6712-01

This document is scheduled to be published in the Federal Register on 10/26/2021 and available online at **federalregister.gov/d/2021-23164**, and on **govinfo.gov**

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Part 64

[CG Docket No. 17-59, WC Docket No. 17-97; FCC 21-105; FR ID 53781]

Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor

AGENCY: Federal Communications Commission

ACTION: Proposed rule

SUMMARY: In this document, the Commission adopted a Further Notice of Proposed Rulemaking that proposes and seeks comment on a number of actions aimed at stopping illegal robocalls from entering U.S. networks. The document proposes to require gateway providers to apply STIR/SHAKEN caller ID authentication to, and perform robocall mitigation on, foreign-originated calls with U.S. numbers. It also proposes and seeks comment on a number of additional requirements to ensure that gateway providers take steps to prevent foreign-originated calls from entering the U.S. network.

DATES: Comments are due on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**, and reply comments are due on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. Written comments on the Paperwork Reduction Act proposed information collection requirements must be submitted by the public, Office of Management and Budget (OMB), and other interested parties on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

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

Proceedings, 63 FR 24121 (1998). Interested parties may file comments or reply comments, identified by CG Docket No. 17-59 and WC Docket No. 17-97 by any of the following methods:

- *Electronic Filers*: Comments may be filed electronically using the Internet by accessing ECFS: https://www.fcc.gov/ecfs/.
- *Paper Filers*: Parties who choose to file by paper must file an original and one copy of each filing.
- Filings can be sent by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.
- Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701.
- U.S. Postal Service first-class, Express, and Priority mail must be addressed to 45 L Street NE, Washington, DC 20554.
- Effective March 19, 2020, and until further notice, the Commission no longer accepts any hand or messenger delivered filings. This is a temporary measure taken to help protect the health and safety of individuals, and to mitigate the transmission of COVID-19. See *FCC Announces Closure of FCC Headquarters Open Window and Change in Hand-Delivery Policy*, Public Notice, 35 FCC Rcd 2788 (March 19, 2020), https://www.fcc.gov/document/fcc-closes-headquarters-open-window-and-changes-hand-delivery-policy.

In addition to filing comments with the Secretary, a copy of any comments on the Paperwork Reduction Act proposed information collection requirements contained herein should be submitted to the Federal Communications Commission via email to PRA@fcc.gov and to Nicole Ongele, FCC, via email to Nicole.Ongele@fcc.gov.

FOR FURTHER INFORMATION CONTACT: For further information, please contact either Jonathan Lechter, Attorney Advisor, Competition Policy Division, Wireline Competition

Bureau, at Jonathan.lechter@fcc.gov or at (202) 418-0984, or Jerusha Burnett, Attorney Advisor, Consumer Policy Division, Consumer and Governmental Affairs Bureau, at jerusha.burnett@fcc.gov. For additional information concerning the Paperwork Reduction Act proposed information collection requirements contained in this document, send an email to PRA@fcc.gov or contact Nicole Ongele at (202) 418-2991.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Fifth Further Notice of Proposed Rulemaking and Fourth Further Notice of Proposed Rulemaking (*FNPRM*) in CG Docket No. 17-59 and WC Docket No. 17-97, FCC 21-105, adopted on September 30, 2021, and released on October 1, 2021. The full text of this document is available for public inspection at the following internet address: https://docs.fcc.gov/public/attachments/FCC-21-105A1.pdf. To request materials in accessible formats for people with disabilities (e.g. braille, large print, electronic files, audio format, etc.), send an email to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at (202) 418-0530 (voice), or (202) 418-0432 (TTY).

Initial Paperwork Reduction Act of 1995 Analysis

This document contains proposed information collection requirements. The Commission, as part of its continuing effort to reduce paperwork burdens, invites the general public to comment on the information collection requirements contained in this document, as required by the Paperwork Reduction Act of 1995, Public Law 104-13.

Comments should address: (a) whether the proposed collection of information is necessary for the proper performance of the functions of the Commission, including whether the information shall have practical utility; (b) the accuracy of the Commission's burden estimates; (c) ways to enhance the quality, utility, and clarity of the information collected; (d) ways to minimize the burden of the collection of information on the respondents, including the use of automated collection techniques or other forms of information technology; and (e) way to further reduce the information collection burden on small business concerns with fewer than 25 employees. 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.

Synopsis

I. INTRODUCTION

1. In this Further Notice of Proposed Rulemaking (FNPRM), we propose to take decisive action to stem the tide of foreign-originated illegal robocalls. Eliminating illegal robocalls that originate abroad is one of the most vexing challenges we face in eliminating the scourge of robocalling because of the difficulties presented by foreign-based robocallers. The rules we propose today will help to address this problem by placing new obligations on the gateway providers that are the point of entry for foreign calls into the United States, requiring them to lend a hand in the fight against illegal robocalls originating abroad.

2. Specifically, we propose to require gateway providers to apply STIR/SHAKEN caller ID authentication to, and perform robocall mitigation on, foreign-originated calls with U.S. numbers. This proposal would subject foreign-originated calls, once they enter the United States, to requirements similar to those of domestic-originated calls, by placing additional obligations on gateway providers in light of the large number of illegal robocalls that originate abroad and the risk such calls present to Americans. We further propose and seek comment on a number of additional robocall mitigation requirements to ensure that gateway providers take steps to prevent illegal calls from entering the U.S. network. Doing so will continue our aggressive and multi-pronged approach to combatting illegal robocalls.

3. We also take this opportunity to make general improvements to our anti-robocalling rules by seeking comment on revisions to the information that filers must submit to the Robocall Mitigation Database and by clarifying the obligations of voice service providers and intermediate providers with respect to calls to and from Public Safety Answer Points (PSAPs) and other emergency services providers.

II. BACKGROUND

4. Unwanted calls, which include illegal robocalls, are consistently the Commission's top source of consumer complaints. The Commission received approximately 232,000 such complaints in 2018, 193,000 in 2019, 154,000 in 2020, and 131,000 in 2021 as of September 28th. 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. Consumer harm from unwanted and illegal calls ranges from simple irritation to fraud and financial loss. In fact, the Federal Trade Commission (FTC) reports that American consumers lost $436 million to fraud over the phone and $86 million to fraud by text message in 2020. This reported fraud is only a fraction of the approximately $13.5 billion in estimated annual costs from illegal robocalls. Caller ID spoofing—the practice whereby a caller misrepresents, or "spoofs," the information in the caller ID field—poses a particular problem because the identity of the calling party is falsified.

5. The Commission and Congress have long acknowledged that illegal robocalls that originate abroad are a significant part of the robocall problem. 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." Congress highlighted this problem in 2018, when it amended the Communications Act of 1934, as amended (the Act), to prohibit spoofing calls or texts originating outside the U.S. Similarly, in 2020, the North American Numbering Council (NANC), the Commission's advisory committee of outside experts on telephone numbering matters, stated that "it is a long-standing problem that international gateway traffic is a significant source of fraudulent traffic." While these calls pose a significant problem, our jurisdiction does not generally apply directly to foreign entities.

6. *Types of Illegal Calls.* Illegal calls can come in many forms. Perhaps the most well-known illegal calls are those that are simply fraudulent, where the caller poses as a

business, or even a government entity, in order to obtain payment or personal information. Fraudulent calls may violate any of a number of state or federal statutes. These calls can take a number of forms, but some common scams include callers posing as the Internal Revenue Service (IRS) or Social Security Administration (SSA), scams following natural disasters, or auto warranty scams. The IRS continues to warn consumers about phone scams, or "vishing" as part of its annual "Dirty Dozen" scams, stating that while overall it has seen a decline in reports of scammers claiming to be the IRS, consumers should remain cautious. The SSA also warns consumers to be wary of phone scams, providing tips to consumers on how to recognize these calls. Taken together, the FTC received over 700,000 reports of fraud by phone or text in 2020 alone.

7. But calls need not be fraudulent to be illegal. Calls can violate the Telephone Consumer Protection Act (TCPA), which 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. The TCPA exempts from this prohibition calls for emergency purposes. In addition, in all but one instance, artificial or prerecorded voice messages must state the identity of the business, individual, or other entity that is responsible for initiating the call clearly at the beginning of the message as well as the telephone number either during or at the end of the message. Finally, the TCPA authorizes the Commission to adopt regulatory exemptions to 47 U.S.C. 227(b)(1)(B) for certain types of calls, including those not made for commercial purposes or that do not include an unsolicited advertisement. 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. The TCPA grants the Commission authority to exempt certain calls from the requirements of 47 U.S.C. 227(b)(1)(A)(iii).

8. Calls are also illegal in some instances where the caller ID information has been spoofed. The Truth in Caller ID Act of 2009 made it illegal to transmit false or misleading caller ID information in order to defraud, cause harm, or wrongfully obtain something of value. And as we explained, in 2018, Congress extended this prohibition to reach spoofing activities directed at consumers in the United States from foreign actors, and applied the prohibition to alternative voice and text message services.

9. 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. 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. When an entity knowingly uses a number that does not belong to it "to make a large number of calls . . . the intent to harm may be imputed" to the spoofing entity. Moreover, the Commission has found that repeated spoofing of unassigned numbers is "a strong indication" that the caller has the intent to defraud or cause harm.

10. *STIR/SHAKEN Caller ID Authentication.* While the Truth in Caller ID Act made spoofing illegal in certain instances, it did not by itself solve a fundamental technical problem: how to identify spoofing in the first instance and track down the call originator after discovering spoofing had occurred. To address this challenge, technologists from the Internet Engineering Task Force (IETF) and the Alliance for Telecommunications Industry Solutions (ATIS) developed standards to allow for the authentication and verification of caller ID information carried over Internet Protocol (IP) networks. The result of their efforts is the STIR/SHAKEN

caller ID authentication framework, which allows for authenticated caller ID information to securely travel with the call itself throughout the entire length of the call path. More specifically, a working group of the IETF called the Secure Telephony Identity Revisited (STIR) developed several protocols for authenticating caller ID information. And 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. The Commission, consistent with Congress's direction in the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act, adopted rules requiring voice service providers to implement STIR/SHAKEN in the IP portions of their voice networks by June 30, 2021, subject to certain exceptions. In this Further Notice of Proposed Rulemaking, we use the terms "voice service provider" and "intermediate provider" consistent with the definitions in Part 64, Subpart HH of the Commission's rules, unless otherwise specified. Thus, "voice service provider" as used in this FNPRM refers, unless otherwise specified, to a provider of "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" and "intermediate provider" refers to "any entity that carries or processes traffic that traverses or will traverse the PSTN at any point insofar as that entity neither originates nor terminates that traffic." The term "voice service provider" has a different meaning in the Commission's *Call Blocking* Orders, and there includes intermediate providers. Our use of the term "voice service provider" in this FNPRM does not expand on or narrow that phrase as used in those Orders and associated rules.

11. At a high level, 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. Regarding the technical process, STIR/SHAKEN requires that the provider authenticating the call attach additional, encrypted information to the metadata that travels along

with a call, which allows the terminating voice service provider to verify that the caller ID is legitimate. The authenticating provider must include in this information its own identity as the provider that authenticated the call and an "attestation level" to signify what it knows about the calling party and its right to use the number in the caller ID. The current STIR/SHAKEN standards allow for three attestation levels. The highest level of attestation—called "full" or "A-level"—asserts that the authenticating provider can confirm the identity of the subscriber making the call and that it is using its associated telephone number. The next-highest level of attestation—called "partial" or "B-level"—asserts that the authenticating provider can confirm the identity of the subscriber but not the telephone number. The lowest level of attestation—called "gateway" or "C-level"—asserts only that the provider is the point of entry to the IP network for a call that originated elsewhere and has no relationship to the call initiator. The authenticating provider must also include a digital "certificate" which says, in essence, that the provider is the entity it claims to be and that it has the right to authenticate the caller ID information.

12. To maintain trust and accountability in the providers that vouch for the caller ID information, a neutral governance system issues these certificates. The STIR/SHAKEN governance system requires several roles in order to operate: (1) a Governance Authority, which defines the policies and procedures for which entities can issue or acquire certificates (This role is currently filled by the Secure Telephone Identity Governance Authority); (2) a Policy Administrator, which applies the rules set by the Governance Authority, confirms that Certification Authorities are authorized to issue certificates, and confirms that voice service providers are authorized to request and receive certificates (After a request for proposals process, the Governance Authority selected iconectiv to fill this role); (3) Certification Authorities, which issue the certificates used to authenticate and verify calls (As the Policy Administrator, iconectiv vets and approves organizations interested in serving as a Certification Authority. The Policy Administrator website reflects that there are currently eight approved Certification Authorities.); and (4)

the authenticating providers themselves, which select an approved Certification Authority from which to request a certificate. Under the current Governance Authority rules, a provider must meet certain requirements to receive a certificate.

13. The Commission requires voice service providers subject to an extension from the requirement to implement STIR/SHAKEN—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. The Commission specifically directed voice service providers that must implement robocall mitigation to "take reasonable steps to avoid originating illegal robocall traffic." The Commission adopted this standards-based approach to "allow . . . voice service providers to innovate and draw from the growing diversity and sophistication of anti-robocall tools and approaches available," and because it found that "there is no one-size-fits-all robocall mitigation solution that accounts for the variety and scope of voice service provider networks." The prohibition went into effect on September 28, 2021. The Commission established just one prescriptive requirement: a commitment to respond "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." The Commission explained that if it 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."

14. The Commission also required voice service providers to, by June 30, 2021, 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." The Commission stated that a robocall mitigation program is sufficient if it "includes detailed practices that can reasonably be expected to significantly reduce the origination of illegal

robocalls," and stated that "the voice service provider must comply with the practices it describes." As of September 28, 2021, 4,948 voice service providers have filed in the Robocall Mitigation Database: 1,302 attest to full STIR/SHAKEN implementation, 1,202 state that they have implemented a mix of STIR/SHAKEN and robocall mitigation, and 2,437 state that they rely solely on robocall mitigation.

