a. International Roaming

138. CTIA asserts in its Petition that wireless roaming is a "complex endeavor, which is more complicated internationally, as U.S. mobile network operators have roaming agreements with hundreds of overseas network operators to enable U.S. consumers to remain connected no matter where they travel or move."[387] When a mobile wireless consumer abroad uses a U.S. phone number to call a consumer in the U.S., "that call may be routed from an originating foreign provider's network over long distance routes that involve multiple foreign mobile network operators often on the basis of least cost routing to reach a U.S. intermediate or terminating provider for delivery to the intended recipient."[388] Because of this, there are a "number of hand-offs for a call on its way back to a U.S. consumer, and any one of hundreds of foreign providers could be chosen as the final foreign provider in the call path that interconnects with a U.S. intermediate or terminating provider."[389] CTIA asserts that, if that final foreign voice service provider fails to implement a robocall mitigation program and certify to such in the Robocall Mitigation Database, all of its traffic—including legal, legitimate traffic—would be "prohibited from reaching the intended recipients. . . ."[390] Thus, CTIA claims that the requirement that domestic providers only accept calls carrying U.S. NANP numbers from foreign voice service providers listed in the Robocall Mitigation Database would risk "significant call completion issues for wireless calls from hundreds of foreign providers' networks, from any mobile wireless consumer using a U.S. phone number to make a call from abroad."[391] CTIA also claims that foreign voice service providers that interconnect with U.S. providers will "likely fail to register" with the Robocall Mitigation Database in a timely manner.[392] Thus, CTIA

[386] *See* CTIA Petition at 1-2.

[387] *Id.* at 4; CTIA Recon Reply at 4.

[388] CTIA Petition at 4.

[389] *Id.* at 5.

[390] *Id.*

[391] *Id.*; *see also* GSMA Support re Petition for Partial Reconsideration of CTIA, WC Docket No. 17-97, at 2-4 (filed Feb. 8, 2021) (GSMA Recon Reply); AT&T Reply, WC Docket No. 17-97, at 3-4 (filed Feb. 8, 2021) (AT&T Recon Reply); T-Mobile Recon Reply at 3-4; USTelecom Reply at 4; INCOMPAS & CCA Recon Reply at 3-6; USTelecom Reply, WC Docket No. 17-97, at 4-5 (filed Feb. 8, 2021) (USTelecom Recon Reply); CTIA Recon Reply at 2-4; Reply of The VON Coalition, WC Docket No. 17-97, at 4-6 (filed Feb. 8, 2021) (VON Recon Reply); Letter from Scott K. Bergmann, Senior Vice President, Regulatory Affairs, CTIA, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 17-97, at 3 (filed Feb. 10, 2021) (CTIA Feb. 10, 2021 *Ex Parte*). *But see* ZipDX LLC Reply, WC Docket No. 17-97, at 4 (filed Feb. 8, 2021) ("Because providers are increasingly fearful of carrying illegal traffic, many are inventing their own filters to decide what calls they accept and which they reject. Most providers are under no obligation to accept any particular call. Some now reject ALL calls from foreign sources. * * * Having a database that at least suggests which foreign providers might be trusted as sources of calls with USA originating numbers would be far better than the current and evolving luck-of-the-draw approach. USA providers would have a place to look as part of their upstream vetting process.") (ZipDX Recon Reply).

[392] CTIA Petition at 5; *see also* Comcast Comments at 10-11; iBasis Comments at 13 (claiming that iBasis has experienced difficulty in informing and assisting foreign providers in registering with the Robocall Mitigation Database and that it has "encountered some that have resisted registering"); INCOMPAS Comments at 15-16;

(continued….)

argues that reconsideration of the requirement is needed to prevent unintended blocking of legitimate, legal traffic and to give foreign providers sufficient time to develop robocall mitigation implementation plans and to register with the Commission.[393]

139. We believe that CTIA's concerns are overstated, and in any event we do not find them sufficient to outweigh the benefits of the requirement. In light of the prevalence of foreign-originated illegal robocalls aimed at U.S. consumers,[394] the requirement is a critical tool in combatting such calls. And far from resulting in a widespread failure to register with the Robocall Mitigation Database among foreign service providers, the requirement—along with the diligent and concerted efforts of U.S. providers—seems to have actively encouraged foreign voice service providers to institute robocall mitigation programs abroad and file certifications to be listed in the database and thus have their traffic continue to be accepted by domestic intermediate and terminating providers. As CTIA itself notes in its comments, since the establishment of the requirement in 2020, "U.S. providers have worked diligently to educate their foreign counterparts about call authentication, robocall mitigation, and registration expectations," outreach that has included individual providers engaging directly with their foreign counterparts, as well as efforts to increase awareness of these changes through existing industry bodies such as the GSMA, the Communications Fraud Control Association, and the M3AAWG.[395] According to CTIA, this work has produced results, with many foreign voice service providers implementing robocall mitigation plans and registering in the Robocall Mitigation Database even as the requirement has been held in abeyance.[396] Based on the education and outreach efforts of CTIA members, 99% of AT&T's international traffic now comes from carriers registered in the Robocall Mitigation Database.[397] Similarly, T-Mobile reports receiving all of its inbound international traffic from providers registered in the Robocall Mitigation Database, and Verizon states that approximately 99% of the traffic it receives from foreign voice service providers is from those registered in the Robocall Mitigation Database,[398] thus mooting T-Mobile's arguments that the *Second Caller ID Authentication Report and Order* contains little evidence "showing the likelihood of widespread compliance as a result of industry pressure" and that the requirement "will punish U.S. wireless subscribers when they are abroad, along with those in the U.S. whom they may try to call."[399] Beyond high levels of Robocall Mitigation Database registration among

---

USTelecom Comments at 5-6; CTIA Recon Reply at 4-5; IDT Telecom, Inc. Reply Comments, WC Docket No. 17-97, at 2 (filed Feb. 8, 2021) (IDT Recon Reply); USTelecom Recon Reply at 5; iBasis Reply at 6; VON Reply at 2; GSMA Recon Reply at 4. And BT Americas Inc. asserts in its comments in support of the CTIA Petition that "the certification process may place foreign carriers in the impossible situation of either having to violate their commitment to the FCC or violate the laws of their home country." BT Americas Recon Comments at 5; *see also* T-Mobile Recon Reply at 7; INCOMPAS & CCA Recon Reply. As we state in the accompanying *Gateway Provider Report and Order*, to the extent that foreign providers face *bona fide* domestic legal constraints that conflict with any of the certifications or attestations required of Robocall Mitigation Database filers, they may still submit a certification to the Robocall Mitigation Database and explain any such domestic legal constraints as part of their certification. *See supra* Section III.G.

[393] CTIA Petition at 7; *see also* GSMA Recon Reply at 2-3; AT&T Recon Reply at 4-5; USTelecom Recon Reply at 6-7; Verizon Reply at 11.

[394] *See Implementing Section 503 of the RAY BAUM's Act; Rules and Regulations Implementing the Truth in Caller ID Act of 2009*, WC Docket Nos. 18-335, 11-39, Second Report and Order, 34 FCC Rcd 7303, 7306-07, para. 10 (2019).

[395] CTIA Comments at 4.

[396] *Id.* at 4-5.

[397] *Id.* at 5; *see also* AT&T Sept. 24, 2021 *Ex Parte* at 1.

[398] CTIA Comments at 5.

[399] T-Mobile Recon Reply at 1-2, 4. This result also runs counter to IDT's concerns that the requirement would be anticompetitive for U.S. companies because it would "incline toward a handful of foreign wholesalers dominating (continued….)

foreign voice service providers, CTIA reports that "domestic voice service providers have continued to modify their interconnection contracts with foreign providers to focus on the need to mitigate illegal robocall traffic."[400]

140. Given the extraordinarily high levels at which foreign voice service providers have implemented robocall mitigation programs and registered with the Robocall Mitigation Database even absent enforcement of the requirement, we find CTIA's initial concerns that foreign voice service providers would fail to register with the database to no longer be an issue.[401] Indeed, it appears that, much as CTIA intended, our decision to hold the requirement in abeyance has permitted domestic providers to interface with their foreign counterparts and encourage them to develop robocall mitigation implementation plans and register with the Robocall Mitigation Database. We, therefore, conclude that the requirement should not result in significant call completion issues and that reconsideration based on this concern is unwarranted.

b. Other Efforts to Curb Illegal Robocalls

141. CTIA's second argument is that the Commission's other actions to prevent illegal and unwanted robocalls from outside the United States—including enforcement actions against VoIP providers facilitating illegal voice traffic, encouraging providers to protect international gateways from robocalls, and adopting a safe harbor for blocking traffic from bad actors—are more targeted and less disruptive than the requirement that domestic providers only accept calls carrying U.S. NANP numbers from foreign voice service providers listed in the Robocall Mitigation Database.[402] Thus, the Commission "should continue to focus on these and similar efforts while developing the record" on the requirement.[403]

142. After having developed a more fulsome record on the requirement in the wake of the *Gateway Provider Notice*, we find that the requirement that domestic providers only accept calls carrying U.S. NANP numbers from foreign voice service providers listed in the Robocall Mitigation Database is not disruptive and that our other actions to prevent illegal and unwanted robocalls from overseas are insufficient on their own to properly address the problem of foreign-originated illegal robocalls. As CTIA itself has noted since filing its initial petition, industry outreach to foreign voice service providers has met with great success, with numerous foreign voice service providers implementing robocall mitigation plans and registering in the Robocall Mitigation Database.[404] With 99% of AT&T and Verizon's and 100% of T-Mobile's inbound international traffic now coming from carriers who are registered in the Robocall

---

the aggregation of USA termination, leading to only a small number of US carriers connecting with them." IDT Recon Reply at 2.

[400] CTIA Comments at 5.

[401] Nor has there been, as IDT feared, a rash of reciprocal registration and filing requirements for U.S. providers from foreign regulators. IDT Recon Reply at 2. As for IDT's concern that the requirement would lead to "an unequal enforcement problem, as many small operators may turn a blind eye to the requirement of their customers' registration, yet will go undetected because of a low profile," IDT Recon Reply at 3, such a generalized risk could be said to apply equally to every regulation we adopt and is not a valid reason to refrain from adopting a specific policy or regulation. Moreover, this argument imparts a heightened degree of malicious intent to small providers based purely upon the size of their operations. We do not believe that small providers are any more or less likely to engage in illegal or malicious conduct than are large ones, and we thus reject the assumptions underpinning this argument.

[402] CTIA Petition at 7-8.

[403] *Id.* at 8; *see also* iBasis Comments at 13; AT&T Recon Reply at 4-7; CTIA Recon Reply at 8; INCOMPAS Comments at 15-16; iBasis Reply at 6; GSMA Recon Reply at 4; INCOMPAS & CCA Recon Reply at 5; USTelecom Recon Reply at 2-4, 7-8; VON Reply at 2.

[404] CTIA Comments at 4-5.

Mitigation Database,[405] we find it unlikely that enforcement of the requirement that domestic providers only accept calls carrying U.S. NANP numbers from foreign voice service providers listed in the Robocall Mitigation Database will result in widespread call completion issues.[406] At the same time, we believe that the requirement is necessary to supplement our other actions, including enforcement actions against VoIP providers facilitating illegal voice traffic, encouraging providers to protect international gateways from robocalls, and adopting a safe harbor for blocking traffic from bad actors.[407] While these steps are certainly important, merely encouraging providers to protect international gateways from illegal foreign-originated robocalls and adopting a safe harbor for those who block traffic from bad actors is not sufficient. If we are to adequately address the significant problem of foreign-originated robocalls, just as with U.S. originated robocalls, those receiving such calls (here, gateway providers) must explicitly be required to accept only those calls carrying U.S. NANP numbers from foreign voice service providers that are listed in the Robocall Mitigation Database. To address the endemic practice of illegal robocalling, we must use every tool at our disposal, especially those which have been shown not to result in significant call completion issues. We thus find CTIA's second argument unpersuasive.

c. Availability of Additional Evidence

143. CTIA's final argument is that reconsideration is appropriate because the Commission did not, in the *Second Caller ID Authentication Report and Order*, seek comment on the impacts of the requirement on international wireless roaming.[408] Without such record evidence, CTIA contends, the Commission lacked "sufficient support to prohibit domestic intermediate and terminating providers from completing calls from foreign voice service providers that have not certified in the [Robocall Mitigation Database]."[409] Thus, CTIA claims that the Commission should reconsider the requirement and further develop its record so that it can craft a "more reasonable approach to encourage international provider certification" without jeopardizing U.S. consumers or the U.S. voice network.[410]

144. As noted above, the Commission solicited a more robust record in response to the *Gateway Provider Notice* regarding the requirement and its possible effects. As that record shows, efforts to educate foreign voice service providers and encourage implementation of robocall mitigation programs and registration with the Robocall Mitigation Database have met with great success.[411] Foreign providers have been granted time to develop robocall mitigation implementation plans and register with the Robocall Mitigation Database, and they appear to have used that time well. In light of this success, we feel confident that we may proceed with enforcement of the requirement that domestic providers only accept calls carrying U.S. NANP numbers from foreign voice service providers listed in the Robocall Mitigation Database without causing significant disruption to the completion of legal, legitimate traffic. The requirement, as crafted, is already "reasonable," and addresses illegal robocalls originating from outside the United States without jeopardizing U.S. consumers or the U.S. voice network.

145. For the forgoing reasons, we deny CTIA's petition.

---

[405] *Id.* at 5; *see also* AT&T Sept. 24, 2021 *Ex Parte* at 1.

[406] *See* AT&T Recon Reply at 2 ("[T]o the extent a foreign carrier fails to make the robocall mitigation certification, or lacks the requisite capabilities to enable the foreign carrier to certify by the compliance deadline, AT&T would have no choice but to block all U.S.-bound voice traffic received directly from the non-certifying foreign carrier."); T-Mobile Recon Reply at 3-4.

[407] *See* CTIA Petition at 7-8.

[408] *Id.* at 10.

[409] *Id.*

[410] *Id.*; *see also* Comcast Comments at 10-11; GSMA Comments at 2; USTelecom Comments at 5-6; USTelecom Recon Reply at 1-2.

[411] *See* CTIA Comments at 5; *see also* AT&T Sept. 24, 2021 *Ex Parte* at 1.

2. VON Petition

146. VON's Petition relies largely on a single argument in seeking reconsideration of the requirement that domestic providers only accept calls carrying U.S. NANP numbers from foreign providers listed in the Robocall Mitigation Database—that the requirement violates the APA because the Commission failed to solicit and consider public comment on it.[412] Thus, VON contends that the Commission should seek additional comments on the proposal to "allow for a more thoughtful vetting of an otherwise very complicated issue."[413] We deny the VON Petition on substantive grounds for the reasons stated below. We alternatively dismiss the Petition as mooted by the Commission's decision to hold enforcement of the requirement in abeyance until a final decision was reached regarding whether to eliminate, retain, or enhance the requirement and the Commission's request for comments on the scope of the requirement in the *Gateway Provider Notice*.[414]

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

147. In the *First Caller ID Authentication Report and Order and Further Notice*, the Commission proposed that, when an intermediate provider receives an unauthenticated call that it will exchange with another intermediate or voice service provider as a SIP call, it must authenticate such a call with a "gateway" or C-level attestation.[415] In seeking comment on that proposal, the Commission noted that multiple commenters had supported imposing STIR/SHAKEN requirements on gateway providers as a way to identify robocalls that originate abroad and to identify which provider served as the entry point for these calls to U.S. networks.[416] The Commission then sought comment on whether this was an effective way to combat illegal calls originating outside the U.S. and whether there were "other rules involving STIR/SHAKEN that we should consider regarding intermediate providers to further combat illegal calls originating abroad."[417] The Commission also reiterated Verizon's suggestion that we impose an obligation to use STIR/SHAKEN on any provider, regardless of its geographic location, if it intends to allow its customers to use U.S. telephone numbers, as well as USTelecom's proposal that the Commission consider obligating gateway providers to pass international traffic only to downstream providers that have implemented STIR/SHAKEN.[418] The Commission sought comment on both proposals and asked if there were any other actions it could take to promote caller ID authentication implementation to combat robocalls originating abroad.[419]

148. In response to the *First Caller ID Authentication Report and Order and Further Notice*, several commenters filed initial comments expressing support for combating robocalls originating abroad by requiring foreign voice service providers that appear in the Robocall Mitigation Database to follow the same requirements as domestic voice service providers.[420]

---

[412] VON Petition at 3-4; VON Recon Reply at 6.

[413] VON Petition at 5; *see also* USTelecom Recon Reply at 1-2.

[414] *See Gateway Provider Notice* at para. 106.

[415] *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3272, para. 64.

[416] *Id*. at 3272, para. 64.

[417] *Id*. at 3272, para. 64.

[418] *Id*. at 3272-73, para. 64.

[419] *Id*. at 3273, para. 64.

[420] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1906, para. 90; T-Mobile 2020 Comments at 6; USTelecom Comments, WC Docket Nos. 17-97 et al., at 5-8 (USTelecom 2020 Comments); Verizon 2020 Comments at 6-8.

149. Courts have long held that the APA requires that the final rule that an agency adopts be a "logical outgrowth of the rule proposed."[421] While the Commission did not explicitly propose a rule in the *First Caller ID Authentication Report and Order and Further Notice* requiring domestic intermediate and terminating providers to accept calls only from foreign voice service providers that use U.S. NANP numbers and are listed in the Robocall Mitigation Database, it did seek comment on: (1) whether to impose STIR/SHAKEN requirements on gateway providers as a way to identify robocalls that originate abroad; (2) whether there were other rules involving STIR/SHAKEN that the Commission should consider regarding intermediate providers to further combat illegal calls originating abroad; (3) Verizon's suggestion to impose on any provider, regardless of its geographic location, an obligation to use STIR/SHAKEN; (4) USTelecom's proposal that the Commission consider obligating gateway providers to pass international traffic only to downstream providers that have implemented STIR/SHAKEN; and (5) whether there were any other actions the Commission could take to promote caller ID authentication implementation to combat robocalls originating abroad.[422] We conclude that the requirement that domestic providers only accept calls carrying U.S. NANP numbers from foreign voice service providers listed in the Robocall Mitigation Database is a logical outgrowth of these repeated and specific requests for comment on the types of obligations the Commission should impose on gateway providers that accept traffic from foreign voice service providers. Indeed, while it did not specifically mention the requirement in its final adopted form, the Commission did seek comment on whether to impose STIR/SHAKEN requirements on gateway providers, as well as other actions that would promote caller ID authentication implementation and combat foreign-originated robocalls.

150. That this requirement is a logical outgrowth of such requests for comment is evident from the fact numerous entities filed comments in response to the *First Caller ID Authentication Report and Order and Further Notice* voicing support for combating robocalls originating abroad by requiring foreign voice service providers that appear in the Robocall Mitigation Database to follow the same requirements as domestic voice service providers.[423] While the two are not exactly the same, this notion of requiring foreign voice service providers who file with the Robocall Mitigation Database to fulfill the same requirements as domestic providers is quite similar to the requirement the Commission eventually adopted, and the fact that it was mentioned by multiple commenters indicates that the requirement was indeed a logically foreseeable outgrowth of the language in the *First Caller ID Authentication Report and Order and Further Notice*. Even were it not a logical outgrowth of the *First Caller ID Authentication Report and Order and Further Notice*, the possibility of a requirement that domestic providers only accept calls carrying U.S. NANP numbers from foreign providers listed in the Robocall Mitigation Database was raised in the initial comments and was open to consideration and comment during the reply stage.

151. We thus find VON's claim that the adoption of the requirement violated the APA to be baseless and, accordingly, deny their Petition on substantive grounds.

b. VON's Petition Is Moot

152. Independently, and in the alternative, we find that the Commission's decision to hold enforcement of the requirement in abeyance until it reached a final decision regarding whether to eliminate, retain, or enhance the requirement, together with the Commission's request for comments on the scope of the requirement in the *Gateway Provider Notice,* renders the VON Petition moot.[424] Even assuming *arguendo* that the initial adoption of the requirement in the *Second Caller ID Authentication*

[421] *Time Warner Cable Inc. v. F.C.C.*, 729 F.3d 137, 169 (D.C. Cir. 2013) (quoting *National Black Media Coalition v. F.C.C.*, 791 F.2d 1016, 1022 (2d Cir. 1986)).

[422] *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3271-72, para. 64.

[423] T-Mobile 2020 Comments at 6; USTelecom 2020 Comments at 5-8; Verizon 2020 Comments at 6-8.

[424] *Gateway Provider Notice* at paras. 103-06.

Report and Order violated the notice and comment requirements of the APA, the same cannot be said of the *Gateway Provider Notice*, which specifically and extensively sought comment on whether "to eliminate, retain, or enhance" the requirement.[425]

153. Much like CTIA in its own Petition, VON did not call for the wholesale elimination of the requirement that domestic providers only accept calls carrying U.S. NANP numbers from foreign voice service providers listed in the Robocall Mitigation Database, but merely time to solicit additional comment and allow for further consideration of the requirement.[426] Regardless of whether the *First Caller ID Authentication Report and Order and Further Notice* provided notice and an opportunity to comment on the requirement, the *Gateway Provider Notice* undoubtedly provided both. The Commission in the *Gateway Provider Notice* stated that, until a final decision was made regarding whether to eliminate, retain, or enhance the requirement, it would not enforce the requirement that domestic voice service providers and intermediate providers accept only traffic carrying U.S. NANP numbers sent directly from foreign voice service providers listed in the Robocall Mitigation Database.[427] As we have satisfied the terms of VON's Petition, we dismiss it as moot.[428]

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

V. ORDER

155. In this *Order*, we make a ministerial change to a codified rule required to correct an inadvertent typographical error and spell out an undefined acronym. We revise section 64.6300(f) of our rules, which defines the term "intermediate provider," to change the word "carriers" to "carries" and to change the reference to "PSTN" to "public switched telephone network."[429] We find that there is good cause for adopting this amendment here because the typographical error may confuse those seeking to understand how the Commission defines the term "intermediate provider" for purposes of complying with our rules governing caller ID authentication, and the use of undefined acronyms, even if well known, is not preferable.[430]

---

[425] *Id*. at para. 106; *Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Proposed Rules, 86 FR 59084, 59101-02, para. 106 (2021).

[426] VON Petition at 5; VON Recon Reply at 6.

[427] *Gateway Provider Notice* at para. 106. We treat our holding enforcement of the prohibition in abeyance the same as a stay. *See, e.g.*, *Amendment of Part 90 of the Commission's Rules; Petition for Clarification and to Hold in Abeyance Changes to Frequency Coordination Requirement*, WP Docket No. 07-100, Order, 27 FCC Rcd 4917, 4918, para. 4 (PSHSB 2012) (treating a "request to hold the rule change in abeyance as a request for stay of the effective date of the rule change").

[428] As with the CTIA Petition, we note that the concerns raised in the VON Petition—namely, that the requirement would limit the number of foreign carriers who can terminate calls in the U.S., restrict the ability of U.S. carriers to terminate calls on behalf of U.S. customers to foreign points, and lead to the disruption of legitimate, non-harmful traffic—have proved to be largely unfounded in the wake of adoption of the requirement, and as noted above, 99% of AT&T and Verizon's and 100% of T-Mobile's inbound international traffic currently comes from carriers who are registered in the Robocall Mitigation Database. Thus, as with CTIA's concerns, we find VON's concerns about the potential failure of foreign providers to register in the database to be largely baseless in reality.

[429] *See* 47 CFR § 64.6300(f).

[430] *See* 47 CFR § 64.6300 *et seq*.

156. Section 553 of the Administrative Procedure Act permits us to amend our rules without undergoing notice and comment where we find good cause that doing so is "impracticable, unnecessary, or contrary to the public interest."[431] The Commission has previously determined that notice and comment is not necessary for "editorial changes or corrections of typographical errors."[432] Consistent with Commission precedent, in this instance we find that notice and comment is unnecessary for adopting a ministerial revision to section 64.6300(f) to correct an inadvertent typographical error and spell out an undefined acronym in the definition of "intermediate provider."

VI. FURTHER NOTICE OF PROPOSED RULEMAKING

157. In the *Gateway Provider Report and Order*, we take steps to protect American consumers from foreign-originated illegal calls by adopting a number of rules that focus on gateway providers as the entry point onto the U.S. network. In this *Further Notice of Proposed Rulemaking*, we further propose and seek comment on expanding some of these rules to cover other providers in the call path, along with additional steps to protect American consumers from all illegal calls, whether they originate domestically or abroad.

158. First, we propose to extend our caller ID authentication requirement to cover domestic intermediate providers that are not gateway providers in the call path. Second, we seek comment on extending some, but not all, of the robocall mitigation duties we adopt in the *Order* to all domestic providers in the call path. These mitigation duties include: expanding and modifying our existing affirmative obligations; requiring downstream providers to block calls from non-gateway providers when those providers fail to comply; the general mitigation standard; and filing a mitigation plan in the Robocall Mitigation Database regardless of STIR/SHAKEN implementation status. We also seek comment on additional measures to address illegal robocalls, including: ways to enhance the enforcement of our rules; clarifying certain aspects of our STIR/SHAKEN regime; and placing limitations on the use of U.S. NANP numbers for foreign-originated calls and indirect number access.