15. The Commission prohibited intermediate providers and terminating voice service providers from accepting calls directly from a voice service provider not listed in the Robocall Mitigation Database, finding that such a prohibition would "encourage all voice service providers to implement meaningful and effective robocall mitigation programs . . . during the period of extension from the STIR/SHAKEN mandate." The Commission extended this prohibition to traffic originated 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." We note that CTIA and the Voice on the Net Coalition (VON) filed petitions for reconsideration of the prohibition as it relates to foreign-originated traffic. This prohibition became effective on September 28, 2021. While the Commission made clear that it did "not require foreign voice service providers to file a certification," it found that the rule "create[d] a strong incentive for . . . foreign voice service providers" to do so to avoid having their traffic blocked. The Commission concluded that the rule's "indirect effect" on foreign providers is consistent with the Commission's and courts' past conclusions regarding the scope of Commission jurisdiction. As of September 28, 2021, 609 foreign voice service providers have filed in the Robocall Mitigation Database, out of a total 4,948 voice service provider filings.

16. 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 placed two requirements on intermediate providers. First, regarding calls an intermediate provider receives

with authenticated caller ID information, the Commission required intermediate providers to pass the authenticated caller ID information unaltered to the next provider in the call path. 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. Second, regarding calls an intermediate provider receives without authenticated caller ID information, the Commission gave intermediate providers two options. An intermediate provider could either authenticate caller ID information for these calls, or, in the alternative, an intermediate provider must cooperatively participate with the industry traceback consortium and respond fully and in a timely manner to all traceback requests. The Commission concluded that it had authority to place these obligations on intermediate providers under section 251(e) of the Act and the Truth in Caller ID Act.

17. In adopting these rules, the Commission defined "voice service," consistent with section 4 of the TRACED Act, in part 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." It defined an "intermediate provider" as "any entity that [carries] or processes traffic that traverses or will traverse the PSTN at any point insofar as that entity neither originates nor terminates that traffic." The Commission also established that its rules governing voice service providers and intermediate providers apply on a "call-by-call" basis; under this approach, "[a] single entity . . . may act as a voice service provider for some calls on its network and an intermediate provider for others."

18. *Call Blocking.* In parallel with its caller ID authentication work, the Commission has encouraged voice service providers, including intermediate providers, to block unwanted and illegal calls in certain situations, while also imposing requirements to reduce the risk that

legitimate calls are blocked. Similarly, the Commission has adopted affirmative obligations for voice service providers, which include intermediate providers for purposes of our call blocking rules, to help eliminate illegal calls from the network.

19. To date, the Commission has taken a mostly permissive approach to call blocking, encouraging terminating voice service providers and, occasionally, all voice service providers (including intermediate providers) to block in certain instances and protecting them from liability under the Commission's rules if they block in error. The Commission, in the 2017 *First Call Blocking Order*, took a clear, bright-line approach by authorizing voice service providers, including intermediate providers, to block calls that purport to be from invalid, unallocated, or unused numbers without first obtaining customer consent. The Commission reasoned that there is no legitimate reason for a caller to spoof these numbers, and therefore these calls are highly likely to be illegal. As a result, no reasonable consumer would want to receive such calls. The *First Call Blocking Order* also permitted blocking of calls using a do-not-originate list, which includes numbers that should never be used to originate calls. The Commission determined that these rules apply to foreign-originated calls that purport to originate from U.S. North American Numbering Plan (NANP) numbers on the grounds that many illegal calls originate from call centers abroad.

20. Subsequent Commission action ensured that terminating voice service providers can respond to the evolving tactics of bad actors. First, in the *Call Blocking Declaratory Ruling and Further Notice of Proposed Rulemaking*, adopted in 2019, the Commission made clear that terminating voice service providers may block calls based on reasonable analytics so long as consumers are given the opportunity to opt out of such blocking. The Commission, in the 2020 *Third Call Blocking Order and Further Notice of Proposed Rulemaking*, then adopted a safe harbor from violations of the Act and the Commission's rules for terminating voice service 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. The *Second Report and Order* in CG Docket No. 17-59 concerns the Reassigned Numbers Database and is not directly relevant to our discussion here. The Commission also established a safe harbor for voice service providers (including intermediate providers) 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. Finally, the Commission, in that *Order*, took steps to reduce the risk of erroneous blocking. In the 2020 *One Ring Scam Order*, the Commission permitted voice service providers (including intermediate providers) to use reasonable analytics on a network-wide basis to block calls from numbers that are highly likely to be associated with one-ring scams and extended the existing safe harbor to include such blocking. Providers may block such calls if they "appear to be one-ring scam calls, even if such identification proves to be erroneous in a particular instance."

21. Most recently, in the December 2020 *Fourth Call Blocking Order*, the Commission expanded the safe harbor for blocking based on reasonable analytics to include certain network-level blocking, without consumer opt out, designed to identify calls that are highly likely to be illegal. The safe harbor is available to terminating voice service providers that disclose to consumers that they are engaging in such blocking. The Commission also adopted enhanced transparency and redress requirements for voice service providers that block calls. Beyond blocking, the Commission, in the *Fourth Call Blocking Order*, established three affirmative obligations that apply to voice service providers (including intermediate providers). First, voice service providers must respond to all traceback requests from the Commission, law enforcement, or the industry traceback consortium, fully and timely. Second, voice service providers must take steps to effectively mitigate illegal traffic when notified of such traffic by the Commission. The Commission noted that "blocking may be necessary for gateway providers to comply with these requirements." Finally, voice service providers must adopt affirmative, effective measures to prevent new and renewing customers from using the network to originate illegal calls.

III. DISCUSSION

22. Now that voice service providers have implemented STIR/SHAKEN or a robocall mitigation program, a key component of our anti-robocall efforts is in effect. However, bad actors abroad continue to remain largely outside of our caller ID authentication scheme. At present, our rules only require the gateway providers that bring foreign calls into the United States to pass along preexisting authenticated caller ID information unaltered, participate in traceback, and take steps to effectively mitigate illegal traffic when notified of such traffic by the Commission. While these obligations are valuable, they are not enough for the task at hand: stopping illegal robocalls that originate abroad and the fraudulent actors producing those calls from preying on Americans.

23. To that end, we propose to place additional requirements on gateway providers to ensure that they are doing their part to combat the scourge of illegal robocalls. Specifically, we propose to require gateway providers to authenticate all SIP calls and employ robocall mitigation techniques on calls that they allow into the United States from abroad that display a U.S. number in the caller ID field, which implies to the call recipient that the call originated in the United States. In this FNPRM, where we refer to caller ID information or the number in the caller ID field, we rely on the definition of "caller identification information" in our rules.

A. Need for Action

24. *Current Rules Addressing Foreign-Originated Robocalls Are Insufficient*. We tentatively conclude that our current rules addressing foreign-originated robocalls are not sufficient to resolve the problem of foreign-originated illegal robocalls:

- Under our caller ID authentication rules, gateway providers—as intermediate providers—are required to pass along authenticated caller ID information unaltered. Although intermediate providers are also required to apply STIR/SHAKEN to unauthenticated calls they receive, they are excused from that requirement if they elect to cooperatively participate with the industry traceback consortium and respond fully and in a timely

manner to all traceback requests they receive from the Commission, law enforcement, and the industry traceback consortium regarding calls for which they act as an intermediate provider. Since May 6, 2021, however, under our call blocking rules, intermediate providers (again, including gateway providers) are also subject to a separate requirement to respond fully and in a timely manner to all traceback requests from those same entities. This rule was adopted in the *Fourth Call Blocking Order* and took effect on May 6, 2021. By complying with that new rule, intermediate providers also meet the traceback requirement in our caller ID authentication rules (§ 64.6302(b)) and, under that rule, are excused from complying with the requirement to apply STIR/SHAKEN to unauthenticated calls. In addition, intermediate providers are not subject to any requirement under the caller ID authentication rules to perform robocall mitigation. This means that even though gateway providers are where a call first enters the U.S. network, they are not subject to the same obligations that apply to domestic originating voice service providers.

- Foreign entities are prohibited from spoofing caller ID with the intent to defraud, cause harm, or wrongfully obtain anything of value when placing calls to recipients in the United States. While this prohibition is valuable, the very nature of spoofing makes it difficult to identify spoofing in the first instance, and track down the call originator after discovering spoofing has occurred.
- Foreign originating voice service providers that use NANP resources that pertain to the United States to send traffic to the United States may have their traffic blocked if they are not in our Robocall Mitigation Database, which requires certification of STIR/SHAKEN implementation or the use of a robocall mitigation program. But this requirement is limited by the fact that the prohibition applies only to traffic received "directly" from a foreign voice service provider not listed in the Robocall Mitigation Database; a foreign voice service provider is not currently required to file if it always routes traffic destined

for U.S. consumers over intermediate provider networks before they reach the U.S. gateway, and a bad actor could easily exploit this loophole.

- Our call blocking rules require voice service providers (including intermediate providers) to respond to traceback requests and take steps to effectively mitigate illegal traffic and require originating providers to take steps to prevent new and renewing customers from using the network to originate illegal calls. However, because a foreign voice service provider upstream from the gateway provider is outside of the scope of our rules, these requirements may not always allow the call originator to be identified or the traffic to be stopped before it reaches United States consumers.

25. We tentatively conclude that it would benefit Americans to subject foreign-originated robocalls, once they reach a gateway provider in the United States, to the same types of measures applied to calls originated in the United States: caller ID authentication and robocall mitigation. We further tentatively conclude the unique challenges associated with foreign-originated robocalls demand that gateway providers be subject to additional caller ID authentication and robocall mitigation requirements, to ensure Americans are protected from calls originating abroad. Unlike other providers, gateway providers have visibility into the foreign network where the call originates and have the ability to identify instances when a call that purports to originate from a U.S. number in fact originated internationally, which can reduce the accuracy and effectiveness of blocking analytics. And unlike terminating voice service providers, gateway providers can stop illegal calls to customers of many terminating voice service providers. We seek comment on these tentative conclusions. Are our current rules addressing foreign-originated robocalls sufficient? Rather than adopt new rules, should we leverage our existing rules in new ways to stop such calls? Or should we adopt new rules that rely on methods other than caller ID authentication and robocall mitigation? If so, what type of rules should we adopt?

26. *A Large Portion of Illegal Robocalls Originate Abroad.* Available evidence

indicates that a large portion of unlawful robocalls terminating within the United States originate outside the United States. USTelecom states that fraudulent calls are "almost always are coming from overseas," while ZipDX states that traceback data "have implicated foreign entities as a primary source of the worst kinds of robocalls." While some fraudulent traffic carries caller ID information matching the origination country (e.g., a call from France carries French caller ID), "the portion of this traffic to the overall fraudulent call volume is relatively small," and it appears that most foreign-originated fraudulent traffic carries a U.S. number in the caller ID field. We seek comment on this evidence, the relative proportion of domestic- and foreign-originated illegal robocalls, the prevalence of caller ID spoofing in foreign-originated robocalls, and trends in foreign-originated robocalling targeted at the United States over time. We also seek comment on the causes of any identified shift from domestic- to foreign-originated illegal robocall campaigns. Have the recent steps the Commission has taken in its call blocking and caller ID authentication orders and the June 30, 2021 STIR/SHAKEN implementation deadline pushed an increasing proportion of illegal robocall origination abroad? Are there other explanations for a shift to foreign-originated robocalls?

27. *Role of Gateway Providers*. While foreign-originated illegal robocalls are a major problem, these calls can only reach U.S. consumers and businesses after they pass through a gateway provider. The NANC has recognized that, to access the U.S. market, foreign originators must send traffic to a gateway provider that is unwilling or unable to block that traffic.

28. The Commission's Enforcement Bureau has repeatedly identified gateway providers as playing a key role in bringing illegal robocalls to the United States. In letters sent to multiple gateway providers in February 2020 to "assist the . . . Commission in stopping the flow of malicious robocalls originating from sources outside the United States," the Enforcement Bureau noted that a gateway provider, "[a]s the point of entry for this traffic into the U.S. telephone network, is uniquely situated to . . . combat apparently illegal robocalls." In spring 2020, in conjunction with a Division of the Federal Trade Commission, the Enforcement Bureau

warned international "gateway providers facilitating COVD-19 related scam robocalls originating abroad that they must cut off these calls or face serious consequences." In April 2020, the FTC and FCC wrote to three gateway providers and demanded that they stop facilitating scam COVID-19-related robocalls from India and Pakistan. In May 2020, the FTC and FCC sent an additional three letters to three separate gateway providers regarding similar campaigns originating in the UK, Germany, and other destinations abroad. Most recently, in spring 2021, the Enforcement Bureau sent cease-and-desist letters to ten providers, including some gateway providers, making clear that, should they not cease transmitting illegal robocall campaigns immediately, "other network operators [would] be authorized to block traffic from these companies."

29. The Department of Justice (DOJ) has also brought enforcement actions against gateway providers that allow illegal robocall traffic into the country. In two recent DOJ cases, DOJ states that "the defendants engaged in wire fraud schemes by knowingly serving as 'gateway carriers' for fraudulent calls; that is, the defendants received fraudulent robocalls from foreign customers and relayed those calls into the United States telecommunications system." The schemes, according to the DOJ, would not have worked unless the defendants, were "willing to accept the fraudsters' robocall traffic into the U.S. telephone system. . . . The [defendants] provide the crucial interface between foreign internet-based phone traffic and the U.S. telephone system." We seek comment on whether these cases are representative of the role that some gateway providers play in allowing illegal robocalls to reach U.S. subscribers.