159. We anticipate that the impact of our proposals will account for another large share of the annual $13.5 billion minimum benefit we originally estimated in the *First Caller ID Authentication Report and Order and Further Notice* for eliminating unlawful robocalls, in addition to the collective impact of the rules we adopt today and the rules adopted earlier in these proceedings.[433] While each of the proposed requirements on their own may not fully accomplish that goal, viewed collectively, we expect that they will achieve a large share of the annual $13.5 billion minimum benefit. We also expect that this share of benefits will far exceed the costs imposed on providers. We seek comment on this analysis and on the possible benefits of the requirements we propose.

A. Extending Authentication Requirement to All Intermediate Providers

160. To further combat illegal robocalls consistent with the rules we adopt today, we propose to require that *all* U.S. intermediate providers authenticate caller ID information consistent with STIR/SHAKEN for SIP calls that are carrying a U.S. number in the caller ID field and to require all providers to comply with the most recent version of the standards as they are released. We seek comment on these proposals.

161. As the Commission has previously explained, application of caller ID authentication by intermediate providers "will provide significant benefits in facilitating analytics, blocking, and traceback by offering all parties in the call ecosystem more information."[434] At the time the Commission reached

[431] 5 U.S.C. § 553(b)(3)(B).

[432] *Amendment of Part 90 of the Commission's Rules*, Docket No. WP 07-100, Notice of Proposed Rulemaking, 22 FCC Rcd 9595, para. 30 (2007).

[433] *Gateway Provider Notice* at paras. 107-09.

[434] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1928, para. 144.

this conclusion, given the concerns that an authentication requirement on all intermediate providers "was unduly burdensome in some cases," the Commission established that instead of authenticating unauthenticated calls, intermediate providers could "register and participate with the industry traceback consortium as an alternative means of complying with our rules."[435]

162. Since the Commission established those requirements in the *Second Caller ID Authentication Report and Order*, in the *Fourth Call Blocking Order*, the Commission subsequently required all providers in the call path—including gateway providers and other intermediate providers—to respond fully and in a timely manner to traceback requests.[436] This rule has effectively mooted the choice given to intermediate providers in the earlier *Second Caller ID Authentication Report and Order* to authenticate calls *or* cooperate with traceback requests.[437] Evidence shows that robocalls are a significant and increasing problem.[438] To further strengthen the STIR/SHAKEN regime and protect consumers and the integrity of the U.S. telephone network, we propose that all intermediate providers should be required to authenticate unauthenticated SIP calls that they receive. We seek comment on this proposal.

163. Intermediate providers could play a crucial role in further promoting effective, network-wide caller ID authentication.[439] Requiring all intermediate providers to authenticate caller ID information for all unauthenticated SIP calls will provide information to downstream providers that will facilitate analytics and promote traceback efforts.[440] SHAKEN verification, even "C-level" attestation, provides relevant and helpful information to downstream providers, particularly as the STIR/SHAKEN regime becomes even more ubiquitous.[441] Adopting this proposal would bring all U.S. providers within the STIR/SHAKEN regime and prevent gaming by providers, allowing "for more robust abilities to either trust the caller or perform traceback because an illegal caller can be more easily identified."[442] Indeed, STIR/SHAKEN becomes more useful the more providers there are that employ it.[443]

164. We believe this proposal is in line with commenter assertions that expanding call authentication requirements will have a "significant impact in curtailing illegal robocalls"[444] and that

---

[435] *Id.* at 1927, para. 144; 47 CFR § 64.6302(b).

[436] *See Fourth Call Blocking Order*, 35 FCC Rcd at 15227-29, paras. 15-21.

[437] *See* 47 CFR § 64.6302(b).

[438] *See* ZipDX Comments at 7-8; Letter from Margot Saunders, National Consumer Law Center, Chris Frascella, Electronic Privacy Information Center, to Marlene Dortch, Secretary, FCC, CG Docket No. 17-59, WC Docket No. 17-97, at 1 (filed on Feb. 10, 2022) (NCLC and EPIC Feb. 10 *Ex Parte*).

[439] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1922-23, para. 132.

[440] *Id.* at 1926, para. 141.

[441] *See* 2022 NANC CATA Best Practices Report at 6-7 ("SHAKEN verification can provide a rich set of inputs for anti-robocalling analytics. Absence or presence of a SHAKEN call signature can be useful input. Successful or failed verifications can also provide useful input. Beyond success or failure, the information elements of the call signature can provide additional useful inputs to anti-robocalling analytics. . . . [T]he value can help facilitate traceback and potentially provide additional information as input to analytics algorithms.").

[442] *Id.* at 6.

[443] *See* INCOMPAS Comments at 7-8; 51 State AGs Reply at 4; T-Mobile Feb. 2 *Ex Parte* at 4 (asserting "the greater the number of providers that employ STIR/SHAKEN, the better for the entire calling ecosystem"); 2022 NANC CATA Best Practices Report at 5 (explaining "[t]he efficacy of STIR/SHAKEN is currently constrained by non-ubiquitous implementation").

[444] INCOMPAS Comments at 7-8 (arguing that "end-to end implementation of the STIR/SHAKEN framework among voice service providers . . . will have a significant impact in curtailing illegal robocalls which is critical to restoring consumer trust in the voice network"); *see also* Comcast Comments at 4-5 (asserting that "expanding STIR/SHAKEN obligations across the voice service ecosystem will benefit all parties and call recipients").

imposing these obligations "on more providers will promote fewer spoofed calls overall."[445] We anticipate that our expansion of the STIR/SHAKEN regime may spur other countries and regulators to develop and adopt STIR/SHAKEN, further increasing the standards' benefit. We seek comment on this analysis and on the possible benefits of the requirement we propose. Are there reasons we should not require all intermediate providers to implement STIR/SHAKEN for SIP calls?[446] Should we specifically target providers that are most responsible for illegal robocalls?[447] Are there any downsides to only targeting specific providers?

165. We also seek comment on the proposal's implementation costs and burdens. Acknowledging that many intermediate providers are also gateway providers to some degree and are now required to implement STIR/SHAKEN per today's *Order*, do the benefits of an intermediate provider authentication requirement outweigh the costs and burdens? Certain commenters assert that gateway providers are in a unique position to "arrest the flow of harmful scam calls and illegal robocalls."[448] Would it be a greater burden to impose this obligation on non-gateway intermediate providers? Indeed, a majority of commenters oppose expanding authentication requirements, even to gateway providers, saying that the implementation costs would be significant without additional benefits.[449] While the Commission previously acknowledged these claims and "thus offer[ed] an alternative method of compliance,"[450] it further noted that "[p]roviding this option . . . further allows for continued evaluation of the role intermediate providers play in authenticating the caller ID information of the unauthenticated calls that they receive amid the continued deployment of the STIR/SHAKEN framework."[451] Has the intervening experience with the entirety of the Commission's caller ID authentication requirements and illegal robocalls shed further light on the role of intermediate providers in preventing these calls from reaching consumers?

166. We do not anticipate that our proposal to expand this requirement to the remaining intermediate providers will be unusually costly or unduly burdensome compared to gateway providers and voice service providers that are already required to authenticate unauthenticated SIP calls as commenters have not provided detailed support for assertions that such a requirement will cost significant time and resources to implement.[452] Further, many of the remaining intermediate providers are also gateway providers[453] that will have already implemented STIR/SHAKEN in at least some portion of its network, likely lowering its compliance costs to meet the requirement we propose.[454] Does this fact undercut the argument that expanding the authentication requirement would impose an undue burden on those providers? In the accompanying *Order*, we find that the benefits of a gateway authentication requirement outweigh the burdens. Should our rationale differ regarding the remaining intermediate providers? We reiterate that as more and more providers implement STIR/SHAKEN, we anticipate that technology and solutions will be more widely available and less costly to implement. We seek comment on this analysis. Is there any reason to believe that authentication is more costly for the remaining intermediate providers as compared to other providers or that the benefit of lower-level attestations would

[445] T-Mobile Comments at 3.

[446] *See, e.g.*, USTelecom Mar. 3 *Ex Parte* at 1.

[447] *See id.* at 2.

[448] *See, e.g.*, NCLC and EPIC Reply at 4-5.

[449] *See* USTelecom Comments at 11; iBasis Comments at 6; i3forum Comments at 5; Verizon Reply at 17.

[450] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1928, paras. 144-45.

[451] *Id.* at 1928, para. 146.

[452] *See, e.g.*, T-Mobile Feb. 2 *Ex Parte* at 3-4; *see also* Section III.D.

[453] *See, e.g.*, iBasis Comments at 13; Belgacom Comments at 3; CTIA Comments at 11.

[454] *See* 51 State AGs Reply at 5.

be limited?

167. *Requirement*. We propose that to comply with the requirement to authenticate calls, all intermediate providers must authenticate caller ID information for all SIP calls they receive with U.S. numbers in the caller ID field for which the caller ID information has not been authenticated and which they will exchange with another provider as a SIP call. This would replace the existing rule under which intermediate providers have the option to authenticate rather than cooperate with traceback efforts[455] and supplement the rule for gateway providers we adopt in the accompanying *Order*. We seek comment on this approach, as well as on whether and how to modify this proposal.

168. Consistent with our existing intermediate provider authentication obligation where such a provider chose the authentication route, and the rule adopted for gateway providers in the accompanying *Order*, we propose that an intermediate provider satisfies its authentication requirement if it adheres to the three ATIS standards that are the foundation of STIR/SHAKEN—ATIS-1000074, ATIS-1000080, and ATIS-1000084—and all documents referenced therein.[456] We also propose that compliance with the most current versions of these standards as of the compliance deadline set in the *Order* released pursuant to this *Further Notice*, including any errata as of that date or earlier, represents the minimum requirement to satisfy our rules.[457]

169. *Compliance Deadline*. We seek comment on when we should require all intermediate providers' authentication obligation to become effective, balancing the public interest of prompt implementation by these providers with the need for these providers to have sufficient time to implement our proposed obligations. We note that voice service providers were previously able to meet the 18-month deadline to authenticate all unauthenticated SIP calls carrying U.S. NANP numbers, but we found a shorter deadline to be reasonable for gateway providers in the accompanying *Order*.[458] Should we require all intermediate providers to authenticate all unauthenticated SIP calls carrying U.S. NANP numbers within six months after we adopt an order released pursuant to this *Further Notice*?[459] Given that there is only a small group of remaining providers that have not already been required to implement STIR/SHAKEN, can implementation be accomplished in six months?[460] Is a shorter deadline reasonable because the industry has much more experience with implementation than when we originally required voice service providers to implement STIR/SHAKEN, and there is evidence that STIR/SHAKEN implementation costs have dropped since we first adopted the requirement for voice service providers?[461] Would imposing a shorter deadline on all intermediate providers unnecessarily impose greater costs and burdens that would not be fully offset by associated benefits? Are there any reasons to impose a longer

[455] 47 CFR § 64.6302(b). As noted above, the call blocking rules have mooted this choice.

[456] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1926-27, paras. 142-43; *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3258-59, para. 36.

[457] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1926-27, paras. 142-43; *First Caller ID Authentication Report and Order and Further Notice*, 36 FCC Rcd at 3258-59, para. 36.

[458] *See* TRACED Act, Public Law 116-105—Dec. 30. 2019, § 4(b) (requiring the Commission to require voice service providers to implement STIR/SHAKEN, subject to exceptions, "not later than 18 months after the date of the enactment of this Act"); *Gateway Provider Notice* at para. 48. Our rules adopted pursuant to the TRACED Act grant certain providers exemptions and extensions from this deadline. *See* 47 CFR § 64.6304 (granting extensions to various classes of providers, including "small" voice service providers); *id.* § 64.6306 (establishing a process to obtain an exemption).

[459] *See* INCOMPAS Comments at 8 (agreeing with the Commission's 18-month deadline).

[460] *See* 51 State AGs Reply at 4-6 (arguing that the obligation should become effective within 30 days of the publication of the order in the Federal Register). *But see* Belgacom International Carrier Services Comments at 3 (suggesting a longer deadline).

[461] *See supra* Section III.D; *see also* 51 State AGs Reply at 4-6.

deadline?

170. We also anticipate that the current token access policy will not present a material barrier to intermediate providers meeting their authentication obligation and that the STI-GA can address any concerns before these providers are required to authenticate calls. Do commenters agree? Additionally, to ensure that these providers are not unfairly penalized and are eligible for the same relief, in line with our current rules for voice service providers, and now gateway providers, we propose to provide a STIR/SHAKEN extension to intermediate providers that are unable to obtain a token due to the STI-GA token access policy.[462] Does this extension alleviate implementation concerns?

171. We also propose, consistent with our requirement for voice service providers and gateway providers, that all intermediate providers have the flexibility to assign the level of attestation appropriate to the call based on the applicable version of the standards and the available call information. As discussed in the accompanying *Order*, there are significant benefits to be gained from higher attestation levels.[463] We seek comment on this proposal. Should we modify this proposal? If so, how should we change it and what would be the impacts on costs and benefits?

172. *Authentication Obligations for All Providers*. We also seek comment on requiring all providers to comply with the current version of the STIR/SHAKEN standards (ATIS-1000074, ATIS-1000080, and ATIS-1000084) and any other IP authentication standards adopted as of the compliance deadline. We conclude that mandating a single version of the standards across providers will promote uniformity and ensure that providers are using the most up-to-date caller ID authentication tools. We seek comment on this conclusion. Is there any reason we should not require providers to comply with updated versions of the standards? We also seek comment on a streamlined mechanism for the Wireline Competition Bureau or other appropriate Bureau to require providers to comply with future versions of the STIR/SHAKEN standard as they are developed and made available. Should we delegate to the Wireline Competition Bureau authority to require all providers to implement a newly available updated standard through notice and opportunity to comment?[464] Should we incorporate the most recent STIR/SHAKEN standards and any updates we require in our rules?[465] What are the pros and cons of these approaches?

173. We seek comment on whether we should require all providers to adopt a non-IP caller ID authentication solution.[466] A number of commenters filed specific proposals in the record for authentication on non-IP networks for gateway providers as well as voice service providers, and some of these solutions work on both IP and non-IP networks.[467] Should we adopt any of these proposals as set forth in the comments or in some modified form? What are the respective benefits and burdens of these specific proposals? Should we adopt any of the TDM call authentication solutions developed by ATIS?[468]

---

[462] *See* 47 CFR § 64.6304(b).

[463] *Supra* Section III.D; *see also* Comcast Comments at 6.

[464] *See, e.g.*, 47 CFR § 20.19(k)(1) (delegating authority for adoption of ANSI C63 standards for wireless handset hearing-aid-compatibility "provided that the standards do not impose with respect to such frequency bands and air interfaces materially greater obligations than those impose on other services subject to this section").

[465] *See, e.g.*, 47 CFR § 20.19(1) (incorporating by reference ANSI standards for wireless handset hearing-aid-compatibility into the rules).

[466] *Gateway Provider Notice* at para. 46.

[467] *See* Twilio Comments at 5; TransNexus Comments at 2, 4; iconectiv Comments at 2; SipNav Comments at 2; AB Handshake Comments at 5; TransNexus Reply at 4.

[468] *See* ATIS-1000097, Technical Report on Alternatives for Call Authentication for Non-IP Traffic (Jul. 2021), https://access.atis.org/apps/group_public/download.php/60536/ATIS-1000097.pdf; ATIS-1000096, Signature-based Handling of Asserted information using toKENs (SHAKEN): Out-of-Band PASSporT Transmission Involving (continued….)

Are there any other alternative proposals that we should consider for all domestic providers in the call path? Should we require compliance with the most recent version of a non-IP standard available at the time an order is released pursuant to this *Further Notice*? Should we delegate authority to the Wireline Competition Bureau or other Bureau to require compliance with newly available versions of the adopted standard through notice and comment and incorporate by reference that standard in our rules? Voice service providers and gateway providers currently have a choice whether to implement a non-IP caller ID authentication solution or, in the alternative, participate with a working group, standards group, or consortium to develop a solution.[469] In the event we move forward with requiring a non-IP solution for all providers, we seek comment on eliminating this alternative obligation as moot because the selected standard would have been developed and its implementation required.

B. Extending Certain Mitigation Duties to All Domestic Providers

174. We seek comment on broadening the classes of providers subject to certain mitigation obligations, including some of the obligations we adopt in the accompanying *Order* for gateway providers. Our existing rules, including the "reasonable steps" robocall mitigation duty, the Robocall Mitigation Database certification and mitigation program adoption and submission requirements,[470] and the affirmative obligations for providers,[471] do not currently apply to all domestic providers, with the exception of the requirement to respond to traceback.[472] Prior to the adoption of today's *Order*, the "reasonable steps" mitigation duty and the requirement to adopt and submit a mitigation plan and certification applied only to originating providers, and the mitigation duty and plan submission requirements only applied to the extent that those providers had not yet fully implemented STIR/SHAKEN.[473] Similarly, the rules that require effective mitigation or blocking following Commission notification require any provider that receives such a notification to investigate and respond to the Commission, but only requires originating and gateway providers to take specific action to prevent illegal traffic.[474]

175. In the accompanying *Gateway Provider Report and Order*, we adopt several new or enhanced robocall mitigation obligations for gateway providers, as well as one for providers immediately downstream in the call path from the gateway provider.[475] We also extend the robocall mitigation program and certification requirements to gateway providers, regardless of whether they have implemented STIR/SHAKEN. Once the rules we adopt today become effective, some providers will

---

TDM Networks (Jul. 2021), https://access.atis.org/apps/group_public/download.php/60535/ATIS-1000096.pdf; ATIS-1000095, Extending STIR/SHAKEN over TDM (June 2021), https://access.atis.org/apps/group_public/download.php/60331/ATIS-1000095.pdf; *see also* TransNexus Comments at 4; Twilio Comments at 5; TransNexus Reply at 4 (all acknowledging ATIS' adoption of a TDM authentication solution).

[469] 47 CFR § 64.6303.

[470] *Id.* § 64.6305(a).

[471] *Id.* § 64.1200(n)(1)-(2).

[472] *Id.* § 64.1200(n)(1).

[473] *Id.* § 64.6305(a) (stating "(1) Any voice service provider subject to an extension granted under 47 CFR 64.6304 that has not fully implemented the STIR/SHAKEN authentication framework on its entire network shall implement an appropriate robocall mitigation program . . . (2) Any robocall mitigation program implemented pursuant to paragraph (a)(1) of this section shall include reasonable steps to avoid originating illegal robocall traffic"). However, all voice service providers, regardless of whether they have implemented STIR/SHAKEN, must submit a certification to the Robocall Mitigation Database. *Id.* § 64.6305(b).

[474] *Id.* § 64.1200(n)(2); *supra* paras. 75-77.

[475] *See supra* Section III.E.

remain outside the scope of these requirements. To close this loophole,[476] we seek comment on requiring *all* domestic providers, regardless of whether they have implemented STIR/SHAKEN, to comply with certain robocall mitigation requirements.

1. Enhancing the Existing Affirmative Obligations for All Domestic Providers

176. In the *Fourth Call Blocking Order*, the Commission adopted three affirmative obligations for providers to better protect consumers from illegal calls.[477] In the accompanying *Order*, we enhanced two of these obligations for gateway providers and adopted a related know-your-upstream-provider requirement. Here, we seek comment on expanding two of those enhanced obligations, as well as enhancing the existing requirement for a provider to take affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls.

177. *24-hour Traceback Requirement*. We seek comment on extending the requirement to respond to traceback requests from the Commission, civil and criminal law enforcement, and the industry traceback consortium within 24 hours of receipt of the request to all U.S.-based providers in the call path. In today's *Order* we require gateway providers to respond to traceback requests within 24 hours due to the need for quick responses when foreign providers are also involved. Would requiring all domestic providers to respond within 24 hours provide additional benefit? Are there alternative reasons to require a 24-hour response when calls are wholly domestic?

178. If we extend this requirement to cover all U.S-based providers in the call path, how should we address situations where providers may not be able to respond within 24 hours? We recognize that providers that do not receive many requests may be less familiar with the process, and that smaller providers in particular may struggle to respond quickly. Are there alternative approaches to our standard waiver process that would better address the needs of providers that cannot reliably respond within 24 hours?

179. In particular, we seek comment on whether we should adopt an approach to traceback based on volume of requests received, rather than position in the call path or size of provider. For example, should we adopt a tiered approach that: requires providers with fewer than 10 traceback requests a month to respond "fully and in a timely manner," without the need to respond within 24 hours; requires providers that receive from 10 to 99 traceback requests a month to maintain an average 24-hour response time; and requires providers with 100 or more traceback requests a month to always respond within 24 hours, barring exceptional circumstances that warrant relief through a waiver under the "good cause" standard of section 1.3 of our rules?[478] Would different thresholds be more appropriate for the tiers? Should the thresholds be based on the prior six months' average number of traceback requests or some other metric?

180. We believe that, at least with regard to smaller providers, the number of requests received is indicative of whether a particular provider contributes significantly to the illegal call problem. We seek comment on this belief. Are there instances where a smaller provider might receive a high volume of traceback requests despite that provider being a good actor in the calling ecosystem? We acknowledge that adopting requests-per-month thresholds will likely mean that larger providers will be required to respond within 24 hours even when those providers are good actors. However, we believe that larger providers are well positioned to meet a 24-hour response requirement and, in fact, already generally do

[476] *See* USTelecom Comments at 3 (explaining "[t]he loophole currently breaks the 'chain of trust' between the origination point of the call and the termination point, inviting services providers that are not known to the Commission and not committed to stopping illegal robocalls to routinely send traffic to U.S. consumers").

[477] *See* 47 CFR § 64.1200(n)(1)-(3); *Fourth Call Blocking Order*, 35 FCC Rcd at 15226-33, paras. 14-36.

[478] These circumstances could include sudden unforeseen circumstances that prevent compliance for a limited period or for a limited number of calls. We caution that any applicant for waiver "faces a high hurdle even at the starting gate." *WAIT Radio v. FCC*, 418 F.2d 1153, 1159 (D.C. Cir. 1969), *cert. denied*, 409 U.S. 1027 (1972).

so. We seek comment on this belief. Are there any substantial cost issues or other issues we should consider in adopting such a requirement?

181. *Blocking Following Commission Notification.* We seek comment on requiring all domestic providers in the call path to block, rather than simply effectively mitigate, illegal traffic when notified of such traffic by the Commission, regardless of whether that traffic originates abroad or domestically. We believe that having a single, uniform rule may provide additional benefits and reduce the overall burden. We seek comment on this belief. Are there benefits to having a single, uniform requirement for all domestic providers? Alternatively, are there benefits to maintaining our existing approach and allowing non-gateway providers to effectively mitigate, rather than block, such traffic?

182. If we extend this requirement and require non-gateway providers to block, should we consider any modifications to the rule? Our effective mitigation rule requires a different response if the provider is an originating provider than if the provider is an intermediate or terminating provider. Specifically, the originating provider *must* effectively mitigate the traffic, while an intermediate or terminating provider must only notify the Commission of the source of the traffic and then, if possible, take steps to mitigate the traffic.[479] As a result, there are four possible ways in which we could enhance this rule: 1) we could require all providers, regardless of position in the call path, to block illegal traffic when notified of such traffic by the Commission; 2) we could requiring originating providers to block traffic when notified by the Commission, but only require intermediate and terminating providers to effectively mitigate that traffic; 3) we could require originating providers to block illegal traffic when notified, but only require intermediate and terminating providers to identify the source of the traffic and, if possible, block; or 4) we could require originating providers to effectively mitigate illegal traffic, and require intermediate and terminating providers to block. In all of these cases, gateway providers would be required to block consistent with the rule we adopt in the *Order*.[480] Are there particular benefits to any of these approaches? Are there any other approaches we could take? Are there any cost difficulties or other issues we should consider?

183. *Effective Measures to Prevent New and Renewing Customers from Originating Illegal Calls*. We seek comment on whether, and if so how, we should further clarify our rule requiring providers to take affirmative, effective measures to prevent new and renewing customers from using their network to originate illegal calls.[481] In the *Fourth Call Blocking Order*, we allowed providers flexibility to determine how best to comply with this requirement.[482] Should we now modify this approach? If so, what steps should we require providers to take with regard to their customers? If we should maintain our flexible approach, is there value in providing further guidance as to how providers can best comply? If so, what might this guidance include? Should we extend a similar requirement to all providers in the call path, in place of or in addition to our existing requirement.[483]

184. We seek comment on requiring originating providers to ensure that customers originating non-conversational traffic[484] only seek to originate lawful calls. For example, should we require

---

[479] *See* 47 CFR § 64.1200(n)(1)-(3); *Fourth Call Blocking Order*, 35 FCC Rcd at 15226-33, paras. 14-36.

[480] *Supra* paras. 75-77.

[481] 47 CFR § 64.1200(n)(3).

[482] *Fourth Call Blocking Order*, 35 FCC Rcd at 15232-33, paras. 32-36.

[483] *See* NCLC and EPIC Feb. 10 *Ex Parte* at 5.

[484] ZipDX has specifically urged us to focus on non-conversational traffic, and to treat it separate from conversational traffic, which it argues should flow unimpeded. ZipDX Reply at 8; *see also* ZipDX Comments at 2, 38; Letter from David Frankel, CEO, ZipDX LLC, to Marlene Dortch, Secretary, Federal Communications Commission, CG Docket No. 17-59, WC Docket No. 17-97 (filed Apr. 19, 2022) (ZipDX Apr. 19 *Ex Parte*). INCOMPAS has expressed concern and urged us to seek additional comment if we "intend to give further

(continued….)

originating providers to investigate such customers prior to allowing them access to high-volume origination services? If so, should we require originating providers to take certain, defined steps as part of this investigation, or allow flexibility? Should we require originating providers to certify, either in the Robocall Mitigation Database or through some other means, that they have conducted these investigations and determined that their customers are originating illegal calls? If a customer nonetheless uses an originating provider's network to place illegal calls, should we adopt a strict liability standard, or allow the provider to terminate or otherwise modify its relationship with the customer and prevent future illegal traffic?

185. ZipDX states that "non-conversational traffic" is "traffic that has an average call duration of less than two minutes."[485] We seek comment on this proposed definition. While some illegal calls are "conversational,"[486] many are not; we believe that stopping non-conversational illegal calls would significantly reduce the number of illegal calls consumers receive. We seek comment on this belief. Is a focus on non-conversational traffic appropriate, or should we maintain our broader focus on illegal calls generally? Alternatively, could we focus on both: maintaining our existing requirement as to illegal calls generally,[487] but adding enhanced obligations for non-conversational traffic?

186. We believe that originating providers, as the providers with a direct relationship to callers, are in the best position to know what traffic a caller seeks to originate. We seek comment on this belief. Is our focus on originating providers correct, or should we include other providers, such as intermediate providers, as ZipDX suggests?[488] If we include intermediate or terminating providers, should the requirement be the same, or modified? We note that there is wanted, and even important, non-conversational traffic. We do not want emergency alerts, post-release follow up calls by hospitals, credit card fraud alerts, or similar important communication to be prevented by an intermediate or terminating provider that is not comfortable with potential liability for carrying non-conversational traffic. How could we tailor our rules to allow this traffic to continue while still preventing illegal non-conversational traffic? Finally, we seek comment on alternative approaches. Should we adopt all or some of ZipDX's specific proposals, which would impose obligations across the network, including requiring providers that choose to accept non-conversational traffic to meet certain obligations such as requiring A-level attestation for such calls, limiting of transit routes for these calls, and Robocall Mitigation Database certification?[489] Are there any other approaches we should consider?

2. Downstream Provider Blocking

187. We seek comment on requiring intermediate and terminating providers to block traffic from bad-actor providers, regardless of whether or not the bad actor is a gateway provider, pursuant to the Commission notification process we adopt in this *Order* for providers downstream from the gateway.[490] As discussed above, we do not currently require any providers other than gateway or originating providers to block or effectively mitigate illegal traffic when notified by the Commission. In the *Order* we further

---

consideration to these proposals." Letter from Christopher L. Shipley, Attorney & Policy Advisor, INCOMPAS, to Marlene H. Dortch, Secretary, FCC, CG Docket No. 17-59, WC Docket No. 17-97, at 2 (filed Apr. 25, 2022).

[485] ZipDX Apr. 19 *Ex Parte* at 9.

[486] For example, one scam commonly targets grandparents; the caller poses as a grandchild or other family member in trouble, to obtain money from the victim. *See* The Office of Minnesota Attorney General Keith Ellison, *Scams Targeting Grandparents*, https://www.ag.state.mn.us/consumer/publications/grandparentscams.asp#:~:text=How%20the%20Scam%20Works,to%20pose%20as%20the%20grandchild. (last visited Apr. 27, 2022).

[487] 47 CFR § 64.1200(n)(3).

[488] *See*, *e.g.*, ZipDX Reply; ZipDX Apr. 19 *Ex Parte*.

[489] ZipDX Reply at 6-15; ZipDX Apr. 19 *Ex Parte*.

[490] *See supra* Section III.E.2.a.

require the intermediate or terminating provider immediately downstream to block all traffic from the identified provider when notified by the Commission that the gateway provider failed to block.[491] There is also an existing safe harbor for any provider to block traffic from a bad-actor provider.[492] We are concerned that the lack of consistency across all provider types could allow for unintended loopholes and we believe that having a single, uniform rule may provide additional benefits and reduce the overall burden. We seek comment on this belief. Are there any situations where we should not require downstream providers to block all traffic from a bad-actor provider that has failed to meet its obligation to block or effectively mitigate? For example, if we require originating providers to block calls upon Commission notification, but only require intermediate and terminating providers to effectively mitigate such traffic, should our downstream provider blocking rule treat the originating provider for that traffic differently from an intermediate provider? If so, how? Are there risks to expanding this requirement to cover all domestic providers? If so, do the benefits justify these risks and their associated costs? If not, should we take another approach to ensure that bad-actor providers cannot continue to send illegal traffic to American consumers? If we extend the requirement, should we use the process described in the *Order* or modify that process in some way?[493] Are there any other issues we should consider?

3. General Mitigation Standard

188. In line with the rule for voice service providers that have not implemented STIR/SHAKEN due to an extension or exemption and the general mitigation standard we adopt today for gateway providers, in addition to specific mitigation requirements for which we seek comment above, we propose to extend a general mitigation standard to voice service providers that have implemented STIR/SHAKEN in the IP portions of their networks and to all intermediate providers.[494] This standard would be the general duty to take "reasonable steps" to avoid originating or terminating (for voice service providers) or carrying or processing (for intermediate providers) illegal robocall traffic.[495] This obligation would include filing a mitigation plan along with a certification in the Robocall Mitigation Database.[496] In line with our rules for voice service providers and the rules we adopt for gateway providers in the accompanying *Order*, we propose that such a plan is "sufficient if it includes detailed practices that can reasonably be expected to substantially reduce the origination [or carrying or processing] of illegal robocalls."[497] We also propose that a program is insufficient if a provider "knowingly or through negligence" serves as the originator or carries or processes calls for an illegal robocall campaign.[498] Similar to our reasoning related to gateway providers, we anticipate that a general mitigation obligation on all domestic providers would serve as "an effective backstop to ensure robocallers cannot evade any granular requirements we adopt."[499] Are there reasons we should not extend to all domestic providers the

[491] *Supra* paras. 78-79.

[492] 47 CFR § 64.1200(k)(4).

[493] *Supra* Section III.E.2.a.

[494] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1899-900, paras. 76-78; 47 CFR § 64.6305(a); Verizon Reply at 12 (supporting meaningful robocall mitigation on all classes of providers, rather than "just picking one class of intermediate provider").

[495] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1899, para. 76.

[496] *See id.* at 1899-900, paras. 76-78; *Gateway Provider Notice* at para. 91.

[497] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1900, para. 78; *infra* Appx. A, § 64.6305; *see also Gateway Provider Notice* at para. 91.

[498] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1900, para. 78; *infra* Appx. A, § 64.6305; *see also Gateway Provider Notice* at para. 91.

[499] *Gateway Provider Notice* at para. 91; *see* CTIA Comments at 8-9 (explaining that the Commission can "leverage its current requirement on all U.S. providers . . . to effectively mitigate illegal traffic when notified by the (continued….)

same general mitigation standard we adopt in the accompanying *Order*?[500] Should we alter the general mitigation standard for all remaining providers in any way? If so, what should those modifications be?

189. We anticipate that extending these requirements to all domestic providers would ease administration because U.S.-based providers would then be subject to the same obligations for all calls, regardless of the providers' respective roles in the call path.[501] Regulatory symmetry would obviate the need for a carrier to engage in a call-by-call analysis to determine the role the provider plays for any given call—e.g., an intermediate provider may serve as a gateway provider for some calls but not for others[502]—and "ensure the accountability of all providers that touch calls to U.S. consumers, regardless of whether they originate, serve as the gateway provider, or simply [carry or process] illegal robocalls."[503] Are there additional benefits of imposing these requirements on all domestic providers? Are there any significant burdens if we impose these requirements on all domestic providers?

190. For the same reasons we describe in the accompanying *Gateway Provider Report and Order*,[504] we propose adopting the "reasonable steps" standard for providers that have implemented STIR/SHAKEN in the IP portions of their networks rather than a standard building upon the obligation for providers to mitigate traffic by taking "affirmative, effective measures to prevent new and renewing customers from using their network to originate illegal calls" adopted in the *Fourth Call Blocking Order*.[505] Regardless, under the current rules and the rules we adopt today, providers must still comply with the requirements to know the upstream provider[506] or to take affirmative, effective measures to prevent new and renewing customers from using the network to originate illegal calls,[507] as applicable, and steps a provider takes to meet one standard could meet the other, and *vice versa*.

191. *Strengthening the Definition of "Reasonable Steps."* Rather than encouraging providers to regularly consider whether their current measures are effective and make adjustments accordingly to comply with the "reasonable steps" standard, we seek comment on whether we should instead define "reasonable steps" to require all domestic providers to take specific mitigation actions.[508] What would

---

Commission"); 51 State AGs Reply at 11-12 (supporting a general mitigation standard and agreeing with the Commission's analysis); NCLC and EPIC Reply at 6 (asserting providers should have flexibility in their robocall mitigation methods).

[500] *See, e.g.*, T-Mobile Feb. 2 *Ex Parte* at 3. To the extent providers' networks are non-IP based, we recognize that they do not currently have an obligation to implement STIR/SHAKEN and thus already have an existing mitigation requirement.

[501] *See* USTelecom Comments at 2-4; CTIA Comments at 6-7; Twilio Comments at 3; iBasis Comments at 13; T-Mobile Comments at 5-6; USTelecom Reply at 2; Verizon Reply at 5-6.

[502] Some commenters have asserted this is very difficult and burdensome. *See, e.g.*, Belgacom International Carrier Services Comments at 2; ZipDX Comments at 15-16; T-Mobile Comments at 4-5; *see also Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1930, para. 151.

[503] USTelecom Mar. 3 *Ex Parte* at 1-2.

[504] *See supra* Section III.E.4.

[505] *Fourth Call Blocking Order*, 35 FCC Rcd at 15232, para. 32; *see also Gateway Provider Notice* at para. 92. We reiterate that the "affirmative, effective measures" standard does not apply to existing customers and focuses on call origination. *Gateway Provider Notice* at para. 92.

[506] *Supra* Sections III.E.2 and III.E.3.

[507] *See Fourth Call Blocking Order*, 35 FCC Rcd at 15232, paras. 32-33 (in support of the "affirmative, effective measures," noting that "[o]riginating and gateway voice service providers are best positioned to prevent illegal calls by stopping them before they enter the network" and that "[w]hen originating and gateway providers stop these calls in the first instance, it ensures that illegal traffic never enters the network").

[508] *See id.* at 5 (asserting that "prerequisites to get on and stay on the [Robocall Mitigation Database] should be expanded").

such a definition look like?[509] Is our standards-based approach sufficient?[510] If not, what, if any, are specific "reasonable steps" we can prescribe to avoid origination, carrying, and processing of illegal robocall traffic other than prohibiting providers from accepting traffic from providers that have not submitted a certification in the Robocall Mitigation Database or have been de-listed from the Robocall Mitigation Database pursuant to enforcement action.?

192. Certain commenters assert that more prescriptive rules will ensure that providers take reasonable steps to stop illegal robocalls.[511] For example, should we require traffic monitoring for upstream service or any other specific type of traffic monitoring?[512] Should any particular traffic monitoring metrics be used?[513] Should providers be required to take any other specific actions to show compliance with their robocall mitigation plan to meet this standard?[514] Should there be a higher burden for VoIP providers to meet the "reasonable steps" standard?[515] If so, what would such a higher burden look like? Are other specific modifications to the "reasonable steps" standard appropriate?

193. We believe it is important to close any existing loopholes and ensure that all domestic providers are subject to the same requirements regardless of their place in the call path, even though the Commission previously declined to follow a "one-size-fits-all" approach to mitigation.[516] We believe the benefits of such an approach would outweigh any burdens on providers.[517] Are these expectations correct? What are the benefits of clarifying and expanding our requirements to all domestic providers? What are the costs or burdens associated with doing so?

194. *Compliance Deadline.* We seek comment on an appropriate deadline for all domestic providers not covered by the existing requirements for voice service providers or the requirements we adopt today for gateway providers to comply with the proposed "reasonable steps" standard. Would 30 or 60 days after the effective date of any order we may adopt imposing this requirement on these providers be sufficient? Are there any reasons we should subject any remaining providers to a longer or shorter deadline? We seek comment on an appropriate deadline that is consistent with the time and effort necessary to implement the standard, balanced against the public benefit that will result in rapid implementation of the standard. What, if any, are the benefits and drawbacks of a shorter deadline?

---

[509] *See* USTelecom Comments at 4-6; CTIA Comments at 12-13; Twilio Comments at 4; USTelecom Reply at 2-5; Verizon Reply at 5-6; NCLC and EPIC Feb. 10 *Ex Parte* at 5.

[510] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1901-02, para. 81 (explaining that, if the Commission determined that its standards-based approach was not sufficient, it would "not hesitate to revisit the obligations we impose through rulemaking at the Commission level").

[511] NCLC and EPIC Feb. 10 *Ex Parte* at 5.

[512] *See* Verizon Reply at 6: *see also* CTIA Comments at 12-13; Twilio Comments at 4; USTelecom Reply at 4 (asserting the record supports the proposition that providers undertake at least a basic level of vetting of the providers from whom they directly accept traffic).

[513] Verizon Reply at 6-7; *see also* iBasis Reply at 6 (arguing a reasonable mitigation plan would involve "the monitoring of high volume traffic for foreign calls using NANPA numbers").

[514] *See* USTelecom Comments at 4-5 (arguing that providers should also include in a robocall mitigation plan the process and the actions they take when they are notified by other providers, the Commission, or the traceback consortium regarding illegal traffic on their network); *see also* iBasis Reply at 6 (noting a reasonable mitigation plan would include "promptly investigating suspicious traffic and responding to traceback requests, and taking affirmative action, including blocking traffic when it determines such action is appropriate to stop the influx of identified illegal calls"); USTelecom Reply at 4.

[515] NCLC and EPIC Feb. 10 *Ex Parte* at 5.

[516] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1901, para. 80.

[517] *See, e.g.*, CTIA Comments at 6-8; T-Mobile Comments at 5; USTelecom Comments at 2-4.

What, if any, are the benefits and drawbacks of a longer deadline?

4. Robocall Mitigation Database

195. *Robocall Mitigation Database Filing Obligation*. In line with the requirement we adopt today for gateway providers, we propose to require all intermediate providers[518] to submit a certification to the Robocall Mitigation Database describing their robocall mitigation practices and stating that they are adhering to those practices, regardless of whether they have fully implemented STIR/SHAKEN. We also propose to require voice service providers that have already filed a certification to submit a robocall mitigation plan to the extent they previously were not required to do so due to fully implementing STIR/SHAKEN.[519]

196. We propose to conclude that certification, operating in conjunction with the previous rules and new robocall mitigation obligations we adopt today, would encourage compliance and facilitate enforcement efforts and industry cooperation to address problems. A number of commenters recommended this proposal.[520] Similar to our findings for gateway providers above, we do not anticipate that a filing requirement would be more costly for other providers than it is for voice service providers that already have an obligation to file in the Robocall Mitigation Database. Are there reasons that all intermediate providers should not be required to submit a certification? Do the remaining providers face additional costs as compared to providers already subject to this requirement under the Commission's existing rules and the rule we adopt today that we should consider? Are there other possible filing obligations that we should impose instead of the requirement to file a certification in the Robocall Mitigation Database?

197. We also propose that all intermediate providers submit the same information that voice service providers, and now gateway providers, are required to submit under the Commission's rules. Specifically, we propose that all intermediate providers must certify to the status of STIR/SHAKEN implementation and robocall mitigation on their networks; submit contact information for a person responsible for addressing robocall mitigation-related issues; and describe in detail their robocall mitigation practices.[521] We propose that voice service providers that were not previously required to submit a robocall mitigation plan describe in detail their robocall mitigation practices.[522] Should these providers be subject to the additional obligation that we adopt for gateway providers in today's *Order*, i.e., should we require all domestic providers to explain what steps they are taking to ensure that the immediate upstream provider is not using their network to transmit illegal calls? Is it useful for all remaining providers to include this information? Should we modify the identifying information that all domestic providers must file (both providers with a current certification obligation and those without)?[523] We anticipate that the burden is limited if we do not adopt a requirement for how detailed this explanation must be. Are there any reasons we should require a more detailed explanation of the steps a provider has taken to meet their robocall mitigation obligations? Again, we anticipate the Commission and public will benefit from understanding how these providers choose to comply with this specific duty because

---

[518] As noted above, all intermediate providers previously were imported into the Robocall Mitigation Database from the rural call completion database's Intermediate Provider Registry. *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1904, para. 88 & n.340. We now propose to have these imported intermediate providers affirmatively file in the Robocall Mitigation Database.

[519] 47 CFR § 64.6305(b); *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1902-03, para. 82-85.

[520] *See* CTIA Comments at 7; iBasis Comments at 13; Twilio Comments at 3; USTelecom Comments at 2; ZipDX Comments at 32.

[521] 47 CFR § 64.6305.

[522] *Id.*

[523] *See, e.g.*, USTelecom Comments at 6; ZipDX Comments at 33; Verizon Reply at 4-5.

compliance is critical to stopping the carrying or processing of illegal robocalls.[524]

198. In line with our new rules applicable to gateway providers, we propose to delegate to the Wireline Competition Bureau the authority to specify the form and format of any submissions.[525] We further propose that this would include whether providers with more than one role in the call path may either submit a separate certification and plan or amend their current certification and any plan[526] and that providers amending their current plan to cover different roles in the call path explain the mitigation steps they undertake as one type of provider and what mitigation steps they undertake as a different type of provider, to the extent they are different.[527]

199. We also propose to extend to all domestic providers the duty to update their certification within 10 business days of "any change in the information" submitted, ensuring that the information is kept up to date, in line with the existing and new requirements for voice service providers and gateway providers, respectively.[528] Is another time period appropriate for some or all of the information we require? Should we establish a materiality threshold for circumstances in which an update is necessary for remaining providers, and, if so, what threshold should we set? In the *Gateway Provider Notice*, we sought comment regarding whether we should require gateway providers to inform the Commission through an update to the Robocall Mitigation Database filing if the provider is subject to a Commission, law enforcement, or regulatory agency action, investigation, or inquiry due to its robocall mitigation plan being deemed insufficient or problematic, or due to suspected unlawful robocalling or spoofing activity.[529] In the accompanying *Order*, we decline to adopt this proposal so that we may more broadly ask the question regarding all domestic providers. Thus, we now seek comment on this proposal for all domestic providers.

200. *Compliance Deadline.* We also seek comment on an appropriate deadline for all domestic providers to submit a certification and mitigation plan to the Robocall Mitigation Database attesting to compliance with the proposed "reasonable steps" standard. Is 30 days following publication in the Federal Register of notice of approval by OMB of any associated PRA obligations sufficient, as many intermediate providers are already required to mitigate call traffic? What are the benefits and drawbacks of a longer deadline? We seek comment on an appropriate deadline that is consistent with the time and effort necessary to implement this requirement, balanced against the public benefit that will result in rapid implementation of the requirement. If we adopt an earlier deadline than the requirement to implement STIR/SHAKEN, should we require that, if a provider has not yet implemented STIR/SHAKEN at that time, the provider must file its certification by the deadline and indicate that it has not yet fully implemented STIR/SHAKEN and that it then update the filing within 10 business days of

[524] USTelecom Comments at 5 (arguing that mitigation programs "should reflect at least a basic level of vetting of the providers from whom they directly accept traffic – beyond ensuring that they are registered in the [Robocall Mitigation Database]"); Verizon Reply at 6 (arguing that intermediate providers should describe in their robocall mitigation plans "the processes they follow to know the identities of the upstream service providers they accept traffic from and to monitor those service providers for illegal robocall traffic"), 7-8 (noting the types of robocall mitigation included in their contracts).

[525] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1902-03, para. 83; *Wireline Competition Bureau Announces Opening of Robocall Mitigation Database and Provides Filing Instructions and Deadlines*, WC Docket No. 17-97, Public Notice, 36 FCC Rcd 7394 (WCB, 2021).

[526] *See* USTelecom Comments at 6.

[527] *See id.*; ZipDX Comments at 32.

[528] *See* 47 CFR § 64.6305(b)(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 (b)(1) through (4) of this section.").

[529] *Gateway Provider Notice* at para. 97.

STIR/SHAKEN implementation, in line with our existing rule for updating such a filing?[530] Are there any other filing deadline issues we should consider? We seek comment on any modifications we should make to the filing process for these remaining providers.

201. *Additional Identifying Information*. While we sought comment in the *Gateway Provider Notice* on whether all Robocall Mitigation Database filers should submit additional identifying information,[531] we do not act on this issue in the accompanying *Order* so that we may both develop a more fulsome record at the same time we consider imposing other obligations on all domestic providers, including the obligation for all intermediate providers to file a certification in the Robocall Mitigation Database. We thus seek further comment on requiring all filers to include additional identifying information. While we sought comment in the *Gateway Provider Notice* on including information such as a Carrier Identification Code, Operating Company Number, and/or Access Customer Name Abbreviation,[532] is this information still relevant given that the September 2021 blocking deadline has now passed? Is there other additional information we should require? For example, we propose to require filers to add information regarding principals, known affiliates, subsidiaries, and parent companies. We seek comment on this proposal. Will such information help identify bad actors and further our enforcement efforts, such as by identifying bad actors previously removed from the Robocall Mitigation Database that continue to be affiliated with other entities filing in the Robocall Mitigation Database?[533] Will such information ease and enhance compliance by facilitating searches within the Robocall Mitigation Database and cross-checking information within the Robocall Mitigation Database against other sources? If we require all domestic providers to submit additional identifying information, how long should providers already in the database have to update information, or should such a requirement be applied on a prospective-only basis? Does the benefit of additional information outweigh the burden of asking a high number of providers to refile? What are the benefits of a prospective-only approach? Would this approach still be beneficial if only some filers submitted this information? Are there any categories of filer, such as foreign voice service providers that use NANP resources that pertain to the United States in the caller ID field, that are unlikely to have this identifying information? If so, how should any new requirements address these filers? Should we require providers to submit information demonstrating that they are foreign or domestic, and should we modify our provider definitions to address this issue?[534] Alternatively, should we consider making the submission of this additional information voluntary to avoid a refiling requirement and account for filers that do not possess the information? Or would submission on a voluntary basis provide little benefit? If we require submission of additional information by some or all filers, what deadline for filing should we set?

202. We also seek comment on any potential changes we should make to the Robocall Mitigation Database to make the filing process easier for providers and to facilitate searches by the Commission. For example, should we allow providers who indicate they are "fully compliant with STIR/SHAKEN" to still submit additional information regarding their compliance (e.g., if they obtained their own token or if they are relying on another arrangement)? Should the database allow for any other explanations or voluntary information submissions? What other changes to the database or filing process

[530] *See* 47 CFR § 64.6305(b)(5).

[531] *Gateway Provider Notice* at para. 100.

[532] *Id.*

[533] *See infra* Section VI.C.

[534] *See* TNS May 11 *Ex Parte* at 2 (arguing that the Commission should clarify that the gateway provider definition will "include calls handed off to a U.S. carrier for termination, regardless of whether the interconnection point is in a U.S. facility, in a hub that the provider or an affiliate receives traffic from, or if the call is exchanged via an IP address of that carrier"); ZipDX May 2 *Ex Parte* at 1-4 (suggesting a modification to the definition of foreign voice service provider in 47 CFR § 64.6300 and additional clarifications to the definition of gateway provider); *see also* 47 CFR § 64.6300 (defining voice service provider, intermediate provider, and foreign voice service provider).

would make compliance easier or more efficient for providers? If revising a filing is burdensome, what steps can the Commission take to reduce that burden? Is the burden of requiring revisions outweighed by the benefits to be obtained from the additional information?