30. We seek comment on the relationship between gateway providers and illegal robocalls entering the U.S. market. Is the problem driven by a few unscrupulous gateway providers that have entered into business arrangements to transit illegal foreign-originated robocall traffic? In a recent case, the DOJ noted that the defendant gateway providers "specifically market their services to foreign call centers and foreign VoIP providers looking to transmit high volumes of robocalls into the United States." Or is the problem more widespread,

for instance because gateway providers do not or cannot easily identify bad actors sending illegal robocalls to the United States through the gateway provider's network? If the problem is widespread, why do gateway providers today decline to identify and act to restrict bad actors and unlawful robocalls? Do foreign originators send illegal robocall traffic to the gateway indirectly, through one or more foreign intermediate providers, in order to conceal the nature of the call before it reaches the U.S. gateway? Are there other mechanisms by which foreign originators of illegal robocalls send their traffic to the United States such that it would be brought onto the U.S. network by an unsuspecting gateway provider?

31. We also seek comment on how foreign robocallers and the voice service providers that serve them use U.S. numbers in the caller ID field for their illegal robocall campaigns. Do these entities primarily spoof U.S. numbers? Or do these bad actors also use U.S. numbers that the voice service provider or their customer has obtained the right to use, either directly from the Numbering Administrator or indirectly through another provider? We note that the Commission recently proposed rules to help prevent VoIP providers from obtaining numbers directly from the Numbering Administrator for use in illegal robocall campaigns, and there are existing reporting rules regarding number usage. Are there other safeguards we should consider to prevent foreign providers from using U.S. NANP numbers in illegal robocall campaigns?

B. Scope of Requirements and Definitions

32. In light of their unique role in bringing foreign-originated illegal robocalls onto U.S. networks, we propose to impose new obligations on gateway providers for foreign-originated calls that use U.S. numbers in the caller ID field. We believe that this approach will narrowly target those providers best able to stop those calls that have the greatest likelihood to be part of illegal robocall campaigns that harm Americans—foreign-originated calls carrying U.S. numbers in the caller ID field.

33. While the Commission has imposed requirements on intermediate providers, including gateway providers, it has never defined "gateway provider" as a distinct category of

entities. We now propose 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. We do not include in this proposed definition a gateway provider that terminates calls in the U.S. To the extent a gateway provider terminates a call in the U.S., it is acting as a terminating voice service provider and is already subject to our existing caller ID authentication and/or robocall mitigation rules. In this proposed definition, by "U.S.-based," we mean that the provider has facilities in the U.S. including a U.S. located point of presence. We seek comment on this proposed definition. Should we define "gateway provider" differently? Should we define "U.S.-based" differently? Should our definition include the first U.S.-based provider in the call path for a foreign-originated call that also terminates that call? Should we extend some or all of the requirements we propose today to such terminating voice service providers, or are existing requirements sufficient? Should we exclude from the definition those providers that serve as a gateway for only a *de minimis* amount of foreign originated traffic? Are such providers unlikely to be the source of illegal robocalls? If so, how should we define de minimis for this purpose? Is there another way to effectively limit our definition to apply only to those gateway providers that are especially likely to be the source of illegal calls on the U.S. network? Does our definition need to be modified to take into account the scenario where a call originates in the U.S., is routed internationally (over the same provider or a different provider's facilities), and then is routed back to a U.S. end-user through a gateway provider? What about a scenario where a call enters the U.S. through a gateway provider, is routed outside of the U.S. and then back into the U.S. through the same or different gateway provider?

34. We seek comment on whether U.S.-based providers that fall under our proposed definition of gateway provider also, in some instances, originate calls from abroad carrying U.S. NANP numbers that are brought into the U.S. by that same provider. In other words, are there instances where the provider that brings the call into the U.S. is also acting as an originating

provider? For such calls, the U.S.-based provider would not fall under our proposed gateway provider definition where it is not acting as an intermediate provider. For example, a U.S.-based provider acts as a gateway provider for calls foreign providers send to it. The same U.S-based provider may also serve an end-user customer in another country that is originating traffic in that country and sending traffic over that U.S.-based provider's network into the U.S. marketplace. In such an instance, the U.S.-based provider is not acting as an intermediate provider and thus would not fall within our proposed definition of gateway provider. However, if a U.S.-based provider has contracted with a foreign provider or customer to allow calls into the U.S. marketplace and the call is brought to the U.S.-based providers' U.S. network by a foreign provider, the U.S.-based provider would be an "intermediate provider" and therefore fall within our proposed definition. Are certain arrangements that are not covered by our proposed definition likely to be part of an illegal robocall campaign? If so, should we broaden or otherwise modify our proposed definition to ensure that such calls fall within the scope of the protections we propose in this FNPRM? Alternatively, should we explicitly include these situations for the purposes of specific rules, such as our proposed mandatory blocking rules?

35. As we have elsewhere in our caller ID authentication rules, we propose to classify providers as gateway providers on a call-by-call basis rather than on a class basis. Thus, a provider would be a "gateway provider"—and subject to rules applied to that class of provider—only for those calls for which it acts as a gateway provider; it would be an "intermediate provider" or "voice service provider"—and subject to rules applied to those classes of provider—for all other calls, e.g., for domestic-originated calls that it carries. We believe it is appropriate to apply that approach here not only for regulatory symmetry, but also because it would capture all instances in which an entity acts as a gateway provider. At the same time, this approach would not subject all traffic handled by an entity to enhanced obligations simply because a portion of that traffic originates abroad. We seek comment on this proposal. Should we instead diverge from our "call-by-call" approach for gateway providers? Do providers have

the ability to treat foreign-originated calls differently on a call-by-call basis? If we were to establish that a provider is a gateway provider for all of its traffic, if any traffic it transits originates abroad, would such an approach place unreasonable obligations on a provider's domestic traffic simply because some traffic is foreign-originated?

36. We further propose to limit the scope of our proposed requirements for gateway providers to those calls that are carrying a U.S. number in the caller ID field. By a "U.S. number," we are referring to NANP resources that pertain to the United States. Under this approach, we would exclude from the scope of our rule those calls that carry a U.S. number in the ANI field but display a foreign number in the caller ID field. We believe that this approach is consistent with our goal to prevent illegal spoofing, which is dependent upon manipulating the caller ID field that is visible to the call recipient. We further propose to apply this requirement on a "call-by-call" basis. Under this approach, a gateway provider would be subject to these requirements for those calls it transits that carry a U.S. number in the caller ID field, but that same gateway provider would not be subject to these requirements for calls displaying numbers associated with another country. We seek comment on these proposals. We also seek comment on the feasibility and desirability of widening the scope of our proposed rules to cover calls carrying non-U.S. numbers in the caller ID field or a subset of non-U.S. numbers. If we include a subset of non-U.S. numbers, what numbers should we include?

37. Limiting our proposed rules to calls that use U.S. numbers in the caller ID field is similar to the approach in our current rule that requires intermediate providers and voice service providers to not accept calls directly from a foreign voice service provider that is carrying U.S. numbers if the foreign voice service provider is not listed in the Robocall Mitigation Database. In that context, we limited application of our rule to foreign voice service providers that "use[] North American Numbering Plan resources that pertain to the United States." We seek comment on whether it is appropriate, in this context, to take a narrower or more expansive approach than

we did in the context of foreign voice service providers whose traffic must be blocked if they are not listed in the Robocall Mitigation Database.

C. Authentication

38. To combat foreign-originated robocalls, we propose to require 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.

39. As the Commission has previously explained, application of caller ID authentication by intermediate—including gateway—providers "will provide significant benefits in facilitating analytics, blocking, and traceback by offering all parties in the call ecosystem more information." At the time the Commission reached this conclusion, in light of record concerns that an authentication requirement on all intermediate providers "was unduly burdensome in some cases," the Commission established that intermediate providers could "register and participate with the industry traceback consortium as an alternative means of complying with our rules," in lieu of authenticating unauthenticated calls.

40. 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 voice service providers—which include gateway providers and other intermediate providers under our call blocking rules—to cooperate with traceback requests. 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. We propose concluding that, given the key role gateway providers play in allowing foreign calls into the United States, gateway providers should be required to authenticate unauthenticated foreign-originated SIP calls that they receive and cooperate with traceback requests with respect to those same calls. Requiring gateway providers to authenticate caller ID information for all unauthenticated foreign-originated SIP calls will offer information to the

downstream providers regarding where a foreign-originated robocall entered the call path, facilitating analytics and promoting traceback efforts. We seek comment on this proposal.

41. Illegal robocalls cost Americans over $13.5 billion annually. Given the prevalence of robocalls from abroad, we anticipate that the deterrence that arises from authenticating unauthenticated foreign-originated calls is likely to be highly beneficial and that those benefits outweigh any concerns about C-level attestations not carrying sufficient information to assist in the policing of illegal robocalling campaigns. Even with a "C-level" (gateway) attestation, we anticipate that authenticating unauthenticated calls will facilitate faster traceback and improve call analytics. We seek comment on this analysis and on the possible benefits of the requirement we propose.

42. We also seek comment on the proposal's costs for gateway providers. While the Commission previously acknowledged claims that it was "unduly burdensome in some cases" to require all intermediate providers to authenticate unauthenticated calls, we anticipate that our proposal will not be unusually costly for gateway providers compared to voice service providers already required to implement caller ID authentication. Further, 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 gateway providers compared to other providers or that the benefit of lower-level attestations would be limited?

43. *Requirements.* We propose that, to comply with the requirement to authenticate calls, 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. This proposal follows the caller ID authentication rule governing intermediate provider authentication of unauthenticated calls they receive, where intermediate providers elect authentication instead of cooperation with tracebacks. As noted, the call blocking rules have mooted this choice. We seek comment on whether and how to alter this proposal.

Are there any scenarios in which transmitting a call with authenticated caller ID information is not possible, and if so, how should we address any such circumstances? Should we adopt a technical feasibility exception, as we have established for voice service providers with respect to the obligation to transmit an authenticated call with authenticated caller identification information to the next voice service provider or intermediate provider in the call path? Would establishing exceptions present the possibility for abuse?

44. We propose that, as with our requirement on voice service provider authentication, a gateway provider satisfies this 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. We also propose that compliance with the most current versions of these standards as of the date of release of any Report and Order following this FNPRM, including any errata as of that date or earlier, represents the minimum requirement to satisfy our rules. We seek comment on this approach. Are there any reasons these standards are not appropriate for gateway providers? Are there any technical challenges that may emerge (e.g., will the addition of the authenticated Identity Header in the SIP message cause UDP fragmentation)? And if so, how can they be mitigated? Alternatively, are there other standards we should require gateway providers to adhere to? Should we require compliance with standards current as of an earlier date? If so, which date?

45. Because we propose permitting gateway providers to authenticate caller ID information in a manner consistent with industry standards, we do not propose limiting the attestation level they may assign to a given call. To the extent standards allow a gateway provider to assign "full" (A-level) or "partial" (B-level) attestation to a call, under this proposal they are free to do so; they would not be limited to assigning "gateway" (C-level) attestation. Stakeholders previously supported this approach regarding intermediate providers, and we seek comment on whether this continues to be the best approach to attestations by gateway providers, a subset of intermediate providers. Is there a reason we should limit gateway providers to

assigning a certain attestation level or levels, and if so what level? Under what circumstances would gateway providers be able to assign, and anticipate assigning, an A- or B-level attestation?

46. *Non-IP Network Technology*. As we have explained, the STIR/SHAKEN framework is an IP-based solution. How should we address gateway providers that use non-IP network technology? How prevalent is non-IP network technology among gateway providers? Are gateway providers using non-IP network technology less likely or more likely to be the point of entry for foreign-originated illegal robocalls onto the U.S. network? Our rules require voice service providers with non-IP network technology to either upgrade their network 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. Should we adopt a similar requirement here? We do not currently apply a similar requirement to intermediate providers, including gateway providers. In our preliminary view, however, adopting such a requirement for gateway providers may be warranted to prevent evasion of any restrictions we establish by bad actors. We seek comment on this view. The Commission previously stated that it would "continue to evaluate whether an effective non-IP caller ID authentication framework emerges" and, "if and when [it] identif[ies] an effective framework, [it] expect[s] to . . . shift . . . from focusing on development to focusing on implementation." We seek comment on adopting this same approach with respect to gateway providers here. Should we instead mandate that gateway providers with non-IP network technology implement a non-IP caller ID authentication solution, such as Out-of-Band STIR? Should gateway providers relying on non-IP technology continue to be fully exempt from any obligation to implement caller ID authentication, like other intermediate providers?

47. *Token Access.* Does the Governance Authority's token access policy serve as a barrier to participation in STIR/SHAKEN for all or a subset of gateway providers? That policy requires entities to have a current FCC Form 499-A on file with the Commission, have been assigned an Operating Company Number (OCN), and have either direct access to numbering resources or filed a certification in the Robocall Mitigation Database in order to obtain a token

necessary to participate in STIR/SHAKEN. We assume that gateway providers that are already acting as voice service providers and are subject to the duty to authenticate calls they originate or terminate may have already obtained a token in order to comply with their duties as a voice service provider. Is that assumption correct? How many gateway providers also serve as voice service providers? While providers so situated may already possess the necessary token, will other gateway providers have difficulty obtaining tokens under the current policy? Do some or all gateway providers have no obligation to file an FCC Form 499-A because they do not fall under one of the categories of entities required to submit the form? If so, should we encourage the Governance Authority to waive for such providers the requirement to file an FCC Form 499-A to obtain a token? Are some or all gateway providers unable to obtain an OCN based on the National Exchange Carrier Association's (NECA) policies? If certain gateway providers are not required to file a Form 499-A or cannot readily obtain an OCN, should we encourage or require the Governance Authority to modify its token access policy to ensure that gateway providers are able to obtain a token and comply with an authentication requirement? And do we need to make changes to our Robocall Mitigation Database to allow compliance with the Governance Authority's filing requirement?