203. *Specific Areas to Be Described in Robocall Mitigation Plan*. We seek comment on whether a robocall mitigation program should be considered sufficient if it only "includes detailed practices that can reasonably be expected to significantly reduce the origination of illegal robocalls.[535] Does this requirement need to be further articulated? We seek comment on specific areas or topics to be described in the mitigation plan submitted to the Robocall Mitigation Database. What, if any, specific types of mitigation must be described in plans submitted to the database? For example, should providers be required to "describe with particularity" in their robocall mitigation plans the processes providers follow "to know the identities of the upstream service providers they accept traffic from and to monitor those service providers for illegal robocall traffic"?[536] That is, should we require all domestic providers to describe their "know-your-upstream provider" processes?[537] Should providers indicate whether they use analytics providers and/or describe the analytics they use? Should all domestic providers describe any contractual requirements for upstream providers? Should all domestic providers include "the process and the actions" they take when they "become aware of it, including when alerted of such traffic by the Commission or the traceback consortium" regarding illegal traffic on their network, as suggested by USTelecom?[538] Would taking any or all of these actions better protect U.S. consumers from illegal robocalls?[539]

204. *Certifications and Data from Intermediate Providers Previously Imported into the Robocall Mitigation Database.* We propose to delegate decisions regarding the certifications and data of intermediate providers previously imported into the Robocall Mitigation Database to the Wireline Competition Bureau, as we do for gateway providers that were previously imported into the database as intermediate providers in the accompanying *Order*. If we take this approach, should we provide any additional guidance to the Wireline Competition Bureau and what would such additional guidance look like? Some commenters indicate that intermediate providers previously imported into the Robocall Mitigation Database should only have to "supplement their [Robocall Mitigation Database] entry by submitting a mitigation plan without having to completely refile,"[540] while others assert that intermediate providers' imported data should be deleted from the database.[541] Should the Commission instead adopt one of these proposals and direct the Wireline Competition Bureau to remove or update these imported

---

[535] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1900, para. 78.

[536] *See* Verizon Reply at 6.

[537] *See id.* (stating that their "rating methodology continuously measures wholesaler and direct peer calling patterns over time and considers factors such as call duration, percentage of calls declined by the recipient, number of calls made using invalid numbers, calls originating from industry or government identified problematic providers, and illegal calls made to our expansive honeypot" and that they "actively monitors these metrics").

[538] USTelecom Comments at 4-5; *see also* iBasis Reply at 6.

[539] NCLC and EPIC Feb. 10 *Ex Parte* at 5 (explaining "[p]roviders can easily identify likely illegal calls through simple analytics, yet providers continue to accept these calls and pass them on to telephone subscribers" and "[s]uing or prosecuting the callers or the complicit providers one-by-one is an entirely inadequate strategy").

[540] *See* iBasis Reply at 6; *see also Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1902-05, paras. 82-89 & n.340.

[541] *See* USTelecom Comments at 6 (suggesting that the Commission remove from the Robocall Mitigation Database any provider currently in the database that was imported by the Commission as an intermediate provider); iBasis Reply at 6 n.27 ("The Commission should reject USTelecom's suggestion that the Commission remove from the [Robocall Mitigation Database] any provider currently in the database that was imported by the Commission as an intermediate provider. . . . Instead, intermediate providers, or at least those that are also gateway providers should supplement their filing with a mitigation plan.").

certifications and data from the database? What are the benefits and burdens of allowing these providers to update their data versus having them completely refile?

205. *Intermediate Provider Blocking Obligation*. We propose to require downstream providers to block traffic received directly from all intermediate providers that are not listed and have not affirmatively filed a certification in the Robocall Mitigation Database or have been removed through enforcement action. Doing so will close a loophole in our rules by ensuring that any provider's traffic will be blocked if its certification does not appear in the Robocall Mitigation Database. It will also obviate any concerns regarding how downstream providers can determine if an upstream provider is a voice service provider, gateway provider, or other domestic intermediate provider. There was record support for this approach, which will equalize treatment of all domestic providers.[542] We seek comment on doing so. What, if any, are the unique costs and benefits to applying this rule to domestic intermediate providers' traffic? Are there any modifications we should make when applying this rule to intermediate providers other than gateway providers? In the Order, we require downstream providers to block traffic from an immediate upstream provider where the upstream provider had not affirmatively filed in the Robocall Mitigation Database and they had a reasonable basis to believe that the immediate upstream provider was either a voice service provider or a gateway provider for some calls. We propose to eliminate this requirement as moot if we adopt the proposed requirement for downstream providers to block traffic from domestic intermediate providers that have not affirmatively filed in the Robocall Mitigation Database; downstream providers will no longer need to determine the upstream provider type before making a blocking determination. We seek comment on this approach.

206. We propose that downstream providers be required to block traffic from non-gateway intermediate providers that have not submitted a certification in the Robocall Mitigation Database 90 days following the deadline for intermediate providers to file a certification. This proposed deadline is consistent with both the rule we adopted in the accompanying *Order* and the rule for voice service providers. We seek comment on this proposal and whether an alternative deadline is appropriate.

C. Enforcement

207. Our rules are only as effective as our enforcement. To that end, we propose to: (1) impose forfeitures for failures to block calls on a per-call basis and establish a maximum forfeiture amount for such violations; (2) impose the highest available forfeiture for failures to appropriately certify in the Robocall Mitigation Database; (3) establish additional bases for removal from the Robocall Mitigation Database, including by establishing a "red light" feature to notify the Commission when a newly-filed certification lists a known bad actor as a principal, parent company, subsidiary, or affiliate; and (4) 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.

208. *Failure to Block Calls*. Mandatory blocking is an important tool for protecting American consumers from illegal robocalls. Penalties for failure to comply with our existing or newly adopted mandatory blocking requirements must be sufficient to ensure that entities subject to our mandatory blocking requirements suffer a demonstrable economic impact. Given that bad actors profit from illegal robocalls, we tentatively conclude that we should impose forfeitures for failure to block after Commission notice on a per-call basis. For example, if ABC Provider fails to block 100 calls, it will be subject to the maximum forfeiture amount for each of those 100 calls. We seek comment on this proposal. What are the pros and cons of our proposal? If adopted, should it be applicable to all domestic providers? Should we exclude certain types of mandatory blocking from this approach? For example, should we take a different approach for blocking based on a reasonable DNO list? Is there any reason why this last approach would be impracticable or unreasonable?

[542] *See, e.g.*, USTelecom Comments at 8; Verizon Reply at 5-6.

209. We propose to authorize that forfeitures for violations of our mandatory blocking rules be imposed on a per-call basis, with a maximum forfeiture amount for each violation of the proposed mandatory blocking requirements of $22,021 per violation. This is the maximum forfeiture amount our rules permit us to impose on non-common carriers.[543] While common carriers may be assessed a maximum forfeiture of $220,213 for each violation,[544] we propose to find that we should not impose a greater penalty on one class of providers than another for purposes of the mandatory blocking requirements. We seek comment on this proposal. Is there any reason to permit a higher maximum forfeiture for violation of the blocking requirements by providers that the Commission has determined to qualify as common carriers? Is one class of providers more likely than another to violate these rules? If so, is that a basis for imposing different forfeiture amounts? Are there particular aggravating or mitigating factors we should take into consideration when determining the amount of a forfeiture penalty? Are the aggravating and mitigating factors set forth in our rules sufficient?[545] Should failure to block calls to emergency services providers or PSAPs or to numbers on a reasonable DNO list constitute aggravating factors to be considered in calculating a forfeiture amount?

210. *Provider Removal from the Robocall Mitigation Database*. Our voice service provider rules provide that if the Commission "finds a certification is deficient in some way, such as if the certification describes a robocall mitigation program that is ineffective" or "that a provider nonetheless knowingly or negligently originates illegal robocall campaigns," the Commission "may take enforcement action as appropriate."[546] These enforcement actions may include, among others, removing a defective certification from the database after providing notice to the voice service provider and an opportunity to cure the filing.[547] We seek comment on whether intermediate providers (other than gateway providers), in addition to voice service providers and gateway providers, should be subject to the removal of provider certifications from the Robocall Mitigation Database.[548] Are there any other reasons we should de-list or exclude providers from the Robocall Mitigation Database?[549] We propose to expand our delegation of authority to the Enforcement Bureau codified in today's *Gateway Provider Report and Order* to de-list or exclude a provider from the Robocall Mitigation Database so that it applies to *all* providers. We seek comment on this proposal. Should we automatically exclude providers or start an enforcement action for providers that look suspicious due to multiple traceback requests?[550] Should we automatically remove a provider from the database for its prior illegal or bad actions related to and/or unrelated to robocalling? Should we automatically remove a provider from the database for bad actions by an affiliate provider related or unrelated to robocalling? What other provider actions would warrant removal from the Robocall Mitigation Database? Under our current rules, when a voice service provider is removed from the Robocall Mitigation Database, downstream providers must block that provider's traffic.[551] Should we deviate from this approach?[552]

---

[543] 47 CFR § 1.80(b)(9).

[544] *Id.* § 1.80(b)(2).

[545] *See id.* § 1.80(b)(10) tbl. 3.

[546] *Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1903, para. 83.

[547] *Id.* The Commission may, of course, impose a forfeiture in addition to removing the provider from the Robocall Mitigation Database.

[548] *See* ZipDX Comments at 32-33.

[549] NCLC and EPIC Feb. 10 *Ex Parte* at 5; *see also* USTelecom Comments at 9; NCLC and EPIC Reply at 12, 15-16.

[550] NCLC and EPIC Reply at 15-16; NCLC and EPIC Feb. 10 *Ex Parte* at 5.

[551] 47 CFR § 64.6305(c).

[552] *See* ZipDX Comments at 33.

211. *Continued violations*. We propose to find that individuals and entities that engage in continued violations of our robocall mitigation rules raise substantial questions regarding their basic qualifications to engage in the provision of interstate common carrier services.[553] We thus propose that such entities be subject to possible revocation of their section 214 operating authority, where applicable, and that any principals (either individuals or entities) of the bad actor entity be banned from serving, either directly or indirectly, as an attributable principal or as an officer or director 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. For purposes of any such revocation, we propose to define "attributable principal" as: (1) in the case of a corporation, a party holding 5% or more of stock, whether voting or nonvoting, common or preferred; (2) in the case of a limited partnership, a limited partner whose interest is 5% or greater (as calculated according to the percentage of equity paid in or the percentage of distribution of profits and losses); (3) in the case of a general partnership, a general partner; and (4) in the case of a limited liability company, a member whose interest is 5% or greater. We seek comment on these proposals and on any alternative proposals or attribution criteria. For purposes of the definition of "attributable principal," is 5% stock ownership or interest an appropriate threshold?[554] Would 10% stock ownership or interest or some lesser or higher threshold be more appropriate?

212. Many of the providers that would come within the purview of this proposed rule may not be classified as common carriers and thus may not operate subject to the blanket section 214 authority applicable to domestic interstate common carriers under section 63.01 of the Commission's rules.[555] Providers not classified as common carriers may hold other Commission-issued authorizations or certifications. We propose to find that such carriers that have an international section 214 authorization, have applied for and received authorization for direct access to numbering resources,[556] or are designated

[553] *See, e.g.*, *Kurtis J. Kintzel et al.; Resellers of Telecommunications Services*, EB Docket No. 07-197, Order to Show Cause and Notice of Opportunity for Hearing, 22 FCC Rcd 17197, 17197, para. 1 (2007).

[554] For purposes of determining foreign ownership limits under section 310(b)(4) of the Act (regarding common carrier wireless licenses or media licenses), an applicant must disclose any individual foreign investor or group acquiring a greater than 5% voting or equity interest in the licensee. 47 CFR § 1.991(i). This reflects "the Commission's longstanding determination, in both the broadcast and common carrier contexts, that a shareholder with a less than five percent interest does not have the ability to influence or control core decisions of the licensee." *Pandora Radio LLC*, 30 FCC Rcd 5094, 5101, para. 19 (2015) (citing *Review of Foreign Ownership Policies for Common Carrier and Aeronautical Radio Licensees under Section 310(b)(4) of the Communications Act of 1934, as Amended*, IB Docket No. 11-133, Second Report and Order, 28 FCC Rcd 5741, 5771, para. 54 (2013) (*Common Carrier Foreign Ownership Order*); *see also Review of Foreign Ownership Policies for Common Carrier and Aeronautical Radio Licensees under Section 310(b)(4) of the Communications Act of 1934, as Amended*, GN Docket No. 15-236, Report and Order, 31 FCC Rcd 11272, n.246 (2016) (citing *Common Carrier Foreign Ownership Order*, 28 FCC Rcd at 5771, para. 54 and stating, "The disclosure requirements of Section 13(d) of the Exchange Act also informed the Commission's decision in 1984 to establish a 5 percent voting stock interest as the benchmark amount for attributing ownership of a broadcast licensee's facilities to an individual corporate shareholder."); *Reexamination of the Commission's Rules and Policies Regarding the Attribution of Ownership Interests in Broadcast, Cable Television and Newspaper Entities*, MM Docket No. 83-46, Report and Order, 97 F.C.C. 2d 997, 1002-12, paras. 6-29 (1984) (establishing a 5 percent voting stock interest as the benchmark amount for attributing broadcast ownership based on the Commission's finding that, as a general rule, a stockholder with a smaller interest does not have the ability to influence or control core decisions of the licensee, regardless of whether the licensee is a widely held or closely held company); 47 CFR § 73.3555, Note 2a to § 73.3555 (codifying the 5 percent attribution standard).

[555] *See* 47 CFR § 63.01. Interconnected VoIP providers are required to file applications to discontinue service under section 214 of the Act and section 63.71 of the Commission's rules. *IP-Enabled Services*, WC Docket No. 04-36, 24 FCC Rcd 6039, 6044-47, paras. 9-13 (2009).

[556] *See Numbering Policies for Modern Communications et al.*, WC Docket No. 13-97 et al., Report and Order, 30 FCC Rcd 6839, 6878, para. 78 (2015), *appeal dismissed*, *NARUC v. FCC*, 851 F.3d 1324 (D.C. Cir. 2017).

as eligible telecommunications carriers under section 214(e) of the Act in order to receive federal universal service support[557] hold a Commission authorization sufficient to subject them to the Commission's jurisdiction for purposes of enforcing our rules pertaining to preventing illegal robocalls. Finally, we propose to find that providers not classified as common carriers registered in the Robocall Mitigation Database hold a Commission certification such that they are subject to the Commission's jurisdiction. We seek comment on these proposed findings and whether they serve as sufficient legal authority for the Commission to seek either revocation of an individual or entity's section 214 operating authority or to impose a ban on an individual or entity from operating in the telecommunications space as described above. Are there any other bases for jurisdiction or legal authority for the Commission to take such action?

D. Obligations for Providers Unable to Implement STIR/SHAKEN

213. We seek comment on whether additional clarity is needed regarding the Commission's rules applicable to certain providers lacking facilities necessary to implement STIR/SHAKEN. The Commission has previously clarified that the STIR/SHAKEN implementation requirement "do[es] not apply to providers that lack control of the network infrastructure necessary to implement STIR/SHAKEN."[558] In the time since, however, the Commission has granted certain providers extensions,[559] as well as established the Robocall Mitigation Database filing requirement.[560] Should the Commission further clarify to whom the STIR/SHAKEN implementation requirement does not apply?

214. Given that providers must block traffic from originating providers not listed in the Robocall Mitigation Database,[561] some providers, including resellers, have filed, irrespective of any obligation to do so. We observe that the Robocall Mitigation Database portal does not prevent these providers from filing. To address this issue, should the Commission amend its rules to deem providers that lack control of the necessary infrastructure to implement STIR/SHAKEN as instead having a continuing extension?[562] Our rules require that voice service providers granted an extension perform robocall mitigation.[563] Should the providers identified above be required to perform robocall mitigation, at least to the extent that they are able despite their lack of control over network infrastructure? If not, why not?

215. These providers may possess information about their customers that the underlying provider (in the case of resellers) may not be aware of or privy to. Should the Commission impose a know-your-customer obligation on these providers, even though they do not have an obligation to

---

[557] 47 U.S.C. § 251(e).

[558] *First Caller ID Authentication Report and Order and Further Notice*, 35 FCC Rcd at 3260, para. 40. We note that we accelerated the STIR/SHAKEN implementation deadline for another class of providers (i.e., non-facilities-based small voice service providers) in the *Small Provider Order*. *See Small Provider Order*, FCC 21-122 at 7-14, paras. 15-26. A provider is non-facilities-based if it "offers voice service to end-users solely using *connections* that are not sold by the provider or its affiliates." *Id*. at 9, para. 19 (emphasis added). We clarify that some "non-facilities-based" small providers may also meet the definition of a provider that does not have control of the necessary infrastructure to implement STIR/SHAKEN. If so, that provider does not have a STIR/SHAKEN implementation obligation. The *Small Provider Order* did not expand or contract the universe of providers required to implement STIR/SHAKEN on the IP portions of their network; it only accelerated the implementation deadline for a subset of providers already subject to an implementation obligation.

[559] *See* 47 CFR § 64.6304.

[560] *See id*. § 64.6305.

[561] *Id*. § 64.6305(c).

[562] *See id*. § 64.6304(d).

[563] *Id*. § 64.6305(a)(1).

implement STIR/SHAKEN,[564] or are our existing requirements outside of the STIR/SHAKEN context sufficient?[565] Is our existing flexible approach sufficient, or should the Commission impose more specific requirements? Should such providers be required to communicate relevant information about their customers to underlying providers, and to what extent?

E. Satellite Providers

216. We seek comment on whether the TRACED Act applies to satellite providers, and, if so, whether we should grant such providers an extension for implementing STIR/SHAKEN. Our rules, consistent with the TRACED Act, provide that a "voice service" is "any service that . . . furnishes voice communications to an end user using resources from the North American Numbering Plan."[566] The Satellite Industry Association (SIA) argues that our STIR/SHAKEN rules should not apply to satellite providers because their voice services do not satisfy the definition set out in our rules and in the TRACED Act. SIA asserts that their services "rely on non-NANP resources for their originating numbers" and that they use U.S. NANP resources only "to forward calls to a small satellite [provider] subscriber's non-NANP number, or direct assignment of NANP numbers to a very small subset of small satellite customers."[567] Does our authority under the TRACED Act extend to satellite providers that do not use NANP resources? Does our authority to require satellite providers to implement STIR/SHAKEN apply to all satellite providers regardless of the scope of the TRACED Act? What about to the extent any satellite providers use NANP numbers for the limited purposes described by SIA? Does use of NANP resources for forwarding calls to non-NANP numbers render that service a "voice service" within the TRACED Act's?[568] Do a *de minimis* number of satellite provider subscribers use NANP resources only as SIA describes above,[569] or are there ways these subscribers use NANP resources that SIA does not describe? Should there be a *de minimis* exception to our rules? If so, how should we define *de minimis* for this purpose?

217. In addition to satellite providers' apparently limited use of U.S. NANP resources that SIA argues is generally outside the scope of the TRACED Act, SIA contends that requiring implementation of STIR/SHAKEN would pose an undue hardship due to unique economic and technological challenges the industry faces.[570] Would requiring satellite providers, irrespective of their use of U.S. NANP resources, to implement STIR/SHAKEN pose an undue hardship? Is it technically feasible for satellite providers to implement STIR/SHAKEN? To what extent are satellite providers the source of illegal robocalls?[571] Do they account for enough of the $13.5 billion cost to American consumers to outweigh the burden on them posed by having to implement STIR/SHAKEN?[572] We have previously provided small voice services providers, including satellite providers, an extension from STIR/SHAKEN implementation until June 30, 2023.[573] When the Wireline Competition Bureau reevaluated this extension in 2021, it declined to grant a request from SIA for an indefinite extension and stated that it would seek further comment on SIA's

---

[564] *See id*. § 64.1200(n)(3) (requiring voice service providers to "[t]ake affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal traffic").

[565] *See id*.

[566] *See* 4 *id*. § 64.3000(m)(1).

[567] Satellite Industry Association Comments, WC Docket Nos. 20-68, 17-97, at 7 (filed. Nov. 12, 2021).

[568] *See id*. at 8-9.

[569] *See id*. at 9.

[570] *See id*. at 3-4, 7.

[571] *See id*. at 9-14 (contending that use of satellite providers for illegal robocalling "is highly unlikely").

[572] *See Gateway Provider Notice* at paras. 108-09.

[573] *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1877, paras. 41-42.

request before the June 30, 2023 extension expires.[574] We seek comment on whether we should grant SIA's request for an indefinite extension for satellite providers. In the alternative, should satellite providers be granted a continuing extension?[575] If so, how long should such an extension be?

F. Restrictions on Number Usage and Indirect Access

218. We seek comment on possible changes to our numbering rules to prevent the misuse of numbering resources to originate illegal robocalls, particularly calls originating abroad. In the *Direct Access Further Notice*, we sought comment placing limitations on interconnected VoIP providers' use of numbering resources obtained pursuant to direct access authorizations the Commission grants.[576] We now seek comment on whether we should implement broader limitations in order to prevent illegal robocalls and whether other countries' regulations may provide a useful roadmap for our own.

219. *Restrictions on Use of U.S. NANP Numbers for Foreign-Originated Calls*. We seek comment on whether we should adopt restrictions on the use of domestic numbering resources for calls that originate outside of the United States for termination in the United States. We note that, according to providers and foreign regulators, other countries, such as Singapore and South Korea, have placed limitations on the use of domestic numbering resources for foreign-originated calls that terminate domestically.[577] Australia has a similar rule.[578] Should we adopt a similar restriction? Should we, as

---

[574] *See Wireline Competition Bureau Reevaluates STIR/SHAKEN Extensions Pursuant to Section 4(b)(5) of the TRACED Act*, Public Notice, DA 21-1593, at 3 (WCB Dec. 16, 2021). The TRACED Act requires that the Commission, 12 months after the date of the TRACED Act's enactment, and thereafter "as appropriate," assess burdens or barriers to implementation of STIR/SHAKEN. *See* 47 U.S.C. § 227b(b)(5)(A)(i). The TRACED Act further provides the Commission discretion to extend compliance with the implementation mandate "upon a public finding of undue hardship." *Id*. § 227b(b)(5)(A)(ii). Not less than annually thereafter, the Commission must consider revising or extending any delay of compliance previously granted and issue a public notice regarding whether such delay of compliance remains necessary. *Id*. § 227b(b)(5)(F). The Commission directed the Wireline Competition Bureau to make these annual assessments and to reevaluate the Commission's granted extensions and revise or extend them as necessary. *See Second Caller ID Authentication Report and Order*, 36 FCC Rcd at 1896, para. 71.

[575] *See* 47 CFR § 64.6304(d).

[576] *See generally Numbering Policies for Modern Communications et al.*, WC Docket No. 13-97 et al., Further Notice of Proposed Rulemaking, FCC 21-94, 9-10, para. 17 (2021) (*Direct Access Further Notice*).

[577] *See generally* Vonage, In-Country, Local or No-CLI Calls Rejected, https://help nexmo.com/hc/en-us/articles/360049658392-In-Country-Local-or-No-CLI-Calls-Rejected, (last visited Apr. 27, 2022) ("Due to local country regulations, calls with a CLI or Caller ID terminating to the same country of origin, or those bearing no CLI at all, are subject to rejection from local operators to protect their subscribers from unwanted, malicious, or spoofing calls . . ."). The Infocomm Media Development Authority of Singapore (IMDA) has required operators to add a "+" prefix to international incoming calls, and IMDA is working with operators to block known numbers with the new prefix used for scams, especially +65 (Singapore's country code). *See* IMDA, Mitigating Spoof Calls, https://www.imda.gov.sg/-/media/Imda/Files/About/Media-Releases/2020/COS2020/Annex-D-COS-2020---Factsheet---Mitigating-Spoof-Calls.pdf?la=en (last visited Apr. 27, 2022); *see also* Vonage, South Korea Voice Features and Restrictions, https://help.nexmo.com/hc/en-us/articles/360015260932-South-Korea-Voice-Features-and-Restrictions (last visited Apr. 27, 2022) ("Local Korean numbers cannot be used as the CLI to send traffic towards South Korea.").

[578] *See* Communications Alliance Ltd, Industry Code, C661: 2020, Reducing Scam Calls, Section 4.2.6, https://www.commsalliance.com.au/__data/assets/pdf_file/0015/72150/C661_2020.pdf (last visited Apr. 27, 2022) ("C/CSPs should not send Inbound International Calls to B-Parties on their own Telecommunications Network or XPOI to the Transit C/CSPs or Terminating C/CSPs where the A-Party CLI of an Inbound International Call is showing an Australian number, unless exceptions apply (as per CA G664:2020).").

YouMail argues, establish a specific area code for foreign-originated calls?[579] If so, should we require providers block or otherwise restrict calls from all other area codes or place heightened due diligence or mitigation obligations on gateway providers receiving calls from such an area code? Is assignment of a valuable numbering resource—an area code—an efficient use of such resource? We seek comment on the approach taken in Germany, where if a call originating outside of Germany carries a German number, the number must not be displayed to a German end user unless the call is an international mobile roaming call.[580] Would this or a similar mandated call-labelling approach be appropriate for some or all foreign-originated calls carrying U.S. numbers?

220. Should we only impose restrictions in those cases where the call is not authenticated? For example, France requires that operators block calls with a French number in the caller ID from an operator outside of France unless the operator assigning, depositing, or receiving the number is able to guarantee the authenticity of the caller ID or the call is an international mobile roaming call of a French operator's end user.[581] Under a similar approach, any calls carrying a U.S. NANP number that arrive in the United States with a STIR/SHAKEN authentication would not be automatically blocked. We seek comment on such an approach.

221. We seek comment on the effect that any of these restrictions or limitations would have on foreign call centers of U.S. corporations that make foreign-originated calls to U.S. customers. In particular, how do call centers operate when calling into countries that bar the foreign origination of calls into the domestic market carrying domestic caller ID information? We seek comment on the burden that these restrictions may have on providers and other entities such as call centers as well as the benefit that would result from bright-line restrictions on the use of U.S. NANP numbers for foreign-originated calls.

222. *Indirect Access Restrictions.* We seek comment on whether we should impose any restrictions on indirect access to U.S. NANP numbers to prevent their use by foreign or domestic robocallers. In the *Direct Access Further Notice*, the Commission sought comment on steps it could take to ensure that VoIP providers obtaining direct access to numbers did not use those numbers to facilitate illegal robocalls.[582] It also asked whether the Commission should require applicants for direct access to numbers to certify that the numbers they apply for will only be used to provide interconnected VoIP services and whether interconnected VoIP providers that receive direct access to numbers must use those numbers for interconnected VoIP services.[583] Some commenters in that proceeding noted that indirect access is common and that unscrupulous providers may be doing so for nefarious purposes, including

---

[579] *See* YouMail Comments at 3 ("[T]he Commission could propose new rules that would require the NANP administrator to designate a new Area Code for exclusive use in foreign locations. Over time, consumers would learn to recognize the area code and its purpose. To stimulate consumers to answer calls from these numbers, VSPs, most especially gateway providers, would have an even stronger incentive to stop robocalling from these numbers.").

[580] *See* ECC Draft Report 338 at 12; Federal Gazette, Telecommunications Act, § 120(4) (June 23, 2021), https://www.bgbl.de/xaver/bgbl/start.xav#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s1858.pdf%27%5D__1650490426894. According to providers, Japan has similar restrictions. *See* Vonage, Japan Voice Features and Restrictions, https://help nexmo.com/hc/en-us/articles/232001088-Japan-Voice-Features-and-Restrictions (last visited Apr. 27, 2022) ("Our Voice products do offer CLI/Caller ID delivery for calls delivered from international numbers in international format, but not from Japan numbers in international or national format (e.g., 81701167890, 70xxxxxxxx/ 80xxxxxxxx/ 90xxxxxxxx). The calls will still succeed, but the Caller ID will be stripped or changed.").

[581] *See* Légifrance, Post and Electronic Communications Code, Book II, Title II, Article 44, Para. V, https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070987/LEGISCTA000006150688/?anchor=LEGIARTI000044330892#LEGIARTI000044330892 (last visited Apr. 27, 2022).

[582] *See generally Direct Access Further Notice*.

[583] *See id.* at para. 17.

illegal robocalling.[584] We note that some illegal robocallers do not spoof numbers but instead obtain numbers from providers that themselves either obtained the number directly from the NANPA or from another provider.[585]

223. While we do not prejudge the outcome of the *Direct Access Further Notice*, we seek comment here on a broader bar on indirect access. Should we adopt any restrictions on indirect access to numbers by interconnected VoIP providers *and* carriers or specifically for use in foreign-originated calls to reduce the ability of robocallers to do so?[586] If so, what should those restrictions be? Should they be modeled after limitations other countries have put in place? We note that some countries limit the number of times a number can be transferred after it is obtained directly from the numbering administrator or completely bar number sub-assignment (indirect access).[587] Would a similar rule be appropriate here? Does a less restrictive approach make sense? For example, in Portugal, further sub-assignment is permitted, but only if the provider that obtained the initial sub-assignment has allocated 60% of the numbers received to its end users.[588] Instead of or in addition to limiting indirect access, could we hold providers that obtain numbers directly from NANPA strictly liable for illegal robocalling undertaken by any entity that obtains the number through indirect access? Would such an approach be enforceable and, if so, how would we enforce it? Does direct access to numbers by VoIP providers reduce or eliminate the need for numbers to be readily available through indirect access? Should we, on our own or in concert with NANPA, instead establish a system for tracking the number of times that a number has been transferred via indirect access, to whom, and who has the right to use a number at a

[584] *See, e.g.*, RingCentral et al., Comments, WC Docket No. 13-97 et al., at 3 (filed Oct. 14, 2021) (RingCentral et al. Direct Access Comments) ("The wholesale market for numbering resources dates back decades, with more carriers providing services through indirectly obtained numbers than not. Any provider can rely on the secondary market to obtain numbers, and irresponsible providers and bad actors may even prefer doing so over engaging directly with the Commission and the Numbering Administrator."); USTelecom Comments, WC Docket No. 13-97 et al., at 5-6 (filed Oct. 14, 2021) (USTelecom Direct Access Comments) ("Bad actors today are getting their hands on thousands of numbers, often through a robust number distribution and resale market that at times also enables a diffusion of responsibility. And they may (and often do) obtain access to numbers from one provider, and then use an entirely different provider to originate their illegal robocalls.").

[585] *See, e.g.*, ZipDX Comments at 12; USTelecom Direct Access Comments at 2 ("Some sophisticated bad actor robocallers already are moving from spoofing fake numbers to using valid numbers in their schemes.").

[586] *See* RingCentral et al. Direct Access Comments at 3, 9 (arguing that VoIP-only restrictions on number access are anticompetitive and that "irresponsible providers would have access to numbers indirectly, just as they do today, through the wholesale market from carriers," but asserting that all providers should be able to resell numbers obtained through direct access "to ensure that U.S. consumers realize these cost, routing, and product innovation improvements far into the future").

[587] *See* CEPT Electronics Communications Committee, ECC Report 311: Sub-assignment and number hosting - Implementation models, rights of use and obligations for E.164 numbers across the electronic communications supply chain, at 16 (approved May 27, 2020) (ECC Report 311), https://docdb.cept.org/download/1420 ("There is no harmonised approach governing sub-assignment in Europe. In some countries, sub-assignment is explicitly allowed, while in a few other countries it is explicitly forbidden. In some countries where it is allowed, it is allowed to one level of sub-assignment only and in other countries the [Numbering Plan Administrator] must be notified of the sub-assignment. There are also differences regarding the obligations associated with the assignment of numbers. In some countries they follow with the sub-assignment, in other countries they remain with the primary assignee while in other countries the responsibilities are shared. The quantity of sub-assigned numbers is also different; some countries allow any quantity while others can impose a minimum amount.").

[588] *See* Lexology, Regulation on number sub-allocation: Extending competition in the provision of electronic communications services (Jan. 19, 2022), https://www.lexology.com/library/detail.aspx?g=91ca1a0e-615f-4155-9312-5d06dce55a48.

particular time?[589] We seek comment on the costs and administrative hurdles of establishing such a system, as well as the benefits and burdens. Could such a tracking system also assist in the enforcement of our robocall rules generally? For example, like STIR/SHAKEN, it would allow a downstream provider to determine whether the originating party (or at least the upstream provider) was authorized to use a number. How could providers use that information, particularly in concert with STIR/SHAKEN data?

G. STIR/SHAKEN by Third Parties

224. We seek comment on whether certain of our rules regarding caller ID authentication and attestation in the Robocall Mitigation Database require clarification. Our rules require that a voice service provider "[a]uthenticate caller identification information for all SIP calls it originates and . . . transmit that call with authenticated caller identification information to the next voice service provider or intermediate provider in the call path."[590] TransNexus asserts that some originating providers have had underlying (in the case of resellers) or downstream providers authenticate calls on the originating provider's behalf.[591] Should the Commission allow a third party to authenticate caller identification information to satisfy the originating provider's obligation? Conversely, should we amend our rules regarding filing in the Robocall Mitigation Database to require attestation of STIR/SHAKEN implementation by the originating provider itself—i.e., require all domestic providers to have their own token from the STI-GA for purposes of authentication? As to both questions, why or why not? Is third-party authentication proper in certain circumstances but improper in others?[592] Is third-party authentication consistent with the standards underlying the STIR/SHAKEN framework?[593] And does authentication by someone other than the originating provider undercut STIR/SHAKEN? We seek comment on whether the Commission needs to amend its current rules in order to account for this practice, whether to prohibit or allow it.

H. Differential Treatment of Conversational Traffic

225. We seek comment on stakeholders' argument that certain traffic is unlikely to carry illegal robocalls and thus should be treated differently under our rules from other voice traffic. Specifically, we seek comment on whether cellular roaming traffic (i.e., traffic originated abroad from U.S. mobile subscribers carrying U.S. NANP numbers terminated in the U.S.) should be treated with a lighter touch.[594] Are these commenters' concerns valid? Is cellular roaming traffic unlikely to carry illegal robocalls? What percentage of cellular roaming traffic is signed? What percentage of unsigned

---

[589] *See Direct Access Further Notice* at para. 5 ("[W]hen interconnected VoIP providers use a carrier numbering partner, the carrier partner is listed in the Local Exchange Routing Guide and industry databases, making it more difficult for other providers to identify the entity with which they are exchanging traffic."); ECC Report 311, at 12 ("A database containing information on which entities have been sub-assigned numbers and on which networks assigned numbers are hosted would assist [Numbering Plan Administrators (NPA)] to monitor the market and ensure compliance with the regulatory framework. Such a database could be either centralised or distributed. It could be maintained by the NPA, by market players or by a third party vendor. It could be accessible by the NPA, by market players or by the public depending on the type of information maintained.").

[590] 47 CFR § 64.6301(a)(2).

[591] *See* TransNexus Comments, WC Docket No. 17-97, at 2-4 (filed Nov. 12, 2021) (TransNexus Small Provider Extension Comments).

[592] *See id.* at 3 (arguing that an intermediate provider's use of an originating service provider's SHAKEN certificate represents "a legitimate outsourcing arrangement" while, conversely, use of an "intermediate provider's SHAKEN certificate" to sign for calls of an upstream provider undermines the STIR/SHAKEN framework).

[593] *See id*.

[594] *See* iBasis Comments at 5; ZipDX Comments at 27; Verizon Reply at 11. We do not adopt a rule in the accompanying *Gateway Provider Report and Order* regarding this traffic because the record is not sufficiently developed on this point. *See supra* Section III.B.

cellular roaming traffic consists of illegal calls? If we treat cellular roaming differently, could robocallers disguise traffic as cellular roaming traffic in order to take advantage of any "lighter touch" regulatory regime we adopt? Is it technically feasible for the gateway provider or downstream providers to clearly identify legitimate cellular roaming traffic for compliance purposes? Several commenters suggest that they are able to do so,[595] but is that true for all domestic providers in the call path and is it realistic for them to do so? For example, ZipDX implies that roaming traffic would need to be placed on separate trunks for it to be practically subject to a different set of rules from other traffic and that segregation currently does not occur in all cases.[596] We seek comment on this assertion and cellular roaming routing practices in general. Should we modify our rules applicable to some or all domestic providers to take these differences in traffic into account? What, if any, regulatory carve-outs for our robocalling rules would be appropriate for any traffic that falls within this category?[597] What would be the costs of distinguishing legitimate roaming traffic from illegal robocalls subject to our robocall protection requirements? Should we treat calls originated from domestic cellular customers carrying U.S. NANP numbers with a similarly light touch? Are there other categories of traffic that should be subject to greater or lesser scrutiny than other voice traffic under our rules?[598] If so, what are those categories of traffic and what rules should apply?

I. Legal Authority

226. We propose to adopt any of the foregoing obligations largely pursuant to the legal authority we relied upon in prior caller ID authentication and call blocking orders, including authority we relied upon in the accompanying *Order*. We seek comment on this approach.

227. *Caller ID Authentication.* Gateway providers are a subset of intermediate providers.[599] In the *Gateway Provider Report and Order*, we rely upon 251(e) of the Act and the Truth in Caller ID Act to require gateway providers to authenticate unauthenticated calls.[600] In the *Caller ID Second Report and Order*, we relied on this authority when requiring intermediate providers to either authenticate unauthenticated calls or cooperate with the industry traceback consortium and respond to traceback requests.[601] We therefore propose to rely upon the same authority to require all intermediate providers to authenticate unauthenticated calls. We seek comment on this approach; is there any reason we may not rely on the same authority here? We also seek comment on whether there are alternative sources of authority we should rely on.

228. *Robocall Mitigation and Call Blocking.* In adopting our robocall mitigation and call blocking rules for gateway providers in the accompanying *Order*, we relied upon sections 201(b), 202(a), 251(e); the Truth in Caller ID Act; and our ancillary authority.[602] We propose to rely on this same authority in adopting additional robocall mitigation and call blocking requirements for all domestic providers, as described above. We seek comment on this approach and whether there are other sources of

---

[595] *See* iBasis Comments at 12-13; ZipDX Comments at 27; Verizon Reply at 11. *But see* Belgacom International Carrier Services Comments at 1 (arguing that such traffic is not always readily identifiable).

[596] *See* ZipDX Comments at 27.

[597] *See* Verizon Reply at 11 ("Consistent with iBasis' comments, the Commission should design its chain of trust rules to permit Robocall Mitigation Database registrants to accept roaming traffic (which is unlikely to include illegal robocalls) in appropriate circumstances even if those foreign providers are not registered.").

[598] *See, e.g.*, ZipDX Apr. 19 *Ex Parte* at 9-12 (arguing for different regulatory treatment of "conversational" and "non-conversational" traffic).

[599] *See supra* Section III.B.

[600] *See* 47 U.S.C. §§ 227(e), 251(e).

[601] *See Caller ID Authentication Second Report and Order,* 36 FCC Rcd at 1931-32, paras. 153-55.

[602] *See supra* Section III.G.

authority we should consider.

229. We seek specific comment on our ancillary authority. We anticipate that the proposed regulations applicable to all domestic providers are "reasonably ancillary to the Commission's effective performance of its . . . responsibilities."[603] Providers not classified as common carriers interconnect with the public switched telephone network and exchange IP traffic, which clearly constitutes "communication by wire and radio."[604] We believe that requiring these providers to comply with our proposed rules is reasonably ancillary to the Commission's effective performance of its statutory responsibilities under sections 201(b), 202(a), 251(e), and the Truth in Caller ID Act as described above. With respect to sections 201(b) and 202(a), absent application of our proposed rules to providers not classified as common carriers, originators of robocalls could circumvent our proposed regulatory scheme by sending calls only to providers not classified as common carriers to reach their destination. We seek comment on this analysis and any other basis of our ancillary authority here.

230. *Enforcement*. We also propose to adopt our additional enforcement rules above pursuant to sections 501, 502, and 503 of the Act.[605] These provisions allow us to take enforcement action against common carriers as well as providers not classified as common carriers following a citation.[606] We also propose to rely on the existing authority in section 1.80 of our rules regarding forfeiture amounts.[607] We seek comment on this proposed authority and any other sources of our enforcement authority.

231. *Numbering Restrictions.* To adopt any of the foregoing numbering restrictions, we propose to rely on section 251(e) and its grant to the Commission of authority over numbering resources as well as sections 201 and 251(b).[608] We have repeatedly relied on these sections in adopting our numbering rules.[609] We also propose to rely on our ancillary authority. We believe that placing restrictions on numbering access for providers not classified as common carriers would be reasonably ancillary to the Commissions' performance under these three sections. Access to numbers is necessary to ensure a level playing field and foster competition by eliminating barriers to, and incenting development of, innovative IP services. We thus propose to conclude that, for these or other reasons, imposing numbering restrictions on providers not classified as common carriers is reasonably ancillary to the Commission's responsibilities to ensure that numbers are made available on an "equitable" basis, to advance the number-portability requirements of section 251(b), or to help ensure just and reasonable rates and practices for telecommunications services regulated under section 201.[610] We also seek comment on

---

[603] *United States v. Southwestern Cable Co.*, 392 U.S. 157, 178 (1968); *see also, e.g.*, *Rural Call Completion*, WC Docket No. 13-39, Report and Order and Further Notice of Proposed Rulemaking, 28 FCC Rcd 16154, 16562, para. 35 (2013) ("Ancillary authority may be employed, at the Commission's discretion, when the Act covers the regulated subject and the assertion of jurisdiction is reasonably ancillary to the effective performance of the Commission's various responsibilities.") (internal citations omitted).

[604] 47 U.S.C. § 152(a).

[605] *Id*. §§ 501-03.

[606] *Id*. § 503(b)(5).

[607] 47 CFR § 1.80.

[608] *See* 47 U.S.C. §§ 201, 251(b), 251(e); *see also* YouMail Comments at 3 n.1 ("With its exclusive authority over telephone numbers in the United States, pursuant to 47 U.S.C. § 251(e)(1), the Commission could propose new rules that would require the NANP administrator to designate a new Area Code for exclusive use in foreign locations.").

[609] *See, e.g.*, *Telephone Number Requirements for IP-Enabled Services Providers et al.*, WC Docket No. 07-243 et al., Report and Order, Declaratory Ruling, Order on Remand, and Notice of Proposed Rulemaking, 22 FCC Rcd 19531, 19541, 19543, paras. 19, 21 (2007) (establishing authority for VoIP local number portability obligations).

[610] *See* 47 U.S.C. § 251(e)(1); *Preserving the Open Internet; Broadband Industry Practices*, GN Docket No. 09-191, WC Docket No. 07- 52, Report and Order, 25 FCC Rcd 17905, 17972, para. 125 (2010).

other possible bases for the Commission to exercise ancillary authority here.

J. Digital Equity and Inclusion

232. The Commission, as part of its continuing effort to advance digital equity for all,[611] including people of color and others who have been historically underserved, marginalized, and adversely affected by persistent poverty and inequality, invites comment on any equity-related considerations[612] and benefits (if any) that may be associated with the proposals and issues discussed herein. Specifically, we seek comment on how our proposals may promote or inhibit advances in diversity, equity, inclusion, and accessibility.

VII. PROCEDURAL MATTERS

233. *Final Regulatory Flexibility Analysis*. As required by the Regulatory Flexibility Act of 1980 (RFA),[613] an Initial Regulatory Flexibility Analysis (IRFA) was incorporated into the *Gateway Provider Notice*.[614] The Commission sought written public comment on the possible significant economic impact on small entities regarding the proposals addressed in the *Gateway Provider Notice*, including comments on the IRFA.[615] Pursuant to the RFA, a Final Regulatory Flexibility Analysis is set forth in Appendix C. The Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, will send a copy of this *Gateway Provider Report and Order*, including the Final Regulatory Flexibility Analysis (FRFA), to the Chief Counsel for Advocacy of the Small Business Administration (SBA).[616]

234. *Initial Regulatory Flexibility Analysis*. As required by the RFA, the Commission has prepared an IRFA of the possible significant economic impact on small entities of the policies and rules addressed in this *Further Notice*. The IRFA is set forth in Appendix D. Written public comments are requested on the IRFA. Comments must be filed by the deadlines for comments on the *Further Notice* indicated on the first page of this document and must have a separate and distinct heading designating them as responses to the IRFA. The Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, will send a copy of this *Further Notice*, including the IRFA, to the Chief Counsel for Advocacy of the SBA.[617]

235. *Paperwork Reduction Act*. This document may contain new and modified information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104-13. Specifically, the rules adopted in 47 CFR §§ 64.1200(n)(1) 64.1200(o), 64.6303(b), 64.6305(b), (c)(2)

---

[611] Section 1 of the Communications Act of 1934 as amended provides that the FCC "regulat[es] interstate and foreign commerce in communication by wire and radio so as to make [such service] available, so far as possible, to all the people of the United States, without discrimination on the basis of race, color, religion, national origin, or sex." 47 U.S.C. § 151.

[612] We define the term "equity" consistent with Executive Order 13985 as the consistent and systematic fair, just, and impartial treatment of all individuals, including individuals who belong to underserved communities that have been denied such treatment, such as Black, Latino, and Indigenous and Native American persons, Asian Americans and Pacific Islanders and other persons of color; members of religious minorities; lesbian, gay, bisexual, transgender, and queer (LGBTQ+) persons; persons with disabilities; persons who live in rural areas; and persons otherwise adversely affected by persistent poverty or inequality. *See* Exec. Order No. 13985, 86 Fed. Reg. 7009, Executive Order on Advancing Racial Equity and Support for Underserved Communities Through the Federal Government (Jan. 20, 2021).

[613] *See* 5 U.S.C. § 603.

[614] *Gateway Provider Notice* at Appx. B.

[615] *Id.*

[616] *See* 5 U.S.C. § 603(a).

[617] *See id*.

and (d) may require new or modified information collections. This document will be submitted to the Office of Management and Budget (OMB) for review under Section 3507(d) of the PRA. OMB, the general public, and other Federal agencies will be invited to comment on the new or modified information collection requirements contained in this proceeding. The modification to 47 CFR § 64.6305(c)(2) is non-substantive and will be submitted to OMB in accordance with its process for non-substantive changes. In addition, we note that pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, we previously sought specific comment on how the Commission might further reduce the information collection burden for small business concerns with fewer than 25 employees.[618]

236. The *Further Notice* also contains proposed new and revised information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public and OMB to comment on the information collection requirements contained in this document, as required by the Paperwork Reduction Act of 1995, Public Law 104-13. In addition, pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, *see* 44 U.S.C 3506(c)(4), we seek specific comment on how we might further reduce the information collection burden for small business concerns with fewer than 25 employees.

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

238. *Ex Parte Presentations—Permit-But-Disclose.* The proceeding this *Further Notice* initiates shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules.[619] Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with section 1.1206(b) of the Commission's rules. In proceedings governed by section 1.49(f) of the Commission's rules or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (*e.g.*, .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.[620]

239. *Comment Filing Procedures.* Pursuant to sections 1.415 and 1.419 of the Commission's rules, 47 CFR §§ 1.415, 1.419, interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using the Commission's

[618] 44 U.S.C. § 3506(c)(4).

[619] 47 CFR §§ 1.1200 *et seq.*

[620] 47 CFR § 1.49(f).

Electronic Comment Filing System (ECFS). *See Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998).

- Electronic Filers: Comments may be filed electronically using the Internet by accessing ECFS: https://www.fcc.gov/ecfs/.

- Currently, the Commission does not accept any hand-delivered or messenger-delivered filings as a temporary measure taken to help protect the health and safety of individuals, and to mitigate the transmission of COVID-19. In the event that the Commission announces the lifting of COVID-19 restrictions, a filing window will be opened at the Commission's office located at 9050 Junction Drive, Annapolis, Maryland 20701.[621]

240. Pursuant to section 1.49 of the Commission's rules, 47 CFR § 1.49, parties to this proceeding must file any documents in this proceeding using the Commission's Electronic Comment Filing System (ECFS): www.fcc.gov/ecfs.

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

242. *Additional Information*. For further information about the *Further Notice*, contact either Jonathan Lechter, Attorney Advisor, Competition Policy Division, Wireline Competition Bureau, at Jonathan.lechter@fcc.gov (202) 418-0984; or Jerusha Burnett, Attorney Advisor, Consumer Policy Division, Consumer and Governmental Affairs Bureau, at jerusha.burnett@fcc.gov, (202) 418-0526.

VIII. ORDERING CLAUSES

243. Accordingly, pursuant to sections 4(i), 4(j), 201, 202, 217, 227, 227b, 251(e), 303(r), and 403 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 154(i), 154(j), 201, 202, 217, 227, 227b, 251(e), 303(r), and 403, IT IS ORDERED that this *Gateway Provider Report and Order* IS ADOPTED.

244. IT IS FURTHER ORDERED THAT, pursuant to sections 4(i), 4(j), 201, 202, 217, 227, 227b, 251(e), 303(r), 403, and 405 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 154(i), 154(j), 201, 202, 217, 227, 227b, 251(e), 303(r), 403, and 405, this *Order on Reconsideration* IS ADOPTED.

245. IT IS FURTHER ORDERED THAT, pursuant to sections 4(i), 4(j), 201, 202, 217, 227, 227b, 251(e), and 303(r) of the Communications Act of 1934, as amended, 47 U.S.C. §§ 154(i), 154(j), 201, 202, 217, 227, 227b, 251(e), and 303(r), this *Order* IS ADOPTED.

246. IT IS FURTHER ORDERED THAT, pursuant to sections 4(i), 4(j), 201, 202, 217, 227, 227b, 251(b), 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, 217, 227, 227b, 251(b) 251(e), 303(r), 501, 502, and 503, this *Further Notice of Proposed Rulemaking* IS ADOPTED.