48. *Compliance Deadline*. We seek comment on when we should require gateway providers' authentication obligation to become effective, mindful of the public interest of prompt implementation by gateway providers with the need for these providers to have sufficient time to implement our proposed obligation. We note that the STIR/SHAKEN caller ID authentication obligations in the TRACED Act became effective 18 months following its enactment, and voice service providers were able to meet that deadline. Our rules adopted pursuant to the TRACED Act grant certain providers exemptions and extensions from this deadline. Accordingly, would a March 1, 2023 deadline, falling approximately 18 months after we adopt this FNPRM, be a reasonable deadline for implementation of our authentication obligation? Would an earlier or later deadline for all gateway providers better balance the benefit of the rule against the burden?

49. Should we modify our proposed deadline for certain classes of gateway providers? For example, should we identify a subset of gateway providers that are most likely to be the conduit for illegal robocalls and subject them to an accelerated timeline? How should we identify such providers? Should we identify those gateway providers that have received at least a certain number of traceback requests or other indicia of involvement in illegal robocalling? If so, what would be an appropriate threshold? What deadline should we give such providers? Instead, should we expect faster implementation of STIR/SHAKEN by those gateway providers that are also voice service providers under our STIR/SHAKEN rules, are not subject to an extension or exemption, and therefore are already authenticating caller ID information for calls they originate? Will a provider so situated be in a better position to implement STIR/SHAKEN quickly? If so, why?

50. In the *Second Caller ID Authentication Report and Order*, the Commission granted several categories of voice service providers that faced undue hardship in implementing STIR/SHAKEN additional time for compliance, consistent with the directive of the TRACED Act: small voice service providers, providers unable to receive a token from the Governance Authority, and services subject to discontinuance. Should we grant any categories of gateway providers extensions or exceptions from our proposed authentication requirement on the basis of undue hardship or for another reason? Are the extensions the Commission previously granted for STIR/SHAKEN based on undue hardship relevant to the context of gateway providers? For instance, should we grant small gateway providers an extension from any deadline we establish, and, if so, which gateway providers should we define as "small?" Or would doing so undermine the value of any requirements we adopt? If we grant an extension to some gateway providers, how much additional time would be appropriate in light of the public interest of prompt participation in the STIR/SHAKEN framework? If we grant an exemption, how would any exemption square with the importance of ubiquitous STIR/SHAKEN? Instead of a categorical approach, should we rely on individualized waiver requests pursuant to the Commission's

longstanding waiver standard? The Commission may exercise its discretion to waive a rule where the particular facts at issue make strict compliance inconsistent with the public interest. In considering whether to grant a waiver, the Commission may take into account considerations of hardship, equity, or more effective implementation of overall policy on an individual basis.

D. Robocall Mitigation

51. While our caller ID authentication rules require voice service providers to implement STIR/SHAKEN or, if they are subject to an extension, to implement an appropriate robocall mitigation program, in this Notice we propose requiring gateway providers to apply both of these protections to calls they bring onto the U.S. network. We further propose and seek comment on additional requirements on gateway providers, at least some of which go beyond those that currently apply to voice service providers. First, we propose to require gateway providers to respond to all traceback requests from the Commission, law enforcement, and the industry traceback consortium within 24 hours. Second, we propose and seek comment on imposing mandatory blocking requirements on gateway providers. Third, we seek comment on establishing know-your-customer requirements for gateway providers. Fourth, we seek comment on requiring gateway providers to adopt certain contractual provisions with foreign providers from which they accept calls. Finally, in addition to adopting one or more of these robocall mitigation requirements, we propose to establish a general duty on gateway providers to mitigate illegal robocalls.

1. 24-Hour Traceback Requirement

52. We propose to require gateway providers to respond fully to all traceback requests from the Commission, civil or criminal law enforcement, and the industry traceback consortium within 24 hours of receiving such request. This requirement would be stricter than our general obligation, which requires that voice service providers (including intermediate providers) respond to traceback requests "in a timely manner." As we have stated in the past, traceback is an essential part of identifying the source of illegal calls. Information gained from traceback can

both aid in enforcement after calls are placed and be used proactively to stop further calls from a particular source. We believe that time is of the essence in all tracebacks, but particularly for foreign-originated calls where the Commission or law enforcement may need to work with international regulators to obtain information from providers outside of U.S. jurisdiction.

53. We seek comment on this proposal. Is a mandatory 24-hour response time appropriate, or should we consider a different response time? Because gateway providers are already required to respond to traceback "timely," we believe that this enhanced requirement presents a minimal burden on gateway providers. We seek comment on this tentative conclusion. Are there any instances where a gateway provider may need more time to respond? If so, what would cause such a delay (e.g., what are the technical and/or operational challenges that would contribute to the delay)? How might we address any such problems to best enable gateway providers to meet such a requirement? Should we instead consider requiring response in a shorter time than 24 hours? Are there additional benefits or burdens to requiring a faster response time? Are there any other issues we should consider in adopting such a requirement, such as the impact on small gateway providers?

54. We seek comment on other means to improve traceback when calls originate internationally. Are there other, or additional, steps the Commission could take to improve this process and make bad actors easier to identify and stop? Should the Commission consider taking these steps in addition to, or instead of, requiring gateway providers to respond within 24 hours? What benefit would these approaches provide? Are there any particular burdens or concerns the Commission should consider when weighing these options?

55. *Compliance Deadline*. We propose to require gateway providers to comply with this requirement by 30 days after publication of the notice of an Order adopting this requirement in the Federal Register. Because gateway providers are already required to respond to traceback requests "fully and timely," we do not believe there is any reason to further delay implementation of this requirement. We seek comment on this proposal and analysis. Would a

different compliance deadline be more appropriate and, if so, why?

2. Mandatory Blocking

56. To date, the Commission has generally taken a permissive approach to call blocking, allowing voice service providers the flexibility to block in certain instances, but not requiring blocking. In adopting the effective mitigation requirement, the Commission did make clear that gateway providers may be required to block in order to comply. The Commission's rules also direct intermediate and voice service providers to only accept calls using NANP numbers sent directly from voice service providers with a filing in the Robocall Mitigation Database. This requirement is distinct from our blocking requirements. Unfortunately, illegal calls continue to plague American consumers. When calls originate outside the United States, enforcement against, or even identification of, the caller is much more difficult. Gateway providers are positioned to reduce the flood of foreign-originated illegal calls before they reach American consumers. If a gateway provider stops a single calling campaign before it enters the U.S. network, no American consumers will receive those calls. Because gateway providers may, in many cases, not have direct relationships with American consumers, they may lack incentive to take aggressive action absent a mandate. To address these issues, we seek comment on several possible approaches to requiring gateway providers to block calls, particularly where those calls bear a U.S. number in the caller ID field.

57. *Gateway Provider Blocking Based on Commission Notification of Illegal Calls.* In the *Fourth Call Blocking Order*, the Commission adopted rules requiring voice service providers, including gateway providers, to "take steps to effectively mitigate" illegal traffic when notified of such traffic by the Commission. The Commission noted that gateway providers may need to block calls in order to comply with this requirement as, unlike originating voice service providers, they often do not have a direct relationship with the call originator. We believe that modifying this rule to affirmatively require gateway providers to block calls upon receipt of notification from the Commission through its Enforcement Bureau would better protect

American consumers from illegal calls and thus seek comment on whether to do so. We therefore propose to strengthen our existing effective mitigation requirement as to gateway providers. Specifically, we propose to require gateway providers, following a prompt investigation to determine whether the traffic identified in the Enforcement Bureau's notice is illegal, to promptly block all traffic associated with the traffic pattern identified in that notice. We seek comment on this proposal.

58. We seek comment on whether allowing gateway providers to investigate prior to blocking strikes the correct balance. Currently, our rules do not specify how quickly a voice service provider must act, but do require that it investigate and report to the Commission "promptly." The report must include any steps taken to effectively mitigate the identified traffic or an explanation as to why the provider has concluded that the identified calls were not illegal. Is this the correct approach given the heightened risk of foreign-originated illegal robocalls, or should we adopt a stricter standard for gateway providers? For example, should gateway providers block calls prior to investigation? If so, should we require that gateway providers implement blocking immediately upon receipt of notification? If not, what is an appropriate delay prior to implementing a block? If we require blocking prior to investigation, how can we ensure that gateway providers are granted due process? What are the risks associated with a too-long or too-short time, and how might we mitigate those risks? Are there any other issues we should consider in determining how quickly a gateway provider must block calls and whether to allow investigation prior to blocking?

59. We seek comment on the contours of the blocking obligation. Should we require the notified gateway provider to block all calls that meet criteria identified by the Enforcement Bureau in its notice that make it highly likely that the calls are part of the same call pattern as those calls that the Commission has determined to be illegal? The *Fourth Call Blocking Order* established specific details that the Enforcement Bureau must include in its notice. Or should we allow gateway providers some discretion to determine the scope of the block based on the

Enforcement Bureau's notice? If we allow discretion, should we instead establish general guidelines in our rules, to ensure that a gateway provider can know that it is in full compliance with our rules? If so, what might these guidelines look like? If we adopt our proposal of permitting a gateway provider to investigate prior to blocking, should we require the gateway provider to indicate what criteria it is using, based on the Enforcement Bureau's notice and its own investigation, in its response to the Commission? Alternatively, should we require that gateway providers, regardless of the specifics of the call pattern, block all calls that purport to originate from the same number(s) as the identified illegal traffic? Is there some other approach that we should consider? What are the risks of each approach? Specifically, what is the risk that lawful calls will be blocked, or that illegal calls will continue from the same source despite the gateway provider's compliance? How can we reduce unnecessary burdens on gateway providers under each approach? Are there any other issues we should consider in determining how a gateway provider may comply with this requirement, such as the impact on small businesses?

60. *Requiring Downstream Providers to Block Calls from Bad-Actor Gateway Providers*. A complementary approach to requiring gateway providers to block calls is to require the voice service provider or intermediate provider downstream from the gateway provider to block where the Commission determines a particular gateway provider is a bad actor. In the *Third Call Blocking Order and Further Notice of Proposed Rulemaking*, we used the phrase "bad actor" when discussing originating or terminating providers that fail to take appropriate steps to prevent their networks from being used to originate or transmit illegal calls. Here, we expand our use of that term to include gateway providers that fail to comply with the rules we propose above. This approach provides a strong incentive for the gateway provider to avoid having its traffic blocked by ensuring that it complies with our rules. In the *Third Call Blocking Order and Further Notice of Proposed Rulemaking*, the Commission encouraged, without requiring, such blocking by establishing a safe harbor for terminating voice service providers and intermediate providers that choose to block calls from bad-actor upstream providers once certain

criteria are met. In conjunction with our mandatory blocking proposal above, we propose that, should a gateway provider fail to comply with those requirements, the Commission, through its Enforcement Bureau, may send a notice to all providers immediately downstream from the gateway provider in the call path. Upon receipt of such notice, all providers must promptly block all traffic from the identified gateway provider, with the exception of 911 and PSAP calls. We seek comment on this approach.

61. Currently, our rules allow a downstream provider to block and cease accepting all traffic from a bad-actor upstream provider which, upon receipt of Commission notice of illegal traffic, fails to either effectively mitigate that traffic or fails to take steps to prevent new and renewing customers from originating illegal calls. If a gateway provider fails to effectively mitigate illegal traffic, calls continue to reach American consumers, and enforcement only comes after the fact. For these reasons, we believe there is value in requiring the voice service provider or intermediate provider immediately downstream from a gateway provider to block all calls from that gateway provider in the event that the gateway provider fails to effectively mitigate, or block if required, illegal traffic once notified of such traffic by the Commission via the Enforcement Bureau. We seek comment on this view.

62. We seek comment on how much time gateway providers should have to begin effectively mitigating, or blocking, calls before directing downstream providers to block all calls from that gateway provider. Should we require that gateway providers take such steps "promptly," consistent with our existing rules? If we instead adopt a stricter requirement for gateway provider action, should we immediately notify downstream providers to block, or allow additional time before taking that step? If we determine more time is appropriate, how long should we delay our notification to downstream providers? If we use the "promptly" standard, how should we determine what is "prompt" for these purposes? Should we notify gateway providers before directing downstream providers to block and thereby give the gateway provider an additional chance to mitigate the traffic? What are the costs and benefits of each approach?

63. We seek comment on how much time to permit downstream providers to begin blocking calls from the identified gateway provider. Should we require that the downstream provider begin blocking immediately? Are there any technical or practical barriers to immediate blocking? If so, how can we address them? If we do not require immediate blocking, how much time should we allow? What are the costs and benefits of each approach? Are there any other issues we should consider around timing?

64. We seek comment on how best to notify downstream providers when blocking is required. Where there are multiple providers immediately downstream from the gateway provider, should we directly notify them all? If so, how can we ensure that every relevant provider is notified? Alternatively, should we notify a single entity, such as the industry traceback consortium, and require that downstream providers work with that entity to obtain this information? If so, does this alter the timeline for compliance? Is there some other approach that would be more appropriate, such as a public notice or use of the Robocall Mitigation Database? We also seek comment on how we can determine whether a downstream provider is complying with this blocking requirement. Should we require the downstream provider to block all calls from the identified gateway provider, or just those that are part of the identified call pattern?

65. Finally, we recognize that blocking of all traffic from a particular gateway provider is likely to have a profound impact on that gateway provider's ability to do business. We therefore seek comment on whether to adopt additional due process steps or requirements to ensure that these rules are not erroneously applied to gateway providers. Is allowing investigation prior to requiring blocking sufficient, or should we adopt additional protections? If we do not allow investigation prior to blocking, should we adopt additional due process protections prior to directing downstream providers to block? Additionally, should we adopt rules to direct downstream providers to cease blocking if the gateway provider later takes appropriate steps to effectively mitigate or block the identified traffic? If so, what should be

included in these rules? When would it be appropriate to direct downstream providers to cease blocking? How much time should we allow for this to occur? Should we use the same means of notification? We seek comment on any other issues we should consider in adopting such a requirement, including the impact on small businesses.