247. IT IS FURTHER ORDERED that parts 0 and 64 of the Commission's rules ARE AMENDED as set forth in Appendix A.

248. IT IS FURTHER ORDERED that, pursuant to sections 1.4(b)(1) and 1.103(a) of the Commission's rules, 47 CFR §§ 1.4(b)(1), 1.103(a), and this *Report and Order* SHALL BE EFFECTIVE 60 days after publication in the Federal Register. Compliance with 47 CFR §§ 64.1200(n)(1) and 64.1200(o) will not be required until OMB completes any review that the Consumer and Governmental Affairs Bureau determines is required under the Paperwork Reduction Act. The Commission directs the Consumer and Governmental Affairs Bureau to announce a compliance date by subsequent Public Notice

[621] *Amendment of the Commission's Rules of Practice and Procedure*, Order, 35 FCC Rcd 5450 (OMD 2020).

and to cause 47 CFR §§ 64.1200(n)(1) and 64.1200(o) to be revised accordingly. Compliance with 47 CFR §§ 64.6303(b), 64.6305(b), 64.6305(c)(2), and 64.6305(d) will not be required until OMB completes any review that the Wireline Competition Bureau determines is required under the Paperwork Reduction Act. The Commission directs the Wireline Competition Bureau to announce a compliance date by subsequent Public Notice and to cause 47 CFR §§ 64.6303(b), 64.6305(b), 64.6305(c)(2), and 64.6305(d) to be revised accordingly.

249. IT IS FURTHER ORDERED that the Petition for Partial Reconsideration filed by CTIA IS DENIED.

250. IT IS FURTHER ORDERED THAT the Petition for Reconsideration filed by Voice on the Net Coalition IS DENIED IN PART and, in the alternative, DISMISSED IN PART.

251. IT IS FURTHER ORDERED that this *Order on Reconsideration* and *Order* SHALL BE effective 60 days after publication in the Federal Register.

252. IT IS FURTHER ORDERED that the Office of the Managing Director, Performance Evaluation and Records Management, SHALL SEND a copy of this *Gateway Provider Report and Order* and *Order on Reconsideration* in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act, see 5 U.S.C. § 801(a)(1)(A).

253. IT IS FURTHER ORDERED that the Commission's Consumer & Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this *Gateway Provider Report and Order* and *Order on Reconsideration*, including the Final Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

254. IT IS FURTHER ORDERED that the Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this *Further Notice of Proposed Rulemaking*, including the Initial Regulatory Flexibility Analysis, to the Chief Counsel for Advocacy of the Small Business Administration.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

APPENDIX A
Final Rules

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

PART 0—COMMISSION ORGANIZATION

Subpart A—Organization

1. Amend section 0.111(a) by revising paragraph (27) and adding paragraph (28) to read:

(27) Identify suspected illegal calls and provide written notice to voice service providers. The Enforcement Bureau shall: (1) identify with as much particularity as possible the suspected traffic; (2) cite the statutory or regulatory provisions the suspected traffic appears to violate; (3) provide the basis for the Enforcement Bureau's reasonable belief that the identified traffic is unlawful, including any relevant nonconfidential evidence from credible sources such as the industry traceback consortium or law enforcement agencies; and (4) direct the voice service provider receiving the notice that it must comply with section 64.1200(n)(2) or section 64.1200(n)(5) of the Commission's rules.

(28) Take enforcement action, including de-listing from the Robocall Mitigation Database, against any provider: (i) whose certification described in section 64.6305(c)-(d) of the Commission's rules is deficient after giving that provider notice and an opportunity to cure the deficiency; or (ii) who accepts calls directly from a domestic voice service provider, gateway provider, or foreign provider not listed in the Robocall Mitigation Database in violation of section 64.6305(e).

PART 64—MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

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

1. Amend section 64.1200 by revising paragraphs (k)(5), (k)(6), and (n)(1) and adding paragraphs (f)(19), (n)(4), (n)(5), (n)(6), (o), and (p) to read as follows:

(f)(19) The term *gateway provider* means a U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider. For purposes of this rule, (i) "U.S.-based" means that the provider has facilities located in the United States, including a point of presence capable of processing the call; and (ii) "receives a call directly" from a provider means the foreign provider directly upstream of the gateway provider in the call path sent the call to the gateway provider, with no providers in-between.

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

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

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

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

(ii) If the provider receiving a traceback request is the gateway provider for any calls specified in the traceback request, the provider must fully respond to the traceback request within 24 hours of receipt of the request. The 24-hour clock does not start outside of business hours, and requests received during that time are deemed received at 8:00 a.m. on the next business day. If the 24-hour response period would end on a non-business day, either a weekend or a federal legal holiday, the 24-hour clock does not run for the weekend or holiday in question, and restarts at 12:01 a.m. on the next business day following when the request would otherwise be due. For example, a request received at 3:00 p.m. on a Friday will be due at 3:00 p.m. on the following Monday, assuming that Monday is not a federal legal holiday. For purposes of this rule, "business day" is defined as Monday through Friday, excluding federal legal holidays, and "business hours" is defined as 8:00 a.m. to 5:30 p.m. on a business day. For purposes of this rule, all times are local time for the office that is required to respond to the request.

(n)(4) If the provider acts as a gateway provider, take reasonable and effective steps to ensure that any foreign originating provider or foreign intermediate provider from which it directly receives traffic is not using the gateway provider to carry or process a high volume of illegal traffic onto the U.S. network. Compliance with this paragraph will not be required until <180 days from publication in the Federal Register>.

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

(i) The Enforcement Bureau will issue a Notification of Suspected Illegal Traffic that identifies with as much particularity as possible the suspected illegal traffic; provides the basis for the Enforcement Bureau's reasonable belief that the identified traffic is unlawful; cites the statutory or regulatory provisions the identified traffic appears to violate; and directs the provider receiving the notice that it must comply with this section. The Enforcement Bureau's Notification of Suspected Illegal Traffic shall give the identified provider a minimum of 14 days to comply with the notice. Each notified provider must promptly investigate the identified traffic and report the results of that investigation to the Enforcement Bureau within the timeframe specified in the Notification of Suspected Illegal Traffic. If the provider's investigation determines that it served as the gateway provider for the identified traffic, it must block the identified traffic within the timeframe specified in the Notification of Suspected Illegal Traffic and include in its report to the Enforcement Bureau: (1) a certification that it is blocking the identified traffic and will continue to do so; and (2) a description of its plan to identify and block substantially similar traffic on an ongoing basis. If the provider's investigation determines that the identified traffic is not illegal, it shall provide an explanation as to why the provider reasonably concluded that the identified traffic is not illegal and what steps it took to reach that conclusion. Absent such a showing, or if the Enforcement Bureau determines based on the evidence that the traffic is illegal despite the provider's assertions, the identified traffic will be deemed illegal. If the notified provider determines during this investigation that it did not serve as the gateway provider for any of the identified traffic, it shall provide

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

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

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

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

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

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

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

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

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

(p) Paragraphs (n)(1) and (o) of this section may contain an information-collection and/or recordkeeping requirement. Compliance with paragraphs (n)(1) and (o) will not be required until this paragraph (p) is removed or contains a compliance date, which will not occur until after the Office of Management and Budget completes review of such requirements pursuant to the Paperwork Reduction Act or until after the Consumer and Governmental Affairs Bureau determines that such review is not required. The Commission directs the Consumer and Governmental Affairs Bureau to announce a compliance date for sections 64.1200(n)(1) and 64.1200(o) by subsequent Public Notice and to cause 47 CFR §§ 64.1200(n)(1) and 64.1200(o) to be revised accordingly.

3. Amend section 64.6300 by redesignating paragraphs (d) through (m) as (e) through (n), respectively, revising redesignated paragraph (g), and adding new paragraph (d) to read as follows:

(d) *Gateway provider.* The term "gateway provider" means a U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider. For purposes of this rule, (i) "U.S.-based" means that the provider has facilities located in the United States, including a point of presence capable of processing the call; and (ii) "receives a call directly" from a provider means the foreign provider directly upstream of the gateway provider in the call path sent the call to the gateway provider, with no providers in-between.

* * * * *

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

4. Amend section 64.6302 by adding paragraph (c) to read as follows:

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

5. Amend section 64.6303 by deleting the introductory language and amending paragraphs (a) and (b) to read as follows:

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

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

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

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

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

(ii) 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.

(iii) Paragraph (b) of this section may contain an information collection and/or recordkeeping requirement. Compliance with paragraph (b) will not be required until this paragraph (b)(iii) is removed or contains a compliance date, which will not occur until after the Office of Management and Budget completes review of such requirements pursuant to the Paperwork Reduction Act or until after the Wireline Competition Bureau determines that such review is not required. The Commission directs the Wireline Competition Bureau to announce a compliance date for section 64.6303(b) by subsequent Public Notice and to cause 47 CFR § 64.6303(b) to be revised accordingly.

6. Amend section 64.6304 by amending paragraphs (b) and (d) to read as follows:

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

* * * * *

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

7. Amend section 64.6305 by redesignating paragraphs (b) and (c) as (c) and (e), respectively, revising paragraph (a) and redesignated paragraphs (c) and (e), and adding new paragraphs (b), and (d), to read as follows:

(a) *Robocall mitigation program requirements for voice service providers.*

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

(2) Any robocall mitigation program implemented pursuant to paragraph (a)(1) of this section shall include reasonable steps to avoid originating illegal robocall traffic and shall include a commitment to respond fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

(b) *Robocall mitigation program requirements for gateway providers.*

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

(2) Any robocall mitigation program implemented pursuant to paragraph (b)(1) of this section shall include reasonable steps to avoid carrying or processing illegal robocall traffic and shall include a commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls.

(3) Paragraph (2) of this subsection may contain an information-collection and/or recordkeeping requirement. Compliance with paragraph (2) will not be required until this paragraph (3) is removed or contains a compliance date, which will not occur until after the Office of Management and Budget completes review of such requirements pursuant to the Paperwork Reduction Act or until after the Wireline Competition Bureau determines that such review is not required. The Commission directs the Wireline Competition Bureau to announce a compliance date for section 64.6305(b) by subsequent Public Notice and to cause 47 CFR § 64.6305(b) to be revised accordingly.

(c) *Certification by voice service providers in the Robocall Mitigation Database.*

(1) Not later than June 30, 2021, a voice service provider, regardless of whether it is subject to an extension granted under §64.6304, shall certify to one of the following:

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

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

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

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

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

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

(iii) A statement of the voice service provider's commitment to respond fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

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

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

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

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

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

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

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

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

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

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

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

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

(6) Paragraph (2) of this subsection may contain an information collection and/or recordkeeping requirement. Compliance with paragraph (2) will not be required until this paragraph (6) is removed or contains a compliance date, which will not occur until after the Office of Management and Budget completes review of such requirements pursuant to the Paperwork Reduction Act or until after the Wireline Competition Bureau determines that such review is not required. The Commission directs the

Wireline Competition Bureau to announce a compliance date for section 64.6305(c)(2)(by subsequent Public Notice and to cause 47 CFR § 64.6305(c)(2) to be revised accordingly.

(d) *Certification by gateway providers in the Robocall Mitigation Database.*

(1) 30 days following Federal Register notice of OMB approval of the relevant information collection obligations, a gateway provider shall certify to one of the following:

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

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

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

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

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

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

(iii) A statement of the gateway provider's commitment to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls.

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

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

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

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

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

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

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

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

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

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

(6) Paragraphs (1) through (5) of this subsection may contain an information collection and/or recordkeeping requirement. Compliance with paragraphs (1)-(5) will not be required until this paragraph (6) is removed or contains a compliance date, which will not occur until after the Office of Management and Budget completes review of such requirements pursuant to the Paperwork Reduction Act or until after the Wireline Competition Bureau determines that such review is not required. The Commission directs the Wireline Competition Bureau to announce a compliance date for section 64.6305(d) by subsequent Public Notice and to cause 47 CFR § 64.6305(d) to be revised accordingly.

(e) *Intermediate provider and voice service provider obligations.*

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

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

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

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

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

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

APPENDIX B
Proposed Rules

The Federal Communications Commission amends parts 0, 1 and 64 of Title 47 of the Code of Federal Regulations as follows:

PART 0—COMMISSION ORGANIZATION

Subpart A—Organization

1. Amend section 0.111(a) by revising paragraph (28) to read as follows:

(28) Take enforcement action, including de-listing from the Robocall Mitigation Database, against any provider: (i) whose certification described in section 64.6305(c)-(e) of the Commission's rules is deficient after giving that provider notice and an opportunity to cure the deficiency; or (ii) who accepts calls directly from a domestic voice service provider, domestic intermediate provider, gateway provider, or foreign provider not listed in the Robocall Mitigation Database in violation of section 64.6305(f).

PART 1—PRACTICE AND PROCEDURE

Subpart A—General Rules of Practice and Procedure

1. Amend section 1.80 by redesignating paragraphs (b)(9) and (b)(10) as (b)(10) and (b)(11) and adding new paragraph (b)(9), to read as follows:

(9) ***Forfeiture penalty for a failure to block.*** Any person determined to have failed to block illegal robocalls pursuant to section 64.6305(e) of the Commission's rules shall be liable to the United States for a forfeiture penalty of no more than $22,021 for each violation, to be assessed on a per-call basis. In addition to the mitigating and aggravating factors set forth in Table 1 to paragraph (b)(11) of this section, other factors to be considered in calculating a forfeiture amount under this paragraph shall include whether the violation includes failure to block calls to emergency services providers or public safety answering points or to numbers on a reasonable do-not-originate list.

PART 64—MISCELLANEOUS RULES RELATING TO COMMON CARRIERS

Subpart HH—Caller ID Authentication

2. Amend section 64.6302 by revising paragraph (b) to read as follows:

(b) Authenticate caller identification information for all calls it receives that use North American Numbering Plan resources that pertain to the United States in the caller ID field and for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call.

3. Amend section 64.6304 by amending paragraph (b) to read as follows:

(b) Voice service providers and 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 a SPC token. Intermediate providers, including gateway providers, that are incapable of obtaining an SPC token due to Governance Authority policy are exempt from the requirements of § 64.6302(b) regarding call authentication.

4. Amend section 64.6305 by redesignating paragraph (e) as (f), revising paragraphs (a), (c), (d), and redesignated paragraph (f), and adding new paragraph (e), to read as follows:

(a) *Robocall mitigation program requirements for voice service providers and intermediate providers (other than gateway providers).* (1) Except those subject to an extension granted under § 64.6304(b), any voice service provider and intermediate provider, not including gateway providers, shall implement an appropriate robocall mitigation program with respect to calls that use North American Numbering Plan resources that pertain to the United States in the caller ID field.

* * * * *

(c) *Certification by voice service providers in the Robocall Mitigation Database.*

* * * * *

(2) A voice service provider shall include a robocall mitigation program consistent with paragraph (a) of this section and shall include the following information in its certification in English or with a certified English translation:

* * * * *

(4) * * *

(iv) All known principals, affiliates, subsidiaries, and parent companies of the intermediate provider;

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

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

* * * * * *

(d) *Certification by gateway providers in the Robocall Mitigation Database.*

* * * * * *

(4) * * *

(iv) All known principals, affiliates, subsidiaries, and parent companies of the intermediate provider;

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

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

(e) *Certification by intermediate providers (other than gateway providers) in the Robocall Mitigation Database.*

(1) An intermediate provider shall certify to one of the following:

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

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

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

(2) An intermediate provider shall include the following information in its certification, in English or with a certified English translation:

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

(ii) A statement of the 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.

(3) All certifications made pursuant to paragraph (e)(1) 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) An intermediate provider filing a certification shall submit the following information in the appropriate portal on the Commission's website.

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

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

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

(iv) All known principals, affiliates, subsidiaries, and parent companies of the intermediate provider;

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

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

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

(f) *Intermediate provider and voice service provider obligations.*

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

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

(3) *Accepting traffic from domestic intermediate providers*. Intermediate providers and voice service providers shall accept calls directly from:

(i) a gateway provider, only if that provider's filing appears in the Robocall Mitigation Database in accordance with paragraph (d) of this section, showing that the gateway provider has affirmatively submitted the filing, and that the filing has not been de-listed pursuant to an enforcement action.

(ii) beginning 90 days after the deadline for filing certifications pursuant to paragraph (e) of this section, a domestic intermediate provider, only if that provider's filing appears in the Robocall Mitigation Database in accordance with paragraph (e) of this section, showing that the intermediate provider has affirmatively submitted the filing, and that the filing has not been de-listed pursuant to an enforcement action.

APPENDIX C
Final Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980 (RFA),[1] as amended, an Initial Regulatory Flexibility Analysis (IRFA) was incorporated into the *Further Notice of Proposed Rulemaking* adopted in September 2021 (*Gateway Provider Notice*).[2] The Commission sought written public comment on the proposals in the *Gateway Provider Notice*, including comment on the IRFA. The comments received are discussed below. This Final Regulatory Flexibility Analysis (FRFA) conforms to the RFA.[3]

A. Need for, and Objectives of, the Order

2. First, the *Gateway Provider Report and Order* takes important steps in the fight against foreign-originated illegal robocalls by holding gateway providers responsible for the calls they allow onto the U.S. network.[4] Finally, the *Order on Reconsideration* strengthens the prohibition on receiving calls carrying U.S. NANP numbers from foreign providers not listed in the Robocall Mitigation Database.[5] The decisions we make here protect American consumers from unwanted and illegal calls while balancing the legitimate interests of callers placing lawful calls.

3. *Gateway Provider Report and Order*. The *Gateway Provider Report and Order* takes important steps to protect consumers from foreign-originated illegal robocalls. These steps help stem the tide of foreign-originated illegal robocalls, which are a significant portion, if not the majority, of illegal robocalls.[6] As the entry point onto the U.S. network for these calls, gateway providers are best positioned to protect all American consumers. Because there is no single solution to the illegal robocall problem, the *Gateway Provider Report and Order* addresses this issue from several angles, all focused on reducing the number of foreign-originated illegal calls American consumers receive and aiding in identifying bad actors.

4. First, the *Gateway Provider Report and Order* requires gateway providers to submit a certification and plan to the Robocall Mitigation Database describing their robocall mitigation practices and stating that they are adhering to those practices, regardless of whether they have fully implemented STIR/SHAKEN, and requires downstream domestic providers receiving traffic from gateway providers to block traffic from such a provider if the gateway provider has not submitted a certification in the Robocall Mitigation Database.[7] Second, the *Gateway Provider Report and Order* requires gateway providers to implement STIR/SHAKEN to authenticate SIP calls that are carrying a U.S. number in the caller ID field.[8] Third, it requires gateway providers to fully respond to traceback requests from the Commission, civil and criminal law enforcement, and the industry traceback consortium within 24 hours of receipt of

---

[1] 5 U.S.C. § 603. The RFA, 5 U.S.C. §§ 601-612, has been amended by the Contract With America Advancement Act of 1996, Public Law No. 104-121, 110 Stat. 847 (1996) (CWAAA). Title II of the CWAAA is the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA).

[2] *Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17-59 Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17-97, FCC 21-105 (Oct. 1, 2021) (*Gateway Provider Notice*).

[3] *See* 5 U.S.C. § 604.

[4] *Gateway Provider Report and Order* at paras. 19-121.

[5] *Order on Reconsideration* at paras. 122-54.

[6] *Gateway Provider Report and Order* at para. 23.

[7] *Id.* at paras. 34-50.

[8] *Id.* at paras. 51-63.

such a request.[9] Fourth, it requires gateway providers to block illegal traffic when notified of such traffic by the Commission and the providers immediately downstream from the gateway to block all traffic from the identified provider when notified by the Commission that the gateway provider failed to meet its obligation to block illegal traffic.[10] This rule builds on the Commission's existing effective mitigation requirement[11] and bad-actor provider blocking safe harbor[12], and proscribes specific steps that the Enforcement Bureau must take before directing downstream providers to block.[13] Fifth, it requires gateway providers to block using a reasonable do-not-originate (DNO) list.[14] Sixth, it requires gateway providers to take reasonable and effective steps to ensure that the immediate upstream provider is not using the gateway provider to originate a high volume of illegal traffic onto the U.S. network.[15] Finally, it requires gateway providers to meet a general obligation to mitigate illegal robocalls regardless of whether they have fully implemented STIR/SHAKEN on the IP portions of their network.[16]

5. *Order on Reconsideration*. The *Order on Reconsideration* strengthens the existing prohibition on receiving calls carrying U.S. NANP numbers from foreign providers not listed in the Robocall Mitigation Database. To ensure that all foreign providers are brought within the prohibition, the *Order on Reconsideration* modifies the rule such that the prohibition applies to calls directly from a foreign provider that originates, carries, or processes a call if that foreign provider is not listed in the Robocall Mitigation Database.[17]

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

6. There were no comments raised that specifically addressed the proposed rules and policies presented in the *Gateway Provider Notice* IRFA.[18] 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

7. 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.[19] 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

[9] *Id.* at paras. 65-71.

[10] *Id.* at paras. 74-86.

[11] 47 CFR § 64.1200(n)(2).

[12] 47 CFR § 64.1200(k)(4).

[13] *Gateway Provider Report and Order* at paras. 74-86.

[14] *Id.* at paras. 87-91.

[15] *Id.* at paras. 96-101.

[16] *Id.* at paras 102-08.

[17] *Order on Reconsideration* at paras. 122-54.

[18] *Gateway Provider Notice* at 50-59, Appx. B.

[19] 5 U.S.C. § 604(a)(3).

Apply

8. 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.[20] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[21] In addition, the term "small business" has the same meaning as the term "small-business concern" under the Small Business Act.[22] 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.[23]

9. *Small Businesses, Small Organizations, Small Governmental Jurisdictions.* Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe here, at the outset, three broad groups of small entities that could be directly affected herein.[24] First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, according to data from the Small Business Administration's (SBA) Office of Advocacy, in general a small business is an independent business having fewer than 500 employees.[25] These types of small businesses represent 99.9% of all businesses in the United States, which translates to 32.5 million businesses.[26]

10. 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."[27] 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.[28] 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.[29]

---

[20] *See* 5 U.S.C. § 603(b)(3).

[21] *See* 5 U.S.C. § 601(6).

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

[23] *See* 15 U.S.C. § 632.

[24] *See* 5 U.S.C. § 601(3)-(6).

[25] *See* SBA, Office of Advocacy, Frequently Asked Questions, "What is a small business?," https://cdn.advocacy.sba.gov/wp-content/uploads/2021/11/03093005/Small-Business-FAQ-2021.pdf. (Nov 2021).

[26] *Id*.

[27] *See* 5 U.S.C. § 601(4).

[28] 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. S*ee* Annual Electronic Filing Requirement for Small Exempt Organizations — Form 990-N (e-Postcard), "Who must file,"

https://www.irs.gov/charities-non-profits/annual-electronic-filing-requirement-for-small-exempt-organizations-form-990-n-e-postcard. We note that the IRS data does not provide information on whether a small exempt organization is independently owned and operated or dominant in its field.

[29] *See* Exempt Organizations Business Master File Extract (EO BMF), "CSV Files by Region," https://www.irs.gov/charities-non-profits/exempt-organizations-business-master-file-extract-eo-bmf. The IRS Exempt Organization Business Master File (EO BMF) Extract provides information on all registered tax-

(continued….)

11. 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."[30] U.S. Census Bureau data from the 2017 Census of Governments[31] indicate that there were 90,075 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States.[32] Of this number there were 36,931 general purpose governments (county[33], municipal and town or township[34]) with populations of less than 50,000 and 12,040 special purpose governments - independent school districts[35] with enrollment populations of less than 50,000.[36] Accordingly, based on the 2017 U.S. Census of Governments data, we estimate that at least 48,971 entities fall into the category of "small governmental jurisdictions."[37]

1. Wireline Carriers

12. *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

---

exempt/non-profit organizations. The data utilized for purposes of this description was extracted from the IRS EO BMF data for businesses for the tax year 2020 with revenue less than or equal to $50,000, for Region 1-Northeast Area (58,577), Region 2-Mid-Atlantic and Great Lakes Areas (175,272), and Region 3-Gulf Coast and Pacific Coast Areas (213,840) which includes the continental U.S., Alaska, and Hawaii. This data does not include information for Puerto Rico.

[30] *See* 5 U.S.C. § 601(5).

[31] *See* 13 U.S.C. § 161. The Census of Governments survey is conducted every five (5) years compiling data for years ending with "2" and "7". *See also* Census of Governments, https://www.census.gov/programs-surveys/cog/about html.

[32] *See* U.S. Census Bureau, 2017 Census of Governments – Organization Table 2. Local Governments by Type and State: 2017 [CG1700ORG02], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. 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). *See also* tbl.2. CG1700ORG02 Table Notes_Local Governments by Type and State_2017.

[33] *See id.* at tbl.5. County Governments by Population-Size Group and State: 2017 [CG1700ORG05], https://www.census.gov/data/tables/2017/econ/gus/2017-governments html. There were 2,105 county governments with populations less than 50,000. This category does not include subcounty (municipal and township) governments.

[34] *See id. at* tbl.6. Subcounty General-Purpose Governments by Population-Size Group and State: 2017 [CG1700ORG06], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 18,729 municipal and 16,097 town and township governments with populations less than 50,000.

[35] *See id.* at tbl.10. Elementary and Secondary School Systems by Enrollment-Size Group and State: 2017 [CG1700ORG10], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 12,040 independent school districts with enrollment populations less than 50,000. *See also* tbl.4. Special-Purpose Local Governments by State Census Years 1942 to 2017 [CG1700ORG04], CG1700ORG04 Table Notes_Special Purpose Local Governments by State_Census Years 1942 to 2017.

[36] 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.

[37] 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.

wired communications networks.[38] 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.[39] By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry.[40] Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.[41]

13. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[42] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[43] Of this number, 2,964 firms operated with fewer than 250 employees.[44] 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.[45] Of these providers, the Commission estimates that 4,737 providers have 1,500 or fewer employees.[46] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

14. 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[47] is the closest industry with an SBA small business size standard.[48] Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.[49]

---

[38] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[39] *Id.*

[40] *Id.*

[41] 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.

[42] *See* 13 CFR § 121.201, NAICS Code 517311.

[43] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[44] *Id.* 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.

[45] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[46] *Id.*

[47] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[48] *See* 13 CFR § 121.201, NAICS Code 517311.

[49] 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.[50] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[51] Of this number, 2,964 firms operated with fewer than 250 employees.[52] 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.[53] Of these providers, the Commission estimates that 4,737 providers have 1,500 or fewer employees.[54] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

15. 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[55] is the closest industry with an SBA small business size standard.[56] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[57] U.S. Census Bureau data for 2017 show that there were 3,054 firms in this industry that operated for the entire year.[58] Of this number, 2,964 firms operated with fewer than 250 employees.[59] 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.[60] Of these providers, the Commission estimates that 929 providers have 1,500 or fewer employees.[61] 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.

16. 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.

---

[50] *Id.*

[51] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[52] *Id.* 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.

[53] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[54] *Id.*

[55] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[56] *See* 13 CFR § 121.201, NAICS Code 517311.

[57] *Id.*

[58] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[59] *Id.* 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.

[60] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/public/attachments/DOC-379181A1.pdf.

[61] *Id.*

Providers of these services include several types of competitive local exchange service providers.[62] Wired Telecommunications Carriers[63] 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.[64] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[65] Of this number, 2,964 firms operated with fewer than 250 employees.[66] 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.[67] Of these providers, the Commission estimates that 3,808 providers have 1,500 or fewer employees.[68] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

17. Interexchange Carriers (IXCs). Neither the Commission nor the SBA have developed a small business size standard specifically for Interexchange Carriers. Wired Telecommunications Carriers[69] is the closest industry with an SBA small business size standard.[70] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[71] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[72] Of this number, 2,964 firms operated with fewer than 250 employees.[73] 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

---

[62] 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.

[63] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[64] *See* 13 CFR § 121.201, NAICS Code 517311.

[65] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[66] *Id.* 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.

[67] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[68] *Id.*

[69] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[70] *See* 13 CFR § 121.201, NAICS Code 517311.

[71] *Id.*

[72] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[73] *Id.* 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.

fewer employees.[74] 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.

18. *Cable System Operators (Telecom Act Standard)*. The Communications Act of 1934, as amended, contains a size standard for small cable system operators, which classifies "a cable operator that, directly or through an affiliate, serves in the aggregate fewer than one percent of all subscribers in the United States and is not affiliated with any entity or entities whose gross annual revenues in the aggregate exceed $250,000,000," as small.[75] As of December 2020, there were approximately 45,308,192 basic cable video subscribers in the top Cable MSOs in the United States.[76] Accordingly, an operator serving fewer than 453,082 subscribers shall be deemed a small operator if its annual revenues, when combined with the total annual revenues of all its affiliates, do not exceed $250 million in the aggregate.[77] Based on available data, all but five of the cable operators in the Top Cable MSOs have less than 453,082 subscribers and can be considered small entities under this size standard.[78] We note however, that the Commission neither requests nor collects information on whether cable system operators are affiliated with entities whose gross annual revenues exceed $250 million.[79] Therefore, we are unable at this time to estimate with greater precision the number of cable system operators that would qualify as small cable operators under the definition in the Communications Act.

19. *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[80] is the closest industry with an SBA small business size standard.[81] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[82] U.S. Census Bureau data for 2017 show that there were 3,054 firms in this industry that operated for the entire year.[83] Of this number, 2,964 firms operated with fewer than 250 employees.[84] Additionally, based on Commission data in the 2021 Universal Service Monitoring Report, as of December 31, 2020, there were

---

[74] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/public/attachments/DOC-379181A1.pdf.

[75] 47 U.S.C. § 543(m)(2); *see also* 47 CFR § 76.901(e).

[76] S&P Global Market Intelligence, *Top Cable MSOs 12/20Q, https://platform.marketintelligence.spglobal.com/ (Dec. 2020)*.

[77] 47 CFR § 76.901(e).

[78] S&P Global Market Intelligence, *Top Cable MSOs 12/20Q, https://platform.marketintelligence.spglobal.com (Dec. 2020)*.

[79] 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. *See* 47 CFR § 76.910(b).

[80] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[81] *See* 13 CFR § 121.201, NAICS Code 517311.

[82] *Id.*

[83] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[84] *Id.* 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.

115 providers that reported they were engaged in the provision of other toll services.[85] Of these providers, the Commission estimates that 113 providers have 1,500 or fewer employees.[86] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

2. Wireless Carriers

20. Wireless Telecommunications Carriers (except Satellite). This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves.[87] 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.[88] The SBA size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[89] U.S. Census Bureau data for 2017 show that there were 2,893 firms in this industry that operated for the entire year.[90] Of that number, 2,837 firms employed fewer than 250 employees.[91] 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.[92] Of these providers, the Commission estimates that 715 providers have 1,500 or fewer employees.[93] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

21. *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."[94] 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.[95] U.S. Census Bureau data for 2017 show that 275 firms in this industry operated for the entire year.[96] Of this number, 242 firms had revenue of less than

---

[85] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[86] *Id.*

[87] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers (except Satellite),"* https://www.census.gov/naics/?input=517312&year=2017&details=517312.

[88] *Id.*

[89] *See* 13 CFR § 121.201, NAICS Code 517312.

[90] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[91] *Id.* 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.

[92] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[93] *Id.*

[94] *See* U.S. Census Bureau, *2017 NAICS Definition, "517410 Satellite Telecommunications,"* https://www.census.gov/naics/?input=517410&year=2017&details=517410.

[95] *See* 13 CFR § 121.201, NAICS Code 517410.

[96] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code 517410, https://data.census.gov/cedsci/table?y=2017&n=517410&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

$25 million.[97] 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.[98] Of these providers, the Commission estimates that approximately 48 providers have 1,500 or fewer employees.[99] Consequently using the SBA's small business size standard, a little more than of these providers can be considered small entities.

3. Resellers

22. *Local Resellers*. Neither the Commission nor the SBA have developed a small business size standard specifically for Local Resellers. Telecommunications Resellers is the closest industry with an SBA small business size standard.[100] 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.[101] Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure.[102] Mobile virtual network operators (MVNOs) are included in this industry.[103] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[104] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[105] Of that number, 1,375 firms operated with fewer than 250 employees.[106] 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.[107] Of these providers, the Commission estimates that 289 providers have 1,500 or fewer employees.[108] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

23. *Toll Resellers*. Neither the Commission nor the SBA have developed a small business

---

[97] *Id*. 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. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[98] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[99] *Id.*

[100] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517911 Telecommunications Resellers,*" https://www.census.gov/naics/?input=517911&year=2017&details=517911.

[101] *Id.*

[102] *Id*.

[103] *Id*.

[104] *See* 13 CFR § 121.201, NAICS Code 517911.

[105] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517911, https://data.census.gov/cedsci/table?y=2017&n=517911&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[106] *Id.* 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.

[107] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[108] *Id.*

size standard specifically for Toll Resellers. Telecommunications Resellers[109] 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.[110] Mobile virtual network operators (MVNOs) are included in this industry.[111] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[112] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[113] Of that number, 1,375 firms operated with fewer than 250 employees.[114] 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.[115] Of these providers, the Commission estimates that 495 providers have 1,500 or fewer employees.[116] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

24. *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[117] 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.[118] Mobile virtual network operators (MVNOs) are included in this industry.[119] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[120] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale

[109] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517911 Telecommunications Resellers,*" https://www.census.gov/naics/?input=517911&year=2017&details=517911.

[110] *Id.*

[111] *Id*.

[112] *See* 13 CFR § 121.201, NAICS Code 517911.

[113] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517911, https://data.census.gov/cedsci/table?y=2017&n=517911&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[114] *Id.* 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.

[115] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[116] *Id.*

[117] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517911 Telecommunications Resellers,*" https://www.census.gov/naics/?input=517911&year=2017&details=517911.

[118] *Id.*

[119] *Id*.

[120] *See* 13 CFR § 121.201, NAICS Code 517911.

services for the entire year.[121] Of that number, 1,375 firms operated with fewer than 250 employees.[122] 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.[123] Of these providers, the Commission estimates that 57 providers have 1,500 or fewer employees.[124] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

4. Other Entities

25. *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.[125] 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.[126] Providers of Internet services (e.g. dial-up ISPs) or voice over Internet protocol (VoIP) services, via client-supplied telecommunications connections are also included in this industry.[127] The SBA small business size standard for this industry classifies firms with annual receipts of $35 million or less as small.[128] U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year.[129] Of those firms, 1,039 had revenue of less than $25 million.[130] 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

26. The *Gateway Provider Report and Order* and *Order on Reconsideration* require providers, primarily but not exclusively gateway providers, to meet certain obligations. These changes

---

[121] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517911, https://data.census.gov/cedsci/table?y=2017&n=517911&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[122] *Id.* 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.

[123] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[124] *Id.*

[125] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517919 All Other Telecommunications,*" https://www.census.gov/naics/?input=517919&year=2017&details=517919.

[126] *Id.*

[127] *Id.*

[128] *See* 13 CFR § 121.201, NAICS Code 517919.

[129] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code 517919, https://data.census.gov/cedsci/table?y=2017&n=517919&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[130] *Id.* 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. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

affect small and large companies equally and apply equally to all the classes of regulated entities identified above.

27. *Gateway Provider Report and Order.* The *Gateway Provider Report and Order* requires gateway providers to submit a certification and plan to the Robocall Mitigation Database describing their robocall mitigation practices and stating that they are adhering to those practices, regardless of whether they have fully implemented STIR/SHAKEN. Additionally, downstream domestic providers receiving traffic from gateway providers must block traffic from such a provider if the gateway provider has not submitted a certification in the Robocall Mitigation Database. Gateway providers are not required to describe their mitigation program in a particular manner, but must clearly explain how they are complying with the know-your-upstream-provider obligation adopted in this Order.

28. A gateway provider must certify whether it has fully, partially, or not implemented STIR/SHAKEN, and include a statement in its certification that it commits to responding fully to all traceback requests from the Commission, law enforcement, and the industry traceback consortium and cooperate with such entities in investigating and stopping illegal robocalls. Submissions may be made confidentially consistent with our existing confidentiality rules. All information must be submitted in English or with a certified English translation and updated within 10 business days.[131] Gateway providers must provide the same identifying information submitted by voice service providers.[132]

29. Gateway providers must also implement STIR/SHAKEN to authenticate SIP calls that are carrying a U.S. number in the caller ID field. To comply with this requirement, a gateway provider must authenticate caller ID information for all SIP calls it receives for which the caller ID information has not been authenticated and which it will exchange with another provider as a SIP call consistent with the relevant ATIS standards. Gateway providers have the flexibility to assign the level of attestation appropriate to the call based on the current version of the standards and the call information available to the gateway provider.[133] A gateway provider using non-IP network technology in all or a portion of its network must provide the Commission, upon request, with documented proof that it is participating, either on its own or through a representative, as a member of a working group, industry standards group, or consortium that is working to develop a non-IP solution, or actively testing such a solution. Under this rule, a gateway provider satisfies its obligations if it participates through a third-party representative, such as a trade association of which it is a member or vendor.[134]

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

31. First, gateway providers must fully respond to traceback requests from the Commission, civil and criminal law enforcement, and the industry traceback consortium within 24 hours of receipt of such a request. The gateway provider should respond with information about the provider from which it directly received the call.[135]

32. Second, gateway providers, and in one case, any intermediate or terminating provider immediately downstream from the gateway, must block calls in certain instances. Specifically, the gateway provider must block illegal traffic once notified of such traffic by the Commission through its Enforcement Bureau. In order to comply with this requirement, gateway providers must block traffic that

[131] *Gateway Provider Report and Order* at para. 38.

[132] *Id.* at para. 42.

[133] *Id.* at paras. 51-63.

[134] *Id.* at paras. 62-63.

[135] *Id.* at Section III.E.1.

is substantially similar to the identified traffic on an ongoing basis.[136] When a gateway provider fails to comply with this requirement, the Commission may require providers immediately downstream from a gateway provider to block all traffic from the identified provider when notified by the Commission.[137] As part of this requirement, a notified gateway provider must promptly report the results of its investigation to the Enforcement Bureau, including, unless the gateway provider determines it is either not a gateway provider for any of the identified traffic or that the identified traffic is not illegal, both a certification that it is blocking the identified traffic and will continue to do so and a description of its plan to identify the traffic on an ongoing basis. In order to comply with the downstream provider blocking requirement, all providers must monitor EB Docket No. 22-174 and initiate blocking within 30 days of a Blocking Order being released.[138] Gateway providers must also block based on a reasonable do-not-originate (DNO list). Gateway providers are allowed flexibility to select the list that works best for them, so long as it is reasonable and only includes invalid, unallocated, and unused numbers, as well as numbers for which the subscriber to the number has requested blocking.[139]

33. Third, gateway providers must take reasonable and effective steps to ensure that the immediate upstream provider is not using the gateway provider to originate a high volume of illegal traffic onto the U.S. network. Gateway providers have flexibility to determine the exact measures to take, so long as those steps are effective.[140] Finally, gateway providers must meet a general obligation to mitigate illegal robocalls. Gateway providers are not required to take specific steps to satisfy this obligation, but must implement "reasonable steps" to avoid carrying or processing illegal robocall traffic and must also implement a robocall mitigation program and, as explained below, file that plan along with a certification in the Robocall Mitigation Database.[141]

34. *Order on Reconsideration*. The *Order on Reconsideration* strengthens the existing rule requiring downstream providers to block calls carrying U.S. NANP numbers sent from foreign providers not listed in the Robocall Mitigation Database. It modifies the requirement to apply to calls sent directly from a foreign provider that originates, as well as carries or processes a call carrying a U.S. NANP number. Therefore, a downstream domestic provider must block such calls sent directly from any foreign provider not listed in the Robocall Mitigation Database.[142]

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

35. 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.[143]

36. Generally, the decisions we made in the *Gateway Provider Report and Order* and *Order on Reconsideration* apply to all providers generally, and do not impose unique burdens or benefits on

[136] *Id.* at paras. 75-77.

[137] *Id.* at paras. 78-79.

[138] *Id.* at paras. Section III.E.2.a.

[139] *Id.* at paras. Section III.E.2.b.

[140] *Id.* at paras. Section III.E.3.

[141] *Id.* at paras. Section III.E.4.

[142] *Order on Reconsideration* at paras. 128-35.

[143] 5 U.S.C. § 603.

small providers. Small providers are as capable of being the entry-point onto the U.S. network for illegal calls as large providers, which necessitates equal treatment if we are to protect consumers from these calls. However, we did take steps to ensure that providers, including small providers, would not be unduly burdened by these requirements. Specifically, we allowed flexibility where appropriate to ensure that providers, including small providers, can determine the best approach for compliance based on the needs of their networks. For example, gateway providers have the flexibility to determine their proposed approach to blocking illegal traffic when notified by the Commission, to choose a reasonable DNO list, and to determine the steps they take to "know the upstream provider." A similarly flexible approach applies to the requirement for gateway providers to implement and describe their mitigation plan filed in the Robocall Mitigation Database.

G. Report to Congress

37. The Commission will send a copy of the *Gateway Provider Report and Order* and *Order on Reconsideration*, including this FRFA, in a report to be sent to Congress and the Government Accountability Office pursuant to the Congressional Review Act.[144] In addition, the Commission will send a copy of the *Gateway Provider Report and Order* and *Order on Reconsideration*, including this FRFA, to the Chief Counsel for Advocacy of the Small Business Administration. A copy of the *Gateway Provider Report and Order* and *Order on Reconsideration* (or summaries thereof) will also be published in the Federal Register.[145]

[144] 5 U.S.C. § 801(a)(1)(A).

[145] *See id*. § 604(b).

APPENDIX D

Initial Regulatory Flexibility Analysis

1. As required by the Regulatory Flexibility Act of 1980, as amended (RFA),[1] the Commission has prepared this Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on small entities by the policies and rules proposed in this Further Notice of Proposed Rulemaking (Further Notice). The Commission requests written public comments on this IRFA. Comments must be identified as responses to the IRFA and must be filed by the deadlines for comments provided on the first page of the Further Notice. The Commission will send a copy of the Further Notice, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA).[2] In addition, the Further Notice and IRFA (or summaries thereof) will be published in the Federal Register.[3]

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

2. In order to continue the Commission's work of protecting American consumers from illegal calls, regardless of their provenance, the *Further Notice* proposes to expand some of our existing rules to cover other providers in the call path and provides additional options to further protect American consumers, regardless of whether illegal calls originate domestically or abroad. Specifically, the *Further Notice* proposes to extend our STIR/SHAKEN authentication requirement to cover all domestic providers in the call path.[4] The *Further Notice* also seeks comment on extending some of the robocall mitigation duties we adopt in the *Gateway Provider Report and Order* (*Order*) to all domestic providers in the call path.[5] These mitigation duties include: expanding and modifying our existing affirmative obligations;[6] requiring downstream providers to block calls from non-gateway providers when those providers fail to comply;[7] the general mitigation standard;[8] and filing a mitigation plan in the Robocall Mitigation Database regardless of STIR/SHAKEN implementation status.[9] The *Further Notice* also seeks comment on additional measures to address illegal robocalls, including: ways to enhance the enforcement of our rules;[10] clarifying certain aspects of our STIR/SHAKEN regime;[11] placing limitations on the use of U.S. NANP numbers for foreign-originated calls and indirect number access,[12] and treating cellular roaming traffic differently.[13]

B. Legal Basis

3. The *Further Notice* proposes to find authority largely under those provisions through which it has previously adopted rules to stem the tide of robocalls in its *Call Blocking* and *Call Authentication Orders*. Specifically, the *Further Notice* proposes to find authority under sections 201(b),

---

[1] *See* 5 U.S.C. § 603. The RFA, *see* 5 U.S.C. § 601-612, has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

[2] *See* 5 U.S.C. § 603(a).

[3] *See id*.

[4] *Further Notice* Section VI.A.

[5] *Id*. Section VI.B

[6] *Id*. Section VI.B.1.

[7] *Id*. Section VI.B.2.

[8] *Id*. Section VI.B.3.

[9] *Id*. Section VI.B.4.

[10] *Id*. Section VI.C.

[11] *Id*. Sections VI.D-E, G.

[12] *Id*. Section VI.F.

[13] *Id*. Section VI.H.

202(a), 251(b) and €, 501, 502, and 503 of the Act, section 1.80 of our rules regarding forfeiture amounts, the Truth in Caller ID Act, and, where appropriate, ancillary authority.[14] The *Further Notice* solicits comment on these proposals.

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

4. The RFA directs agencies to provide a description of and, where feasible, an estimate of the number of small entities that may be affected by the proposed rules and by the rule revisions on which the Notice seeks comment, if adopted.[15] The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction."[16] In addition, the term "small business" has the same meaning as the term "small-business concern" under the Small Business Act.[17] 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.[18]

5. *Small Businesses, Small Organizations, Small Governmental Jurisdictions.* Our actions, over time, may affect small entities that are not easily categorized at present. We therefore describe here, at the outset, three broad groups of small entities that could be directly affected herein.[19] First, while there are industry specific size standards for small businesses that are used in the regulatory flexibility analysis, according to data from the Small Business Administration's (SBA) Office of Advocacy, in general a small business is an independent business having fewer than 500 employees.[20] These types of small businesses represent 99.9% of all businesses in the United States, which translates to 32.5 million businesses.[21]

6. *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."[22] 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.[23] Nationwide, for tax year 2020, there

---

[14] *Id*. Section VI.I.

[15] *See* 5 U.S.C. § 603(b)(3).

[16] *See id*. § 601(6).

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

[18] *See* 15 U.S.C. § 632.

[19] *See* 5 U.S.C. § 601(3)-(6).

[20] *See* SBA, Office of Advocacy, Frequently Asked Questions, "What is a small business?," https://cdn.advocacy.sba.gov/wp-content/uploads/2021/11/03093005/Small-Business-FAQ-2021.pdf. (Nov 2021).

[21] *Id*.

[22] *See* 5 U.S.C. § 601(4).

[23] 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. S*ee* Annual Electronic Filing Requirement for Small Exempt Organizations — Form 990-N (e-Postcard), 'Who must file,"

(continued….)

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.[24]

7. 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."[25] U.S. Census Bureau data from the 2017 Census of Governments[26] indicate that there were 90,075 local governmental jurisdictions consisting of general purpose governments and special purpose governments in the United States.[27] Of this number there were 36,931 general purpose governments (county[28], municipal and town or township[29]) with populations of less than 50,000 and 12,040 special purpose governments - independent school districts[30] with enrollment

https://www.irs.gov/charities-non-profits/annual-electronic-filing-requirement-for-small-exempt-organizations-form-990-n-e-postcard. We note that the IRS data does not provide information on whether a small exempt organization is independently owned and operated or dominant in its field.

[24] *See* Exempt Organizations Business Master File Extract (EO BMF), "CSV Files by Region," https://www.irs.gov/charities-non-profits/exempt-organizations-business-master-file-extract-eo-bmf. The IRS Exempt Organization Business Master File (EO 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 EO BMF data for businesses for the tax year 2020 with revenue less than or equal to $50,000, for Region 1-Northeast Area (58,577), Region 2-Mid-Atlantic and Great Lakes Areas (175,272), and Region 3-Gulf Coast and Pacific Coast Areas (213,840) which includes the continental U.S., Alaska, and Hawaii. This data does not include information for Puerto Rico.

[25] *See* 5 U.S.C. § 601(5).

[26] *See* 13 U.S.C. § 161. The Census of Governments survey is conducted every five (5) years compiling data for years ending with "2" and "7". *See also* Census of Governments, https://www.census.gov/programs-surveys/cog/about html.

[27] *See* U.S. Census Bureau, 2017 Census of Governments – Organization Table 2. Local Governments by Type and State: 2017 [CG1700ORG02], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. 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). *See also* tbl.2. CG1700ORG02 Table Notes_Local Governments by Type and State_2017.

[28] *See id*. at tbl.5. County Governments by Population-Size Group and State: 2017 [CG1700ORG05], https://www.census.gov/data/tables/2017/econ/gus/2017-governments html. There were 2,105 county governments with populations less than 50,000. This category does not include subcounty (municipal and township) governments.

[29] *See id*. at tbl.6. Subcounty General-Purpose Governments by Population-Size Group and State: 2017 [CG1700ORG06], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 18,729 municipal and 16,097 town and township governments with populations less than 50,000.

[30] *See id.* at tbl.10. Elementary and Secondary School Systems by Enrollment-Size Group and State: 2017 [CG1700ORG10], https://www.census.gov/data/tables/2017/econ/gus/2017-governments.html. There were 12,040 independent school districts with enrollment populations less than 50,000; *see also* tbl.4. Special-Purpose Local Governments by State Census Years 1942 to 2017 [CG1700ORG04], CG1700ORG04 Table Notes_Special Purpose Local Governments by State_Census Years 1942 to 2017.

populations of less than 50,000.[31] Accordingly, based on the 2017 U.S. Census of Governments data, we estimate that at least 48,971 entities fall into the category of "small governmental jurisdictions."[32]

1. Wireline Carriers

8. *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.[33] 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.[34] By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry.[35] Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.[36]

9. The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[37] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[38] Of this number, 2,964 firms operated with fewer than 250 employees.[39] 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.[40] Of these providers, the Commission estimates that 4,737

---

[31] 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.

[32] 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.

[33] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[34] *Id*.

[35] *Id*.

[36] 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.

[37] *See* 13 CFR § 121.201, NAICS Code 517311.

[38] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[39] *Id*. 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.

[40] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

providers have 1,500 or fewer employees.[41] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

10. *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[42] is the closest industry with an SBA small business size standard.[43] Wired Telecommunications Carriers are also referred to as wireline carriers or fixed local service providers.[44] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[45] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[46] Of this number, 2,964 firms operated with fewer than 250 employees.[47] 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.[48] Of these providers, the Commission estimates that 4,737 providers have 1,500 or fewer employees.[49] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

11. *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[50] is the closest industry with an SBA small business size standard.[51] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[52] U.S. Census Bureau data for 2017 show that there were 3,054 firms in this industry that operated for the entire year.[53] Of this number, 2,964 firms operated with fewer than

---

[41] *Id*.