66. *Blocking Based on Reasonable Analytics.* Our rules currently permit broad blocking based on reasonable analytics by terminating voice service providers only and, in most cases, require those providers to allow customers to opt out. One-ring scam blocking also uses "reasonable analytics" and may be used by any voice service provider or intermediate provider in the call path without requiring any opt-out provisions. However, the use of analytics for one-ring scam calls is more narrowly tailored, designed to identify only one particular type of illegal call. In contrast, the Commission's other authorizations of blocking based on reasonable analytics have permitted terminating voice service providers broad discretion to block unwanted calls or calls that are highly likely to be illegal and are not limited to analytics designed to identify a specific, identified, type of call. The *Fourth Call Blocking Order* expanded the safe harbor for blocking based on reasonable analytics to include network-based blocking without any opt-out requirement where the provider's analytics are designed to identify calls that are "highly likely to be illegal" so long as they meet other requirements. In all cases of broad authorizations of blocking based on reasonable analytics, the voice service provider must disclose to customers that it is engaging in this blocking. Because these broad authorizations allow only terminating voice service providers to block calls, only customers of those voice service providers that block calls are protected. In our effort to increase protection for American consumers, we propose to require gateway providers to block calls that are highly likely to be illegal based on reasonable analytics, preventing these calls from entering the U.S. network. We further propose additional requirements around this blocking consistent with our existing authorization of blocking based on reasonable analytics designed to identify calls that are highly likely to be illegal for terminating voice service providers. Specifically, we propose to require gateway providers to: 1)

incorporate caller ID authentication information where available; 2) manage the blocking with human oversight and network monitoring sufficient to ensure that it blocks only calls that are highly likely to be illegal, which must include a process that reasonably determines that the particular call pattern is highly likely to be illegal before initiating blocking of calls that are part of that pattern; 3) cease blocking calls that are part of the call pattern as soon as the gateway provider has actual knowledge that the blocked calls are likely lawful; and, 4) apply all analytics in a non-discriminatory, competitively neutral manner. We seek comment on these proposals.

67. We believe requiring gateway providers to use reasonable analytics to block will increase blocking of illegal calls entering the U.S. network, and will build on the success of current reasonable analytics blocking. We thus believe using the "highly likely to be illegal" standard for gateway provider blocking makes sense. We seek comment on this view. We also recognize that a standard with flexibility, such as this one, can result in over- or under-inclusive blocking and that, unlike terminating voice service provider blocking, consumers will have no recourse for erroneous gateway provider blocking.

68. How should we address this potential problem? We propose to require gateway providers to manage the blocking with human oversight and network monitoring sufficient to ensure that only calls that are highly likely to be illegal are blocked. This is consistent with our requirement for terminating voice service providers that block calls that are highly likely to be illegal without consumer opt out. Is this the correct approach? If not, should we require a different process? If so, what would this process look like? Are there steps we could take to otherwise reduce the risk that lawful calls will be blocked? Should we adopt additional requirements to ensure that a gateway provider can be certain that its blocking is within the scope of our rules, rather than under- or over-inclusive? Would a gateway provider that makes use of comparatively conservative blocking analytics be subject to liability for under-blocking? If so, how might we address this issue? Are there any other issues we should consider in taking this approach?

69. Consistent with our existing safe harbor for the blocking of calls based on reasonable analytics, we propose to require gateway providers to incorporate caller ID authentication information, where that information is available, and to ensure that all analytics are applied in a non-discriminatory, competitively neutral, manner. Is this the appropriate approach? Should we modify or remove either of these requirements in this context? If so, how might we change them? We also propose to require that gateway providers cease blocking calls that are part of the call pattern as soon as the gateway provider has actual knowledge that the blocked calls are likely lawful. We believe that this is the best approach to reduce the risk of lawful calls being blocked. We seek comment on this belief. Should we modify our approach in this context? For example, should we require gateway providers to obtain further confirmation that calls are lawful? Or, in contrast to that option, should we require a gateway provider to cease blocking whenever it receives information that particular calls may be lawful? If we take this approach, should we require gateway providers to investigate this information to determine whether it is accurate and, if it is inaccurate, resume blocking?

70. Should we provide further guidance as to what constitutes "reasonable analytics" in this context? Other than in the *First Call Blocking Order*, we have declined to establish specific standards, both out of a concern that such standards will create a road map for bad actors seeking to avoid blocking and to allow flexibility in response to evolving threats. Under the *First Call Blocking Order*, voice service providers, as well as intermediate providers, are permitted to block based on the number in the caller ID field. Specifically, blocking is permitted where the number is unused, unallocated, or invalid, or where the subscriber to the number has indicated that it does not use the number to originate calls and requests that all calls purporting to originate from that number be blocked. However, we want to ensure that a gateway provider has notice as to whether or not it is in compliance with our rules. Are there standards we could adopt here that would provide certainty to gateway providers without allowing bad actors to easily circumvent blocking? Would this approach reduce the burden on small businesses by providing

certainty? We further seek comment on whether we should consider bases for blocking other than reasonable analytics and how they would better serve consumers. Are there any other issues we should consider if we set specific standards?

71. *Gateway Provider Do Not Originate*. The Commission has authorized voice service providers (including intermediate providers) to block calls where: (1) the subscriber to the number indicated that that number should never be used to originate calls; (2) the number was unallocated; (3) the number was unused; or, (4) the number was invalid. Voice service providers and intermediate providers need not obtain consumer consent for blocking these calls, as there is no valid reason for these numbers to originate calls. There are at least two do-not-originate list implementations in use by industry that take different approaches to the issue. We seek comment on requiring gateway providers to block calls purporting to originate from numbers on a do-not-originate list.

72. Should we require gateway providers to block calls from numbers on a do-not-originate list? If so, what numbers should be included on the list? The Industry Traceback Group, for example, maintains a "measured and tightly controlled process" for adding numbers to the do-not-originate list it operates based on the rules adopted in the *First Call Blocking Order*. Its policies allow for a do-not-originate request from federal and state government entities where the number is legitimately used for inbound calls only, is currently spoofed to perpetrate impersonation-focused fraud, is authorized for participating in the list by the party to which the telephone number is assigned, and is recognized by consumers as belonging to a legitimate entity. Private entities that wish to have numbers added to the list must meet additional requirements. The additional policies for private entities include a thorough vetting process and a requirement that there be "active and significant fraudulent activity" involving spoofing. There also may be an administrative charge assessed. Should we take a similar approach for adding numbers to a do-not-originate list? Alternatively, should we take a broader approach and allow any number that should never be originating calls outside the United States

to be added by the person or entity to which the number is assigned? Should we include other categories of numbers, such as unused or unallocated numbers? Are there any specific standards or vetting processes we should adopt to ensure that numbers are not added in error? What benefits and risks would each specific approach create? Are there any other factors we should consider in determining what numbers may be added to the list?

73. We seek comment on how we might implement such a list. Who should maintain the list? For example, should it be the maintained by the Commission, the industry traceback consortium, or some other entity? What are the advantages and disadvantages of each approach? Should the list be public or private? If public, how can we ensure that bad actors cannot abuse the list? If private, how can we ensure the security of the list? How might we collect these numbers, and how can we ensure that the costs of collecting, vetting, and maintaining the list are recouped? Should the list be combined with an existing do-not-originate list, such as the Industry Traceback Group's list, or should it be completely separate? Should we adopt a formal process for removing numbers from the list? Are there any approaches that would reduce these costs without eliminating the benefits? Are there any other particular issues we should consider in determining how to implement the list, including the impact on small businesses?

74. *Alternative Blocking Programs*. We seek comment on other potential mandatory blocking programs for gateway providers. Are there any other approaches to mandatory blocking we should consider? If so, what are the specifics of each approach, and what issues should we consider when adopting rules? What benefits would the blocking provide? What risks would the blocking pose, including the risk of blocking lawful calls? What burdens would the blocking pose for gateway providers? Should we consider the approach instead of, or in conjunction with, another type of blocking?

75. *Protections for Lawful Calls*. We believe that all blocking contains some risk of erroneous blocking, e.g., blocking calls that are not illegal. For example, a particular caller's call patterns could look similar enough to the patterns of an illegal caller and a gateway provider,

acting in good faith, could believe that the caller is placing illegal calls and thus block them. We seek comment on appropriate transparency and redress options that could accompany mandatory blocking requirements for gateway providers. What transparency and redress requirements should we adopt? Are the requirements we have already adopted sufficient, or are there reasons to adopt additional, or alternative, requirements? Should our transparency and redress requirements vary depending on what blocking approach we adopt? If so, how? Are there steps we should take to reduce issues related to language barriers? Are there any other issues we should consider?

76. We want to be particularly careful of the risk of blocking emergency calls, such as calls to 911, or calls from PSAPs and government emergency outbound numbers. We seek additional comment on protections for public safety calls more broadly elsewhere in this item. We seek comment on how to address these concerns. What is the risk of such calls being blocked under each of our proposals? Should we require that gateway providers never block such calls, or is a different approach more appropriate?

77. *Limitation of Liability for Compliance with Mandatory Blocking*. Aside from the Commission's prior statement that gateway providers may need to block calls in order to comply with the requirement to effectively mitigate illegal traffic, our existing rules generally do not require blocking. Instead, they focus on permitting blocking and ensuring that voice service providers will not be subject to liability under the Act and the Commission's rules when blocking in certain instances. We seek comment on whether, if we adopt mandatory blocking requirements, we should take a similar approach here. Our previous safe harbors were designed to incent blocking by ensuring that providers do not face liability for good faith blocking. Here, blocking would be mandatory. Given this, is there a need for such a safe harbor? Could gateway providers be subject to liability under the Act or the Commission's rules for steps taken to comply with any of the blocking options we discuss in this FNPRM? If so, what is the source of this liability? Should we provide a blanket safe harbor under the Act and the Commission's

rules, or should we limit that protection to actions taken to comply in good faith? If we have a good faith requirement, should we define good faith, and, if so, how? Should gateway providers be required to make a particular showing to demonstrate good faith sufficient to absolve them of liability for inadvertently blocking legal calls? For example, should we require an officer of a gateway provider to certify to the Commission, in the company's Robocall Mitigation Database certification or elsewhere, that they have acted in good faith and complied with our redress requirements? Are there any other issues we should consider?

78. We seek comment on how to determine whether a gateway provider has met its obligation to block under each of these options. As the Commission has previously concluded, "we do not expect perfection in mitigation." To address this concern, should we establish a good faith standard under which a gateway provider making its best, good faith efforts to block is not liable in cases where illegal traffic is not blocked? What would this obligation look like? How might we determine that a gateway provider is acting in good faith rather than willful ignorance? Should we make clear that a gateway provider will not be liable for failing to block where the information is not readily available, or should we adopt a different standard? We seek comment on what information is "readily available" to gateway providers at the time of the call. Is certain information available to gateway providers, but too expensive or inconsistently available to be considered "readily available" for all or some providers? What information might not be readily available at the time of the call but is readily available after the fact, allowing or requiring gateway providers to mitigate or block the traffic from the same source at a later time? Are there specific criteria we should use to provide regulatory certainty? Are there other issues we should consider?

79. *Compliance Deadline*. We propose to require gateway providers to comply with any mandatory blocking requirement by 30 days after publication of the notice of any Order adopting blocking requirements in the Federal Register or the publication of notice of Office of Management and Budget (OMB) approval under the Paperwork Reduction Act (PRA), where

appropriate. We seek comment on this proposal. Should we allow additional implementation time for any or all of the proposed blocking requirements? If so, how much of a delay is appropriate and, if so, why?

3. "Know Your Customer" Requirements for Gateway Providers

80. Our rules currently require a voice service provider 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." This rule generally applies to originating providers and, under our proposed definition, gateway providers do not have a direct relationship with the call originator and instead receive calls from a number of upstream originating or intermediate providers. As a result, gateway providers may not have a "customer" to "know" for the purpose of complying with a "know your customer" requirement. We believe, however, that extending "know your customer" obligations to gateway providers could benefit U.S. consumers. First, we propose and seek comment on requiring gateway providers to confirm that a foreign call originator is authorized to use a particular U.S. number that purports to originate the call. We then seek comment on whether, and how, to apply additional "know your customer" requirements to gateway providers to reduce the risk of illegal calls entering the U.S. network, including who the gateway provider's "customer" should be for this purpose.

81. *Use of U.S. NANP Numbers for Foreign-Originated Calls.* While there are valid reasons for some U.S. numbers to originate calls internationally, spoofing allows a bad-actor foreign caller to appear to a consumer as a U.S.-based entity, making it more likely a U.S. consumer will answer the phone. We propose and seek comment on requiring gateway providers to confirm that a foreign originator is authorized to use the particular U.S. number that purports to originate the call. We further propose to make clear that this requirement applies only when an originator seeks to place a high volume of calls using a U.S. number, and does not apply to traffic consistent with private, individual use.

82. We seek comment on how a gateway provider can best comply with this requirement. Is it feasible for a gateway provider to obtain useful information? If so, can the gateway provider reliably gather this information prior to calls being placed? If so, how? If information is not available until after some calls have been placed, should we instead require the gateway provider to obtain this information within a set amount of time after receiving the first call purporting to originate from a particular U.S. number? How might a gateway provider get this information? How long is appropriate for gathering this information? Should our requirement be based on the number of calls placed, or the time since the first call was placed? We also seek comment on whether there is the possibility for gateway providers to have contractual relationships with call originators, distinct from their position on the call path, such that they will transmit all calls for a particular caller. If so, does this change the feasibility of obtaining useful information? Should any requirement we adopt apply to all gateway providers, or only to gateway providers with contractual relationships with callers, distinct from the relationship between a caller and originating voice service provider?

83. We seek comment on the scope and extent of this requirement. Should we adopt a carve out to ensure that gateway providers do not prevent origination of emergency calls, including calls to 911, calls from PSAPs, or calls from government emergency outbound numbers? If so, what might this look like? In addition, we specifically propose to impose this requirement only where the originator seeks to place a high volume of calls. We seek comment on this proposal. We are concerned about ensuring that individual callers, such as U.S. residents traveling abroad, are not prevented from placing calls using a number to which they are subscribed while in a foreign country. To address this, should the requirement only be triggered after the gateway provider sees a set number of calls purporting to originate from a particular U.S. number? If so, what is the appropriate threshold to constitute a "high volume" of calls? Are there other measures we could adopt that would ensure that traffic consistent with individual use does not trigger this requirement without allowing the rule to be circumvented by clever

callers? Are there any other issues we should consider?

84. *Upstream Provider as the "Customer."* Alternatively, should we impose a requirement similar to the rule adopted in the *Fourth Call Blocking Order*, and require gateway providers to take steps to know the upstream providers from which they receive traffic and prevent those providers from originating illegal traffic onto the U.S. network? While at least a step removed from the call originator, the provider upstream from a particular gateway provider does have a direct relationship with that gateway provider. As a result, it is more likely for a gateway provider to have ready access to information about that upstream provider. We therefore seek comment on defining the provider immediately upstream from the gateway provider to be the gateway provider's "customer." If we adopt this definition, what should the gateway provider "know" to be able to reasonably claim it "knows" this "customer"? Should we limit our requirement to information readily available to the gateway provider, or should we require additional information that may be more difficult for a gateway provider to obtain? What information would provide the most benefit in stopping illegal calls? Is such information readily available to the gateway provider? If not, what costs or challenges might the gateway provider face in obtaining this information? Are there ways we could reduce or eliminate these costs or complications? What should a gateway provider be required to do with this information? For example, should we require gateway providers to cease accepting traffic from upstream providers that meet certain criteria? Should this requirement only apply to foreign-originated calls that use a U.S. number in the caller ID field? How does this approach compare to the approach of considering the call originator the "customer" discussed further below? Are there any other technical, legal, or policy considerations we should pay particular attention to if we define the customer as the upstream provider, including the impact on small businesses?

85. *Call Originator as the "Customer."* Alternatively, should we consider the call originator the gateway provider's "customer" for purposes of such a requirement? We believe that the originator, as the entity placing the calls, is probably the most relevant "customer" for

the purpose of stopping illegal calls. Unfortunately, the gateway provider, in many cases, may have no direct relationship with the originator, making it significantly more difficult to obtain information. We seek comment on considering the call originator the "customer" for purposes of a know-your-customer requirement. What would be sufficient for a gateway provider to reasonably claim that it "knows" this "customer"? What are the barriers to gateway providers obtaining necessary information from originators and how could we address those barriers? How does this approach compare to the approach of considering the upstream provider the "customer," discussed above? Are there any other technical, legal, or policy considerations we should pay particular attention to if we define the customer as the call originator?

86. *Compliance Deadline*. We propose to require gateway providers to comply with "know-your-customer" requirements by 30 days after publication of the notice of any Order adopting such a requirement in the Federal Register. We seek comment on this proposal. Is there any need to delay compliance? If so, why and how much time do gateway providers reasonably need to comply?

4. Contractual Provisions

87. The NANC and industry stakeholders have recommended that gateway providers require their customers to adopt contractual provisions that would help mitigate illegal robocalling. We seek comment on whether, in light of increased risk of foreign-originated illegal robocall campaigns and the critical role gateway providers play in allowing such calls to reach the U.S. market, we should require gateway providers to adopt specific contractual provisions addressing robocall mitigation with foreign providers from which the gateway provider directly receives traffic carrying U.S. NANP numbers, and, in some cases, traffic from their foreign-end user customers (collectively for purposes of this subsection, foreign partners). Under our proposed definition of gateway provider above, a U.S.-based provider would fall outside of the definition of gateway provider if it is not also acting as an intermediate provider with respect to a particular call. Consistent with that definition, we are also seeking comment on imposing

mandatory contractual obligations on gateway providers where they have entered into contracts with foreign end-user customers to accept their traffic into the U.S, marketplace. To the extent we adopt a broader definition of gateway provider to include those instances where the U.S.-based provider originates calls outside of the U.S. and the U.S.-based provider is not acting as an intermediate provider, we also seek comment on whether we should apply mandatory contractual provisions in those cases. What are the benefits and costs of requiring such contractual amendments?

88. We seek comment on what specific contractual provisions, if any, we should require. Should we require gateway providers to ensure by contract that their foreign partners validate that the calling party is authorized to use the U.S. NANP telephone numbers, for calls with such numbers in the caller ID display? Are we correct in anticipating that if a foreign partner cannot validate the number, there is a significant risk that the number is being spoofed and is therefore likely to be involved in an illegal robocalling campaign? How should we address circumstances in which the foreign partner cannot validate the number on its own? For instance, should we require the gateway provider to require foreign partners by contract to use a third-party telephone number validation service? Should we require gateway providers to ensure that their foreign partners employ know-your-customer practices, and if so should we mandate requiring specific know-your-customer practices? Should we require gateway providers to contractually obligate foreign partners to submit a certification to the Robocall Mitigation Database? We seek comment on what similar contractual provisions providers already have in place, their effectiveness in stopping illegal robocall traffic, and how widespread they are.

89. We seek comment on implementation of any requirement to adopt specific contractual provisions. Should we expand, contract, or alter the scope of foreign partners with which we would require gateway providers to enter into specific contractual provisions? What steps, if any, should we require gateway providers to take to ensure that foreign partners are living up to their contractual commitments? Should we require gateway providers to impose

specific consequences, such as a refusal to accept traffic, on foreign partners that fail to live up to any required contractual provisions? What consequences should we impose a gateway provider that fails to enter into or enforce any required contractual provisions?

90. Consistent with the other mitigation obligations proposed in this FNPRM, we propose to require gateway providers comply with any contractual provisions 30 days after the effective date of an Order adopting such requirements. We seek comment on this proposal. We also seek comment on whether such a period provides sufficient time to comply with such obligations with respect to existing contracts in order to negotiate contractual amendments with foreign partners. Should we modify the deadline for certain classes of providers based on their burden or the benefit that would result in those classes' compliance with the rule? Should we consider any other issues in setting a compliance deadline?

5. General Mitigation Standard

91. In addition to the specific mitigation requirements for which we seek comment above, we also propose to require gateway providers to meet a general obligation to mitigate illegal robocalls. Robocallers have shown that they can adapt to specific safeguards targeting illegal traffic. A general obligation can serve as an effective backstop to ensure that robocallers cannot evade any granular requirements we adopt. In the *Second Caller ID Authentication Report and Order*, the Commission required those voice service providers subject to a robocall mitigation requirement to take "reasonable steps to avoid originating illegal robocall traffic," and established that a robocall mitigation program is sufficient if it "includes detailed practices that can reasonably be expected to significantly reduce the origination of illegal robocalls" and the provider "compl[ies] with the practices it describes." The Commission stated that a program is "insufficient if a provider knowingly or through negligence serves as the originator for unlawful robocall campaigns." We believe imposing an analogous requirement on gateway providers would provide a valuable backstop and help reduce the likelihood that illegal robocalls might make their way to U.S. consumers. Under this approach, gateway providers would be required

to take reasonable steps to avoid transiting illegal robocall traffic. What would be the benefits and drawbacks of doing so? What would constitute "reasonable steps" in this context, aside from any of the actions proposed in this FNPRM? Would the consistency of obligations between gateway providers and voice service providers facilitate innovation and development of novel, effective robocall mitigation techniques? Would it ease compliance? Is a standards-based approach sufficient to address the difficult task of mitigating foreign-originated illegal robocalls? Should we adopt a standards-based approach but establish a different standard for effective robocall mitigation for gateway providers? What should that standard be? Does a standards-based approach make compliance more difficult, particularly for small entities that may less easily be able to identify appropriate practices?

92. Instead of establishing a general mitigation standard based on the standard in the *Second Caller ID Authentication Report and Order*, should we instead adopt a general standard by building upon the obligation in the *Fourth Call Blocking Order* for voice service providers (including intermediate providers) to mitigate robocall traffic by adopting "affirmative, effective measures to prevent new and renewing customers from using their network to originate illegal calls"? This duty differs in certain respects from the duty for voice service providers subject to a robocall mitigation requirement to take "reasonable steps to avoid originating illegal robocall traffic." For example, there is no duty for gateway providers to take action with respect to existing customers. Should we establish a general mitigation obligation for gateway providers based on a modified version of this duty? What should those modifications be? Should we require gateway providers to take affirmative, effective measures to prevent current, new, and renewing customers from using their network to transit illegal calls? Are other modifications appropriate? Instead or in addition to making such modifications, should we provide additional guidance to gateway providers about what measures would be deemed "affirmative" and "effective"? What should that guidance be?

93. We seek comment on an appropriate deadline for any general mitigation standard

we adopt. We believe that any compliance deadline we adopt should, at a minimum, be 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. We therefore urge commenters proposing a standard to propose a specific deadline consistent with these principles.

E. Robocall Mitigation Database

94. We propose to require 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. We also take this opportunity to address other issues related to the Robocall Mitigation Database that are not specifically related to gateway providers. First, we seek comment on revisions to the information that filers must submit to the Robocall Mitigation Database. Second, we clarify the obligations of voice service providers and intermediate providers with respect to calls to and from PSAPs and other emergency services providers.

95. *Gateway Providers.* While we declined to impose a filing requirement on intermediate providers that had no robocall mitigation obligations in the *Second Caller ID Authentication Report and Order*, we believe that requiring gateway providers to do so now in conjunction with any new robocall mitigation obligations we adopt is appropriate and situates gateway providers consistently with voice service providers under our STIR/SHAKEN rules. We seek comment on our proposal to require gateway providers to submit a certification. We anticipate that requiring certification will encourage compliance and facilitate enforcement efforts and industry cooperation to address problems. We also anticipate that a registration requirement would not be more costly for gateway providers than voice service providers. We seek comment on this analysis. Are there additional benefits of requiring registration? Do gateway providers face additional costs compared to voice service providers that we should consider? Rather than require gateway providers to file in the Robocall Mitigation Database, should we instead impose some other filing obligation? What would that obligation be?

96. We propose requiring gateway providers to submit the same information that

voice service providers must submit under Commission rules. Specifically, we propose requiring gateway providers to 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. In the alternative, we seek comment on whether to alter or remove any of these obligations as applied to gateway providers, and whether gateway providers should submit any additional information beyond the information required from originating and terminating voice service providers. If we adopt specific robocall mitigation requirements, should we relieve gateway providers of the obligation to describe their robocall mitigation practices? Would this belt-and-suspenders approach to certification only add compliance costs with limited benefit? If we did not require gateway providers to describe their robocall mitigation practices, should they be required to submit any alternative information? If so, what should that be? We seek comment on any modifications we should make to the filing process for those gateway providers that are also voice service providers.

97. Similar to our recently proposed rules for VoIP direct access applicants, should we require 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 . . . "? We propose that information in any gateway provider certification would also be subject to the existing duty to update that certification within 10 business days, ensuring that the information is kept up to date. 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, and if so what threshold should we set?

98. We propose to extend the prohibition on accepting traffic from unlisted providers to gateway providers. Under this proposal, intermediate providers and terminating voice service

providers would be prohibited from accepting traffic from a gateway provider not listed in the Robocall Mitigation Database. We believe 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 illegal robocalls. We seek comment on that conclusion and this proposal. Taking into consideration the time between the effective date of the prohibition on voice service providers (September 28, 2021) from accepting traffic from other unlisted voice service providers and the comment due date of this FNPRM, is there any preliminary evidence that the prohibition has been beneficial in the ways the Commission envisioned? We also propose that this prohibition should go into effect 90 days following the effective date of the requirement for gateway providers to submit a certification to the Robocall Mitigation Database. Ninety days between the effective date of the filing obligation and the beginning of the requirement to reject traffic from non-filers is the same time period as that adopted in the *Second Caller ID Authentication Report and Order* for voice service providers. We seek comment on providers' experience with that 90-day timeframe and whether it would be appropriate in this instance. Should we set a shorter time period to ensure Americans benefit from this scheme sooner? Or do voice service providers and intermediate providers need additional time, beyond 90 days, to come into compliance with any blocking obligation and, if so, why? How, if at all, should we tailor the information that gateway providers must submit to the Robocall Mitigation Database to ensure that a downstream provider has sufficient information to know whether to block calls depending on the call-by-call "role" of the upstream provider? For example, if an upstream provider is acting as a gateway provider for a call and has submitted a certification as a voice service provider to the Robocall Mitigation Database, but has not submitted its certification as a gateway provider, what information does that downstream provider need to know to block the call under our proposed rule if and when it becomes effective?

99. In line with our proposals above to require gateway providers to implement mitigation requirements by 30 days after publication of the notice of an Order adopting this requirement in the Federal Register, we propose to require gateway providers to submit a certification to the Robocall Mitigation Database by that same date and to thereafter amend such certification of compliance to attest to STIR/SHAKEN compliance by the deadline established in this proceeding, subject to publication in the Federal Register of notice of approval by OMB of any associated PRA obligations. We seek comment on this approach and any alternatives. For example, should we instead require gateway providers submit an interim certification by an earlier date so that the Commission and the general public know the status of gateway providers' STIR/SHAKEN implementation? Would the benefits of requiring an additional interim filing outweigh the burdens? What other considerations should we take into account in setting any filing deadlines?