[42] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[43] *See* 13 CFR § 121.201, NAICS Code 517311.

[44] 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.

[45] *Id*.

[46] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[47] *Id*. 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.

[48] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[49] *Id*.

[50] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[51] *See* 13 CFR § 121.201, NAICS Code 517311.

[52] *Id*.

[53] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311,

(continued….)

250 employees.[54] 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.[55] Of these providers, the Commission estimates that 929 providers have 1,500 or fewer employees.[56] 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.

12. *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.[57] Wired Telecommunications Carriers[58] 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.[59] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[60] Of this number, 2,964 firms operated with fewer than 250 employees.[61] 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.[62] Of these providers, the Commission estimates that 3,808 providers have 1,500 or fewer employees.[63] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

13. We have included small incumbent LECs in this present RFA analysis. As noted above, a "small business" under the RFA is one that, *inter alia*, meets the pertinent small-business size standard (e.g., a telephone communications business having 1,500 or fewer employees) and "is not dominant in its field of operation."[64] The SBA's Office of Advocacy contends that, for RFA purposes, small incumbent

https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[54] *Id*. 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.

[55] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/public/attachments/DOC-379181A1.pdf.

[56] *Id*.

[57] 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.

[58] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[59] *See* 13 CFR § 121.201, NAICS Code 517311.

[60] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[61] *Id*. 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.

[62] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[63] *Id*.

[64] 5 U.S.C. § 601(3).

LECs are not dominant in their field of operation because any such dominance is not "national" in scope.[65] We have therefore included small incumbent LECs in this RFA analysis, although we emphasize that this RFA action has no effect on Commission analyses and determinations in other, non-RFA contexts.

14. *Interexchange Carriers (IXCs)*. Neither the Commission nor the SBA have developed a small business size standard specifically for Interexchange Carriers. Wired Telecommunications Carriers[66] is the closest industry with an SBA small business size standard.[67] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[68] U.S. Census Bureau data for 2017 show that there were 3,054 firms that operated in this industry for the entire year.[69] Of this number, 2,964 firms operated with fewer than 250 employees.[70] 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.[71] 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.

15. *Cable System Operators (Telecom Act Standard)*. The Communications Act of 1934, as amended, contains a size standard for small cable system operators, which classifies "a cable operator that, directly or through an affiliate, serves in the aggregate fewer than one percent of all subscribers in the United States and is not affiliated with any entity or entities whose gross annual revenues in the aggregate exceed $250,000,000," as small.[72] As of December 2020, there were approximately 45,308,192 basic cable video subscribers in the top Cable MSOs in the United States.[73] Accordingly, an operator serving fewer than 453,082 subscribers shall be deemed a small operator if its annual revenues, when combined with the total annual revenues of all its affiliates, do not exceed $250 million in the aggregate.[74] Based on available data, all but five of the cable operators in the Top Cable MSOs have less than 453,082 subscribers and can be considered small entities under this size standard.[75] We note however, that the

---

[65] Letter from Jere W. Glover, Chief Counsel for Advocacy, SBA, to William E. Kennard, Chairman, FCC (filed May 27, 1999). The Small Business Act contains a definition of "small business concern," which the RFA incorporates into its own definition of "small business." 15 U.S.C. § 632(a); 5 U.S.C. § 601(3). SBA regulations interpret "small business concern" to include the concept of dominance on a national basis. 13 CFR § 121.102(b).

[66] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[67] *See* 13 CFR § 121.201, NAICS Code 517311.

[68] *Id*.

[69] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[70] *Id*. 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.

[71] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/public/attachments/DOC-379181A1.pdf.

[72] 47 U.S.C. § 543(m)(2); *see also* 47 CFR § 76.901(e).

[73] S&P Global Market Intelligence, *Top Cable MSOs 12/20Q, https://platform.marketintelligence.spglobal.com/ (Dec. 2020)*.

[74] 47 CFR § 76.901(e).

[75] S&P Global Market Intelligence, *Top Cable MSOs 12/20Q, https://platform.marketintelligence.spglobal.com (Dec. 2020)*.

Commission neither requests nor collects information on whether cable system operators are affiliated with entities whose gross annual revenues exceed $250 million.[76] Therefore, we are unable at this time to estimate with greater precision the number of cable system operators that would qualify as small cable operators under the definition in the Communications Act.

16. *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[77] is the closest industry with an SBA small business size standard.[78] The SBA small business size standard for Wired Telecommunications Carriers classifies firms having 1,500 or fewer employees as small.[79] U.S. Census Bureau data for 2017 show that there were 3,054 firms in this industry that operated for the entire year.[80] Of this number, 2,964 firms operated with fewer than 250 employees.[81] 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.[82] Of these providers, the Commission estimates that 113 providers have 1,500 or fewer employees.[83] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

2. Wireless Carriers

17. *Wireless Telecommunications Carriers (except Satellite)*. This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves.[84] 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.[85] The SBA size standard for this industry classifies a business as small if it has 1,500 or fewer employees.[86] U.S. Census Bureau data for 2017 show that there were 2,893 firms in this

[76] 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. *See* 47 CFR § 76.910(b).

[77] *See* U.S. Census Bureau, *2017 NAICS Definition, "517311 Wired Telecommunications Carriers,"* https://www.census.gov/naics/?input=517311&year=2017&details=517311.

[78] *See* 13 CFR § 121.201, NAICS Code 517311.

[79] *Id*.

[80] *See* U.S. Census Bureau, *2017 Economic Census of the United States, Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517311, https://data.census.gov/cedsci/table?y=2017&n=517311&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[81] *Id*. 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.

[82] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[83] *Id*.

[84] *See* U.S. Census Bureau, *2017 NAICS Definition, "517312 Wireless Telecommunications Carriers (except Satellite),"* https://www.census.gov/naics/?input=517312&year=2017&details=517312.

[85] *Id*.

[86] *See* 13 CFR § 121.201, NAICS Code 517312.

industry that operated for the entire year.[87] Of that number, 2,837 firms employed fewer than 250 employees.[88] 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.[89] Of these providers, the Commission estimates that 715 providers have 1,500 or fewer employees.[90] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

18. ***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."[91] 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.[92] U.S. Census Bureau data for 2017 show that 275 firms in this industry operated for the entire year.[93] Of this number, 242 firms had revenue of less than $25 million.[94] 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.[95] Of these providers, the Commission estimates that approximately 48 providers have 1,500 or fewer employees.[96] Consequently using the SBA's small business size standard, a little more than of these providers can be considered small entities.

3. Resellers

19. *Local Resellers*. Neither the Commission nor the SBA have developed a small business size standard specifically for Local Resellers. Telecommunications Resellers is the closest industry with an SBA small business size standard.[97] The Telecommunications Resellers industry comprises

---

[87] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517312, https://data.census.gov/cedsci/table?y=2017&n=517312&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[88] *Id*. 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.

[89] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[90] *Id*.

[91] *See* U.S. Census Bureau, *2017 NAICS Definition, "517410 Satellite Telecommunications,"* https://www.census.gov/naics/?input=517410&year=2017&details=517410.

[92] *See* 13 CFR § 121.201, NAICS Code 517410.

[93] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code 517410, https://data.census.gov/cedsci/table?y=2017&n=517410&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[94] *Id*. 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. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[95] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[96] *Id*.

[97] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517911 Telecommunications Resellers,*" https://www.census.gov/naics/?input=517911&year=2017&details=517911.

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.[98] Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure.[99] Mobile virtual network operators (MVNOs) are included in this industry.[100] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[101] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[102] Of that number, 1,375 firms operated with fewer than 250 employees.[103] 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.[104] Of these providers, the Commission estimates that 289 providers have 1,500 or fewer employees.[105] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

20. *Toll Resellers*. Neither the Commission nor the SBA have developed a small business size standard specifically for Toll Resellers. Telecommunications Resellers[106] 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.[107] Mobile virtual network operators (MVNOs) are included in this industry.[108] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[109] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[110] Of that number,

---

[98] *Id.*

[99] *Id.*

[100] *Id.*

[101] *See* 13 CFR § 121.201, NAICS Code 517911.

[102] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517911, https://data.census.gov/cedsci/table?y=2017&n=517911&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[103] *Id*. 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.

[104] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[105] *Id*.

[106] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517911 Telecommunications Resellers,*" https://www.census.gov/naics/?input=517911&year=2017&details=517911.

[107] *Id*.

[108] *Id.*

[109] *See* 13 CFR § 121.201, NAICS Code 517911.

[110] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517911, https://data.census.gov/cedsci/table?y=2017&n=517911&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

1,375 firms operated with fewer than 250 employees.[111] 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.[112] Of these providers, the Commission estimates that 495 providers have 1,500 or fewer employees.[113] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

21. *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[114] 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.[115] Mobile virtual network operators (MVNOs) are included in this industry.[116] The SBA small business size standard for Telecommunications Resellers classifies a business as small if it has 1,500 or fewer employees.[117] U.S. Census Bureau data for 2017 show that 1,386 firms in this industry provided resale services for the entire year.[118] Of that number, 1,375 firms operated with fewer than 250 employees.[119] 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.[120] Of these providers, the Commission estimates that 57 providers have 1,500 or fewer employees.[121] Consequently, using the SBA's small business size standard, most of these providers can be considered small entities.

4. Other Entities

22. *All Other Telecommunications.* This industry is comprised of establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications

---

[111] *Id.* 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.

[112] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[113] *Id.*

[114] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517911 Telecommunications Resellers,*" https://www.census.gov/naics/?input=517911&year=2017&details=517911.

[115] *Id.*

[116] *Id.*

[117] *See* 13 CFR § 121.201, NAICS Code 517911.

[118] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Employment Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEEMPFIRM, NAICS Code 517911, https://data.census.gov/cedsci/table?y=2017&n=517911&tid=ECNSIZE2017.EC1700SIZEEMPFIRM&hidePreview=false.

[119] *Id.* 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.

[120] Federal-State Joint Board on Universal Service, Universal Service Monitoring Report at 26, Table 1.12 (2021), https://docs.fcc.gov/*pubId.lic*/attachments/DOC-379181A1.pdf.

[121] *Id.*

telemetry, and radar station operation.[122] 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.[123] Providers of Internet services (e.g. dial-up ISPs) or voice over Internet protocol (VoIP) services, via client-supplied telecommunications connections are also included in this industry.[124] The SBA small business size standard for this industry classifies firms with annual receipts of $35 million or less as small.[125] U.S. Census Bureau data for 2017 show that there were 1,079 firms in this industry that operated for the entire year.[126] Of those firms, 1,039 had revenue of less than $25 million.[127] Based on this data, the Commission estimates that the majority of "All Other Telecommunications" firms can be considered small.

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

23. The *Further Notice* proposes to impose several obligations on various providers, many of whom may be small entities. Specifically, the *Further Notice* proposes to require all U.S. intermediate providers to authenticate caller ID information consistent with STIR/SHAKEN for SIP calls that are carrying a U.S. number in the caller ID field and to require all providers to comply with the most recent version of the standards as they are released.[128] The *Further Notice* also seeks comment on extending certain mitigation duties to all domestic providers, including: (1) extending the requirement to respond to traceback requests from the Commission, civil and criminal law enforcement, and the industry traceback consortium within 24 hours of receipt of the request to all U.S.-based providers in the call path;[129] (2) requiring all domestic providers in the call path to block, rather than simply effectively mitigate, illegal traffic when notified of such traffic by the Commission;[130] and (3) requiring the intermediate provider or terminating provider immediately downstream from an upstream provider that fails to block, or effectively mitigate if we decline to extend the blocking requirement further, illegal traffic when notified by the Commission.[131] It also seeks comment on whether and how to clarify our rule requiring providers to take affirmative, effective measures to prevent new and renewing customers from using their network to originate illegal calls.[132] The *Further Notice* also proposes to extend a general mitigation standard to voice service providers that have implemented STIR/SHAKEN in the IP portions of their networks and to

---

[122] *See* U.S. Census Bureau, *2017 NAICS Definition*, "*517919 All Other Telecommunications,*" https://www.census.gov/naics/?input=517919&year=2017&details=517919.

[123] *Id*.

[124] *Id.*

[125] *See* 13 CFR § 121.201, NAICS Code 517919.

[126] *See* U.S. Census Bureau, *2017 Economic Census of the United States*, *Selected Sectors: Sales, Value of Shipments, or Revenue Size of Firms for the U.S.: 2017,* Table ID: EC1700SIZEREVFIRM, NAICS Code 517919, https://data.census.gov/cedsci/table?y=2017&n=517919&tid=ECNSIZE2017.EC1700SIZEREVFIRM&hidePreview=false.

[127] *Id*. 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. We also note that according to the U.S. Census Bureau glossary, the terms receipts and revenues are used interchangeably, *see* https://www.census.gov/glossary/#term_ReceiptsRevenueServices.

[128] *Further Notice* Section VI.A.

[129] *Id*. Section VI.B.1

[130] *Id*. Section VI.B.1

[131] *Id*. Section VI.B.2.

[132] *Id*. Section VI.B.1.

all domestic intermediate providers.[133] The *Further Notice* also proposes to require all domestic intermediate providers to submit a certification to the Robocall Mitigation Database describing their robocall mitigation practices and stating that they are adhering to those practices, regardless of whether they have fully implemented STIR/SHAKEN.[134]

24. With regard to our enforcement of these proposed rules, the *Further Notice* proposes to: (1) impose forfeitures for failures to block calls on a per-call basis and establish a maximum forfeiture amount for such violations; (2) impose the highest available forfeiture for failures to appropriately certify in the Robocall Mitigation Database; (3) establish additional bases for removal from the Robocall Mitigation Database, including by establishing a "red light" feature to notify the Commission when a newly-filed certification lists a known bad actor as a principal, parent company, subsidiary, or affiliate; and (4) 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.[135]

25. The *Further Notice* seeks comment on whether certain of our rules regarding caller ID authentication and attestation in the Robocall Mitigation Database require clarification, specifically whether the Commission should allow a third party to authenticate caller identification information to satisfy the originating provider's obligation, and whether our rules regarding filing in the Robocall Mitigation Database should be amended to require attestation of STIR/SHAKEN implementation by the originating provider itself.[136] The *Further Notice* also seeks comment on whether additional clarity is needed regarding the Commission's rules about certain providers lacking facilities to implement STIR/SHAKEN.[137]

26. The *Further Notice* also seeks comment on whether the TRACED Act applies to satellite providers, and, if so, whether we should grant such providers an extension for implementing STIR/SHAKEN.[138]

27. The *Further Notice* seeks comment on possible changes to our numbering rules to prevent the misuse of numbering resources to originate illegal robocalls, particularly those originating abroad, including: (1) whether we should adopt restrictions on the use of domestic numbering resources for calls that originate outside of the United States for termination in the United States; and (2) whether we should impose any restrictions on indirect access to U.S. NANP numbers to prevent their use by foreign or domestic robocallers.[139]

28. Lastly, the *Further Notice* seeks comment on stakeholders' argument that cellular roaming traffic (i.e., traffic originated abroad from U.S. mobile subscribers carrying U.S. NANP numbers terminated in the U.S.) should be treated with a "lighter touch" because it is unlikely to carry illegal robocalls.[140]

E. Steps Taken to Minimize the Significant Economic Impact on Small Entities, and

[133] *Id*. Section VI.B.3.

[134] *Id*. Section VI.B.4.

[135] *Id*. Section VI.C.

[136] *Id*. Section VI.D.

[137] *Id*. Section VI.E.

[138] *Id*. Section VI.F.

[139] *Id*. Section VI.G.

[140] *Id*. Section VI.H.

Significant Alternatives Considered

29. The RFA requires an agency to describe any significant alternatives that it has considered in reaching its proposed approach, which may include the following four alternatives (among others): (1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance and reporting requirements under the rules for such small entities; (3) the use of performance rather than design standards; and (4) an exemption from coverage of the rule, or any part thereof, for such small entities.[141]

30. The *Further Notice* seeks comment on the particular impacts that the proposed rules may have on small entities. In particular, it seeks comment on the impact on small providers of extending the requirement to respond to traceback requests from the Commission, civil and criminal law enforcement, and the industry traceback consortium within 24 hours of receipt of the request to all U.S.-based providers in the call path.[142] The *Further Notice* recognizes that providers that do not receive many requests may be less familiar with the process, and that smaller providers in particular may struggle to respond quickly, and it seeks comment on whether the waiver process established in the Report and Order is sufficient to address the needs of all providers, or whether it should be modified to allow greater flexibility.[143] In particular, the *Further Notice* seeks comment on whether we should adopt an approach to traceback based on volume of requests received, rather than position in the call path or size of provider. For example, the *Further Notice* asks whether the Commission should adopt a tiered approach that requires providers with fewer than 10 traceback requests a month to respond "fully and timely," without the need to maintain an average response time of 24 hours; requires providers that receive from 10 to 99 traceback requests a month to respond within 24 hours or request a waiver and maintain an average response time of 24 hours; and requires providers with 100 or more traceback requests a month to always respond within 24 hours, barring exceptional circumstances.[144] The *Further Notice* also seeks comment on whether the TRACED Act applies to satellite providers and, if so, whether we should grant such providers an extension for implementing STIR/SHAKEN.[145] The *Further Notice* seeks comment on whether a *de minimis* number of satellite provider subscribers use NANP resources, and whether there should thus be a *de minimis* exception to our rules.[146] The *Further Notice* notes that the Commission has previously provided small voice services providers, including satellite providers, an extension from STIR/SHAKEN implementation until June 30, 2023, and seeks comment on whether we should grant an indefinite extension for satellite providers or, in the alternative, a defined continuing extension.[147]

F. Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rules

None.

STATEMENT OF
CHAIRWOMAN JESSICA ROSENWORCEL

Re: *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59; *Call Authentication Trust Anchor,* WC Docket No. 17-97; Report and Order, Order on Reconsideration, Order, and Further Notice of Proposed Rulemaking (May 19, 2022)

[141] 5 U.S.C. § 603(c)(1)-(4).

[142] *Id.* Section VI.B.1.

[143] *Id.*

[144] *Id.*

[145] *Id.* Section VI.F.

[146] *Id.*

[147] *Id.*

Robocalls are aggravating. What is worse is when we crack down on these junk calls, the scam artists behind them find new ways to reach us. Increasingly, that means robocalls are coming in from overseas. In fact, one study suggests that last year as much as two-thirds of this stuff may now come from abroad.

So today we get tough on international robocalls. That's because we need to cut these calls off before they reach our shores, our homes, and our phones.

In practice, what this means is that we are making gateway providers—the carriers that serve as the domestic entry point for calls from abroad—use STIR/SHAKEN call authentication technology, register in our Robocall Mitigation Database, and comply with traceback requests from the Federal Communications Commission and law enforcement to help figure out where these junk calls are originating from overseas.

These measures will help us tackle the growing number of international robocalls. Because we can't have these scam artists multiplying abroad and hiding from our regulatory reach. We also can't have them hiding from our state counterparts. That is why I am proud that today we are announcing that we now have 36 State Attorneys General who have signed a Memorandum of Understanding with the FCC to share resources and information to crack down on robocalls.

This is progress. But we do need additional authority over robocalls to fight this scourge on all fronts. Last year the Supreme Court narrowed the definition of autodialer in a case involving the Telephone Consumer Protection Act. It's perverse, because their decision leads to less consumer protection from these annoying calls. We need help from Congress to fix that. We also need more tools from Congress to catch those behind these calls, including the ability to go to court directly and collect fines from these bad actors—each and every one of them.

Thank you to the Robocall Response Team for their efforts on gateway providers, including Jerusha Burnett, Aaron Garza, Alejandro Roark, Karen Schroeder, Mark Stone, and Kristi Thornton from the Consumer and Governmental Affairs Bureau; Lisa Gelb, Daniel Stepanicich, Kristi Thompson, and Lisa Zaina from the Enforcement Bureau; Kimberly Cook and Jim Schlichting from the International Bureau; Belford Lawson, Maura McGowan, and Joy Ragsdale from the Office of Communications Business Opportunities; Eugene Kiselev, Virginia Metallo, Mark Montano, Chuck Needy, Michelle Schaefer, and Emily Talaga from the Office of Economics and Analytics; Valerie Hill, Richard Mallen, Linda Oliver, William Richardson, and Derek Yeo from the Office of General Counsel; Cathy Williams from the Office of the Managing Director; Kenneth Carlberg and David Furth from the Public Safety and Homeland Security Bureau; and Pam Arluk, Allison Baker, Michele Berlove, Matt Collins, Megan Capasso Danner, Elizabeth Drogula, Jesse Goodwin, Trent Harkrader, Jonathan Lechter, Zach Ross, and John Visclosky from the Wireline Competition Bureau.

STATEMENT OF
COMMISSIONER GEOFFREY STARKS

Re: *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59; *Call Authentication Trust Anchor,* WC Docket No. 17-97; Report and Order, Order on Reconsideration, Order, and Further Notice of Proposed Rulemaking (May 19, 2022)

Our battle against illegal and unwanted robocalls continues. Robocalls continue to be the biggest source of complaints the Commission receives. So far this year, the Commission has received 43,800 robocall complaints. Now is not the time to take our foot off the gas, because according to YouMail, there were 3.9 billion robocalls placed last month.[1] This is far too many, but a positive sign is the number is trending downward from last year. Thus, while we have taken great strides in partnership with industry to mitigate robocalls, more work remains. Today, we take another important step. This item adopts significant new requirements, and also proposes to go further to stop robocalls before they reach us at home, work, or on the move.

The item we adopt today takes robust steps to stop robocalls before they reach our domestic networks. Critically, gateway providers' networks are the point of entry for foreign-originated robocalls, which is where the vast majority of robocalls originate. If we can make it more difficult for these illegal and unwanted calls to hit our networks, we will be much closer to winning the fight against robocalls.

So, I support requiring gateway providers to apply STIR/SHAKEN caller ID authentication to unauthenticated foreign-originated SIP calls with U.S. numbers in the caller ID field. I also support requiring these providers to adopt robocall mitigation programs. Authenticating calls is a key part of STIR/SHAKEN, and this requirement will help close a loophole that bad actors use. The item rightly identifies that that while STIR/SHAKEN is effective, alone it isn't enough. All carriers should be mitigating robocall traffic as well. I urge carriers that may not already be required to do so, to start now.

But, at the same time, I recognize the significant efforts that these gateway providers, and many providers in general have already undertaken. Many of these gateway providers are using a variety of tools, including analytics and robocall mitigation practices, to help fight robocalls. I'm confident that these tools, when added with the requirements adopted today, will be even more effective.

We must also highlight the importance of enforcement of our rules. If we cannot enforce our rules, we are fighting with one hand behind our back. So, I support the requirement that gateway providers respond to traceback requests within 24 hours of such a request. It is integral that providers quickly respond so that the Commission, providers, and law enforcement can identify the source of illegal calls and act swiftly.

I am also glad to support empowering the Enforcement Bureau to notify gateway providers of illegal traffic, and thereby requiring gateway providers, and in some circumstances, providers immediately downstream in the call path, to block not just the robocall traffic, but all calls from the identified provider. This is an important incentive to providers to keep illegal traffic off your networks, and a shot across the bow to bad actors. Do not bring illegal calls to the United States, and if you do, your traffic will be blocked. It is time for us to deploy all tools in our enforcement authority to stop and punish the bad actors that support these calls.

I also support an expansion of the requirement for providers to file in the Robocall Mitigation Database. The Database has been a success. And, it has seen an increasing number of foreign providers submit information. I hope that today's order will further incentivize gateway providers to push their foreign partners to implement STIR/SHAKEN and file in the Database. Expanding STIR/SHAKEN

[1] U.S. Phones Received Over 3.9 Billion Robocalls in April, Says YouMail Robocall Index, https://www.prnewswire.com/news-releases/us-phones-received-over-3-9-billion-robocalls-in-april-says-youmail-robocall-index-301540784 html (May 5, 2022).

deployments abroad will only help to fight robocalls, as robocalls are truly an international problem.

The Further Notice proposes to take additional steps that will bring us closer to an important goal of mine -- regulatory symmetry for all providers: voice, gateway, and intermediary. We currently have different obligations on voice and gateway provides than United States intermediate providers. Bad actors can and do take advantage of these regulatory arbitrage opportunities.

I'm also heartened to see a request in the Further Notice for comment on strengthening enforcement. If we identify a bad actor, it's time to make it harder to operate. If it's a repeat offender, we should go further. I look forward to seeing the record develop on how to strengthen enforcement, and I appreciate the Chairwoman taking my request to lower the proposed attributable interest threshold that a repeater offender may own from 10% down to 5%. Repeat offenders here need to have their control and influence limited.

Overall, this is an important item and a positive step. I'm optimistic that these new requirements, plus our increased emphasis on enforcement, will continue to make it harder for robocalls to proliferate. I will continue to remain vigilant in pushing the Commission to do all it can to eliminate these illegal and unwanted calls going forward. I thank the Commission staff that continues to tirelessly labor on these issues for all their hard work. I approve.