100. *Identifying Information for All Filers.* We take this opportunity to seek comment on whether we should require Robocall Mitigation Database filers—including voice service providers and, if required, gateway providers—to submit additional identifying indicia, such as a Carrier Identification Code, Operating Company Number, and/or Access Customer Name Abbreviation. We anticipate that requiring some additional identifying information may ease compliance by facilitating searches within the Robocall Mitigation Database and cross-checking information within the Robocall Mitigation Database against other sources. Do commenters agree? If so, what additional information should we require? What are the benefits and costs of such a requirement? We recognize that as of the date we adopt this FNPRM, a large number of voice service providers have already filed in the Robocall Mitigation Database, and requiring any additional information would require these providers to revise their filings. As we have explained, to date, approximately 4,948 voice service providers have submitted information into the Robocall Mitigation Database. Additionally, we realize that the September 28 blocking deadline has passed and that the identifying information we seek comment on may not be as

useful as it would have been prior to this deadline. Based on these facts, does the benefit of requiring additional information nonetheless outweigh the burden of asking such a high number of voice service providers to refile? If not, should we consider applying this requirement on a prospective-only basis? Would this approach still have benefit even 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, that are unlikely to have this identifying information? If so, how should any new requirements address these filers? 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?

101. *Public Safety Calls.* We take this opportunity to clarify that even if a voice service provider (or, if we adopt our proposal in today's FNPRM, a gateway 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. Additionally, consistent with the Commission's previous statement that its call-blocking rules "do not authorize the blocking of calls to 911 under any circumstances," calls to 911 must not be blocked, even if originated by a voice service provider not in the Robocall Mitigation Database or otherwise subject to blocking. And as regards outbound emergency calls, we reiterate the Commission's position that all voice service providers and intermediate providers "must make all reasonable efforts to ensure that calls from PSAPs and government outbound emergency numbers are not blocked." We adopt this clarification to ensure completion of emergency calls and to clarify that the scope of the exception for emergency calls is identical between our call blocking rules and our rules prohibiting acceptance of traffic from voice service providers not listed in the Robocall

Mitigation Database.

102. We seek comment on whether we should modify our rules to reflect this clarification. We also seek comment on whether we should expand upon our clarification. Does our clarification contain any ambiguities that we should address, and if so how should we address them? For example, should we make clear what "reasonable efforts" we expect voice service providers and intermediate providers to take to ensure completion of outbound emergency calls? If so, what specific steps should we require? Would prohibiting providers from blocking calls on a "whitelist" of public safety numbers be effective, or would it instead provide a roadmap for bad actors to exploit? We note that the Commission has previously declined to adopt such a list, finding that it "would likely to do more harm than good." We seek comment on whether circumstances have changed since the Commission's prior decision that would make this option more viable. Are there fewer concerns for such a list in the context of gateway providers? Are there other ways bad actors could exploit this emergency exception to originate illegal robocalls, either directed at PSAPs (because calls to 911 may not be blocked) or directed to the general public by posing as emergency callers (because providers must make all reasonable efforts to ensure that calls from PSAPs and government outbound emergency numbers are not blocked)? If so, what steps can we take to minimize that threat while ensuring the vital goal of emergency call completion? How should we account for emergency calls if we require gateway providers to file in the Robocall Mitigation Database? Are emergency calls to U.S. PSAPs likely to originate abroad? We also propose that any calls to and from PSAPs and government outbound emergency numbers that may be otherwise subject to mandatory call blocking duties adopted pursuant to this FNPRM should be subject to the same emergency call exception and clarification that we adopt today, as well as any further clarifications that we adopt pursuant to the questions above, and we seek comment on this proposal.

F. Alternative Approaches

103. We seek comment on alternative approaches to stop illegal foreign-originated

robocalls. This FNPRM proposes imposing obligations on gateway providers because they are in the unique position of acting as the conduit for all foreign-originated calls. We anticipate that rules focused on gateway providers would be the most efficient and effective way to prevent illegal robocalls from reaching U.S. consumers and businesses from abroad. At the same time, we want to explore all available options and thus seek comment on whether we should instead pursue alternative approaches to enhancing our rules to target foreign-originated robocalls.

104. We first seek comment on strengthening our prohibition on U.S.-based providers accepting traffic carrying U.S. NANP numbers that is received "directly from" foreign voice service providers that are not in the Robocall Mitigation Database. By its terms, this 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—at present, the prohibition only applies to traffic received directly from the originating foreign provider. Some have argued that this loophole allows a significant portion of foreign-originated robocall traffic carrying U.S. NANP numbers to reach the U.S. outside of the prohibition. We seek comment on whether this is the case and, if so, whether we should expand the prohibition and require U.S.-based providers to reject traffic carrying U.S. NANP numbers directly from *any* foreign provider not in the Robocall Mitigation Database. What are the benefits and burdens of this approach? Should we require U.S.-based providers to ensure that foreign intermediate providers comply with specific robocall mitigation practices, such as know-your-customer practices, and describe in their certifications the specific robocall mitigation practices they have implemented? Are most foreign intermediate providers also originating and exchanging traffic with U.S. NANP numbers directly with U.S. providers, indicating that most foreign providers are already covered under the current prohibition? 609 foreign voice service providers have already filed in the Robocall Mitigation Database. We seek comment on what percentage of foreign providers currently subject to the prohibition this represents, compared to the percentage of foreign providers that would be subject to our proposed expanded prohibition. If we expand the

prohibition to encompass foreign intermediate providers, what compliance deadline should we set?

105. Conversely, should we limit or eliminate the foreign provider prohibition rather than expand it? Some argue that the compliance burden of the current rule on foreign voice service providers is significant, that many providers did not register by the deadline, and therefore there is a significant risk that domestic providers will unnecessarily block foreign-originated calls. We seek comment on the validity of these assertions and whether a rule expansion would compound those burdens and risks. Others argue that, at a minimum, foreign voice service providers needed additional time to submit a certification to the Robocall Mitigation Database. If the burdens of the current rule are large and the benefits small, should we consider eliminating the current rule, particularly if we adopt effective measures for gateway providers to stop illegal robocall traffic from entering the U.S. market?

106. In light of the unique difficulties foreign service providers may face in timely registering with the Commission's new Robocall Mitigation Database, the fact that the foreign provider prohibition can be evaded by transmitting traffic via one or more foreign intermediate providers, and in order to avoid the potential disruption associated with such delays while permitting the Commission to explore these potentially more effective measures, we conclude that the public interest will be served by not enforcing the foreign provider prohibition during the pendency of this proceeding. While ZipDX suggests a "narrower deferment" that would allow enforcement if a foreign provider is responsible for a "significant or on-going illegal robocalling activity," we decline taking such an approach because it would involve engaging in a line-drawing exercise for which we do not have sufficient guidance and data and ZipDX does not suggest a specific, administrable approach. We anticipate that we will make a final decision regarding whether to eliminate, retain, or enhance the foreign provider prohibition as part of our larger consideration of how best to address illegal robocalls originating abroad in the order issued pursuant to this FNPRM. Therefore, until that time, domestic voice service providers and

intermediate providers may accept traffic carrying U.S. NANP numbers sent directly from foreign voice service providers not listed in the Robocall Mitigation Database.

G. Expected Benefits and Costs

107. As noted above, a large portion of illegal robocalls originate abroad, and that share may be growing. We therefore anticipate that the benefits of our proposals will far outweigh the costs imposed on gateway providers.

108. As to expected benefits, the Commission found in the *First Caller ID Authentication Report and Order and Further Notice of Proposed Rulemaking* that widespread deployment of STIR/SHAKEN will increase the effectiveness of the framework for both voice service providers and their subscribers, producing a potential benefit of at least $13.5 billion annually due to the reduction in nuisance calls and fraud. In addition, the Commission identified many non-quantifiable benefits, such as restoring confidence in incoming calls and reliable access to emergency and healthcare communications.

109. We anticipate that the impact of our proposals, including the deterrence that arises from authenticating unauthenticated foreign-originated calls, will account for a large share of that $13.5 billion benefit because of the significant share of illegal calls originating outside our country. 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 $13.5 billion minimum benefit. We seek comment on this analysis and on the possible benefits of the requirements we propose.

110. We believe that the costs imposed on gateway providers by our proposed changes, at least some of which are likely minimal, will be far exceeded by the expected benefits. For example, many intermediate providers that would be classified as gateway providers under our proposed definition are already voice service providers and have already implemented or are required to soon implement STIR/SHAKEN authentication on their networks. Moreover, as the Commission stated in the *First Caller ID Authentication Report and Order and Further Notice of*

Proposed Rulemaking, an overall reduction in illegal robocalls will greatly lower providers' network costs by eliminating both the unwanted traffic congestion and the labor costs of handling numerous customer complaints. We therefore believe that the proposals in this FNPRM would impose only minimal short-term costs on gateway providers while lowering long-term network costs for gateway providers and other domestic service providers. We seek comment on this analysis and whether it remains valid in light of industry experience in implementing STIR/SHAKEN and the Commission's various blocking regimes? Is it equally applicable to gateway providers? We also seek detailed comment on the potential costs associated with each proposal. Will these costs vary according to the size of the provider? Does the benefit of each proposal outweigh its cost? How do the proposed compliance deadlines for each requirement and possible alternative deadlines affect the benefits and costs?

111. *Digital Equity and Inclusion.* The Commission, as part of its continuing effort to advance digital equity for all, including people of color, persons with disabilities, persons who live in rural or Tribal areas, and others who are or have been historically underserved, marginalized, or adversely affected by persistent poverty or inequality, invites comment on any equity-related considerations and benefits (if any) that may be associated with the proposals and issues discussed herein. 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." The term "equity" is used here consistent with Executive Order 13985 as the consistent and systematic fair, just, and impartial treatment of all individuals, including individuals who belong to underserved communities that have been denied such treatment, such as Black, Latino, and Indigenous and Native American persons, Asian Americans and Pacific Islanders and other persons of color; members of religious minorities; lesbian, gay, bisexual, transgender, and queer (LGBTQ+) persons; persons with disabilities; persons who live in rural areas; and persons

otherwise adversely affected by persistent poverty or inequality. Specifically, we seek comment on how our proposals may promote or inhibit advances in diversity, equity, inclusion, and accessibility, as well the scope of the Commission's relevant legal authority.

H. Legal Authority

112. We propose to adopt the foregoing obligations pursuant to the legal authority we relied upon in prior caller ID authentication and call blocking orders.

113. *Caller ID Authentication.* We propose to 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. In the *Second Caller ID Authentication Report and Order*, the Commission found it had the authority to impose caller ID authentication obligations on intermediate providers under these provisions. It reasoned that "[c]alls that transit the networks of intermediate providers with illegally spoofed caller ID are exploiting numbering resources" and so found authority under section 251(e). And 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," and it stressed that intermediate providers "play an integral role in the success of STIR/SHAKEN across the voice network." While that *Order* did not specifically discuss gateway providers, we propose to conclude that we can impose an authentication obligation on gateway providers on the same basis. Indeed, we propose to define gateway providers as a subset of intermediate providers; thus, we tentatively conclude that the *Second Caller ID Authentication Report and Order* already accounted for the actions we propose today. We seek comment on this proposal. Should we revisit the Commission's earlier conclusion that it has authority to place these obligations on intermediate—including gateway—providers? Are there other sources of authority, including the TRACED Act, that we could invoke to impose our caller ID authentication rules on gateway providers?

114. *Robocall Mitigation and Call Blocking.* We propose to adopt our robocall

mitigation and call blocking provisions on gateway providers pursuant to sections 201(b), 202(a), 251(e), the Truth in Caller ID Act, the TRACED Act, and, where appropriate, 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*. We seek comment on this proposal.

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

116. In the *Fourth Call Blocking Order*, the Commission required voice service providers "to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls," which includes a duty to "know" their customers. Additionally, the Commission required voice service providers, including intermediate providers, to "take steps to

effectively mitigate illegal traffic when notified by the Commission," which may require blocking when applied to gateway providers. The Commission also adopted traceback obligations. The Commission concluded that it had the authority to adopt these requirements pursuant to sections 201(b), 202(a), and 251(e) of the Act, as well as the Truth in Caller ID Act and its ancillary authority. Sections 201(b) and 202(a) provide the Commission with "broad authority to adopt rules governing just and reasonable practices of common carriers." Accordingly, the Commission found that the new blocking rules were "clearly within the scope of our section 201(b) and 202(a) authority" and "that it is essential that the rules apply to all voice service providers," applying its ancillary authority in section 4(i). The Commission also found that section 251(e) and the Truth in Caller ID Act provided the basis "to prescribe rules to prevent the unlawful spoofing of caller ID and abuse of NANP resources by all voice service providers," a category that includes VoIP providers and, in the context of our call blocking orders gateway providers. We believe that these same statutory provisions authorizing our current mitigation and blocking rules support the mandatory mitigation and blocking obligations we propose to impose on gateway providers here. Are there additional sources of authority that we should consider?

117. We propose to find additional authority in section 7 of the TRACED Act. The Commission initiated a rulemaking to "help protect a subscriber from receiving unwanted calls or text messages from a caller using an unauthenticated number" in the *Third Call Blocking Order and Further Notice of Proposed Rulemaking* but declined to take further action in the *Fourth Call Blocking Order.* We believe that several of the proposals we make today would have the effect of protecting consumers from unwanted calls from unauthenticated numbers. In particular, we believe that our mandatory blocking and "know-your-customer" proposals would further these goals. We seek comment on this belief. Is this an appropriate use of the authority granted in TRACED Act section 7? What should we consider, including the considerations

listed in section 7(b) of the TRACED Act, in determining whether any rules we adopt are consistent with our authority under that section?

118. While we propose to conclude that our direct sources of authority provide an ample basis to adopt our proposed rules on all gateway providers, we believe that our ancillary authority in section 4(i) provides an independent basis to do so with respect to gateway providers that have not been classified as common carriers, and we seek comment on this view. We anticipate that the proposed regulations are "reasonably ancillary to the Commission's effective performance of its . . . responsibilities." Specifically, gateway providers interconnected with the public switched telephone network and exchanging IP traffic clearly constitutes "communication by wire and radio." We believe that requiring gateway providers to comply with our proposed rules is reasonably ancillary to the Commission's effective performance of its statutory responsibilities under section 152(a), as well as reasonably ancillary to our exercise of authority 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. We seek comment on this analysis.

119. *Indirect Effect on Foreign Service Providers.* We propose to conclude that, to the extent any of the rules we seek to adopt today have an effect on foreign service providers, that effect is only indirect and therefore consistent with the Commission's authority. 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 past Commission precedent confirmed by the courts. This includes the authority, pursuant to section 201, for the Commission to require U.S. providers to modify their contracts with a foreign provider with respect to "foreign communication" to ensure that the charges and practices are "just and reasonable." We seek comment on whether any of our proposed rules exceed the scope of our

jurisdiction over foreign communications that enter the United States. We also seek comment on whether any of our proposed rules would be contrary to any of our international treaty obligations, other international laws and rules, or create a risk of foreign retaliation.

IV. Initial Regulatory Flexibility Analysis

120. As required by the Regulatory Flexibility Act of 1980, as amended (RFA), 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 FNPRM. 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 FNPRM. The Commission will send a copy of the FNPRM, including this IRFA, to the Chief Counsel for Advocacy of the Small Business Administration (SBA). In addition, the FNPRM and IRFA (or summaries thereof) will be published in the **Federal Register**.

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

121. In order to continue the Commission's work combating illegal calls, this FNPRM proposes to impose several obligations on gateway providers. Specifically, the FNPRM proposes to require gateway providers to authenticate and employ robocall mitigation techniques on all SIP calls that they allow into the United States from abroad that display a U.S. number in the caller ID field. The FNPRM also proposes that gateway providers should engage in robocall mitigation by (1) responding to all traceback requests from the Commission, law enforcement, and the industry traceback consortium within 24 hours; (2) complying with mandatory call blocking requirements; (3) complying with enhanced know-your-customer obligations; (4) complying with a general duty to mitigate illegal robocalls; and (5) filing a certification in the Robocall Mitigation Database. The Commission also proposes one blocking requirement for intermediate and terminating providers immediately downstream from the gateway provider, which would require those providers to block all traffic from a gateway provider that fails to block or effectively mitigate illegal traffic when notified of such traffic by the Commission.

B. Legal Basis

122. The FNPRM 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 FNPRM proposes to find authority under sections 201(a) and (b), 202(a), 251(e), the Truth in Caller ID Act, the TRACED Act and, where appropriate, ancillary authority. The FNPRM also proposes to conclude that, to the extent any of the rules we seek to adopt today have an effect on foreign service providers, that effect is only indirect and therefore consistent with the Commission's authority. The FNPRM solicits comment on these proposals.

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

123. 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. The RFA generally defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small governmental jurisdiction." In addition, the term "small business" has the same meaning as the term "small-business concern" under the Small Business Act. A "small-business concern" is one which: (1) is independently owned and operated; (2) is not dominant in its field of operation; and (3) satisfies any additional criteria established by the SBA.

1. Wireline Carriers

124. *Wired Telecommunications Carriers*. The U.S. Census Bureau defines this industry as "establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a

variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband internet services. By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry." The SBA has developed a small business size standard for Wired Telecommunications Carriers, which consists of all such companies having 1,500 or fewer employees. U.S. Census Bureau data for 2012 show that there were 3,117 firms that operated that year. Of this total, 3,083 operated with fewer than 1,000 employees. Thus, under this size standard, the majority of firms in this industry can be considered small.

125. *Local Exchange Carriers (LECs)*. Neither the Commission nor the SBA has developed a size standard for small businesses specifically applicable to local exchange services. The closest applicable NAICS Code category is Wired Telecommunications Carriers. Under the applicable SBA size standard, such a business is small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2012 show that there were 3,117 firms that operated for the entire year. Of that total, 3,083 operated with fewer than 1,000 employees. Thus under this category and the associated size standard, the Commission estimates that the majority of local exchange carriers are small entities.

126. *Incumbent LECs*. Neither the Commission nor the SBA has developed a small business size standard specifically for incumbent local exchange services. The closest applicable NAICS Code category is Wired Telecommunications Carriers. Under the applicable SBA size standard, such a business is small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2012 indicate that 3,117 firms operated the entire year. Of this total, 3,083 operated with fewer than 1,000 employees. Consequently, the Commission estimates that most providers of incumbent local exchange service are small businesses that may be affected by our actions. According to Commission data, one thousand three hundred and seven (1,307) Incumbent Local Exchange Carriers reported that they were incumbent local exchange service providers. Of this

total, an estimated 1,006 have 1,500 or fewer employees. Thus, using the SBA's size standard the majority of incumbent LECs can be considered small entities.

127. *Competitive Local Exchange Carriers (Competitive LECs), Competitive Access Providers (CAPs), Shared-Tenant Service Providers, and Other Local Service Providers.* Neither the Commission nor the SBA has developed a small business size standard specifically for these service providers. The appropriate NAICS Code category is Wired Telecommunications Carriers and under that size standard, such a business is small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2012 indicate that 3,117 firms operated during that year. Of that number, 3,083 operated with fewer than 1,000 employees. Based on these data, the Commission concludes that the majority of Competitive LECS, CAPs, Shared-Tenant Service Providers, and Other Local Service Providers, are small entities. According to Commission data, 1,442 carriers reported that they were engaged in the provision of either competitive local exchange services or competitive access provider services. Of these 1,442 carriers, an estimated 1,256 have 1,500 or fewer employees. In addition, 17 carriers have reported that they are Shared-Tenant Service Providers, and all 17 are estimated to have 1,500 or fewer employees. Also, 72 carriers have reported that they are Other Local Service Providers. Of this total, 70 have 1,500 or fewer employees. Consequently, based on internally researched FCC data, the Commission estimates that most providers of competitive local exchange service, competitive access providers, Shared-Tenant Service Providers, and Other Local Service Providers are small entities.

128. 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." The SBA's Office of Advocacy contends that, for RFA purposes, small incumbent LECs are not dominant in their field of operation because any such dominance is not "national" in scope. 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.

129. *Interexchange Carriers (IXCs)*. Neither the Commission nor the SBA has developed a small business size standard specifically for Interexchange Carriers. The closest applicable NAICS Code category is Wired Telecommunications Carriers. The applicable size standard under SBA rules is that such a business is small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2012 indicate that 3,117 firms operated for the entire year. Of that number, 3,083 operated with fewer than 1,000 employees. According to internally developed Commission data, 359 companies reported that their primary telecommunications service activity was the provision of interexchange services. Of this total, an estimated 317 have 1,500 or fewer employees. Consequently, the Commission estimates that the majority of interexchange service providers are small entities.

130. *Cable System Operators (Telecom Act Standard).* The Communications Act of 1934, as amended (the Act), also contains a size standard for small cable system operators, which is "a cable operator that, directly or through an affiliate, serves in the aggregate fewer than one percent of all subscribers in the United States and is not affiliated with any entity or entities whose gross annual revenues in the aggregate exceed $250,000,000." As of 2018, there were approximately 50,504,624 cable video subscribers in the United States. Accordingly, an operator serving fewer than 505,046 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. We note that the Commission neither requests nor collects information on whether cable system operators are affiliated with entities whose gross annual revenues exceed $250 million. Therefore we are unable at this time to estimate with greater precision the number of cable system operators that would qualify as small cable operators under *the* definition in the Act.

131. *Other Toll Carriers.* Neither the Commission nor the SBA has developed a size standard 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. The closest applicable size standard under SBA rules is for Wired Telecommunications Carriers. The U.S. Census Bureau defines this industry as "establishments primarily engaged in operating and/or providing access to transmission facilities and infrastructure that they own and/or lease for the transmission of voice, data, text, sound, and video using wired communications networks. Transmission facilities may be based on a single technology or a combination of technologies. Establishments in this industry use the wired telecommunications network facilities that they operate to provide a variety of services, such as wired telephony services, including VoIP services, wired (cable) audio and video programming distribution, and wired broadband internet services. By exception, establishments providing satellite television distribution services using facilities and infrastructure that they operate are included in this industry." Under that size standard, such a business is small if it has 1,500 or fewer employees. Census data for 2012 show that there were 3,117 firms that operated that year. Of this total, 3,083 operated with fewer than 1,000 employees. Thus, under this category and the associated small business size standard, the majority of other toll carriers can be considered small.

2. Wireless Carriers

132. *Wireless Telecommunications Carriers (except Satellite)*. This industry comprises establishments engaged in operating and maintaining switching and transmission facilities to provide communications via the airwaves. Establishments in this industry have spectrum licenses and provide services using that spectrum, such as cellular services, paging services, wireless internet access, and wireless video services. The appropriate size standard under SBA rules is that such a business is small if it has 1,500 or fewer employees. For this industry, U.S. Census Bureau data for 2012 show that there were 967 firms that operated for the entire year. Of this total, 955 firms employed fewer than 1,000 employees and 12 firms employed of 1000 employees or more. Thus under this category and the associated size

standard, the Commission estimates that the majority of wireless telecommunications carriers (except satellite) are small entities.

133. The Commission's own data—available in its Universal Licensing System—indicate that, as of August 31, 2018 there are 265 Cellular licensees that will be affected by our actions. The Commission does not know how many of these licensees are small, as the Commission does not collect that information for these types of entities. Similarly, according to internally developed Commission data, 413 carriers reported that they were engaged in the provision of wireless telephony, including cellular service, Personal Communications Service (PCS), and Specialized Mobile Radio (SMR) Telephony services. Of this total, an estimated 261 have 1,500 or fewer employees, and 152 have more than 1,500 employees. Thus, using available data, we estimate that the majority of wireless firms can be considered small.

134. *Satellite Telecommunications.* This category comprises firms "primarily engaged in providing telecommunications services to other establishments in the telecommunications and broadcasting industries by forwarding and receiving communications signals via a system of satellites or reselling satellite telecommunications." Satellite telecommunications service providers include satellite and earth station operators. The category has a small business size standard of $35 million or less in average annual receipts, under SBA rules. For this category, U.S. Census Bureau data for 2012 show that there were a total of 333 firms that operated for the entire year. Of this total, 299 firms had annual receipts of less than $25 million. Consequently, we estimate that the majority of satellite telecommunications providers are small entities.

3. Resellers

135. *Local Resellers*. The SBA has not developed a small business size standard specifically for Local Resellers. The SBA category of Telecommunications Resellers is the closest NAICs code category for local resellers. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications

services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. Mobile virtual network operators (MVNOs) are included in this industry. Under the SBA's size standard, such a business is small if it has 1,500 or fewer employees. U.S. Census Bureau data from 2012 show that 1,341 firms provided resale services during that year. Of that number, all operated with fewer than 1,000 employees. Thus, under this category and the associated small business size standard, the majority of these resellers can be considered small entities. According to Commission data, 213 carriers have reported that they are engaged in the provision of local resale services. Of these, an estimated 211 have 1,500 or fewer employees and two have more than 1,500 employees. Consequently, the Commission estimates that the majority of local resellers are small entities.

136. *Toll Resellers*. The Commission has not developed a definition for Toll Resellers. The closest NAICS Code Category is Telecommunications Resellers. The Telecommunications Resellers industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. MVNOs are included in this industry. The SBA has developed a small business size standard for the category of Telecommunications Resellers. Under that size standard, such a business is small if it has 1,500 or fewer employees. 2012 Census Bureau data show that 1,341 firms provided resale services during that year. Of that number, 1,341 operated with fewer than 1,000 employees. Thus, under this category and the associated small business size standard, the majority of these resellers can be considered small entities. According to Commission data, 881 carriers have reported that they are engaged in the provision of toll resale services. Of this total, an estimated 857 have 1,500 or fewer employees. Consequently, the Commission estimates that the majority of toll resellers are small entities.

137. *Prepaid Calling Card Providers.* Neither the Commission nor the SBA has developed a small business definition specifically for prepaid calling card providers. The most appropriate NAICS code-based category for defining prepaid calling card providers is Telecommunications Resellers. This industry comprises establishments engaged in purchasing access and network capacity from owners and operators of telecommunications networks and reselling wired and wireless telecommunications services (except satellite) to businesses and households. Establishments in this industry resell telecommunications; they do not operate transmission facilities and infrastructure. Mobile virtual networks operators (MVNOs) are included in this industry. Under the applicable SBA size standard, such a business is small if it has 1,500 or fewer employees. U.S. Census Bureau data for 2012 show that 1,341 firms provided resale services during that year. Of that number, 1,341 operated with fewer than 1,000 employees. Thus, under this category and the associated small business size standard, the majority of these prepaid calling card providers can be considered small entities. According to Commission data, 193 carriers have reported that they are engaged in the provision of prepaid calling cards. All 193 carriers have 1,500 or fewer employees. Consequently, the Commission estimates that the majority of prepaid calling card providers are small entities that may be affected by these rules..

4. Other Entities

138. *All Other Telecommunications*. The "All Other Telecommunications" category is comprised of establishments primarily engaged in providing specialized telecommunications services, such as satellite tracking, communications telemetry, and radar station operation. This industry also includes establishments primarily engaged in providing satellite terminal stations and associated facilities connected with one or more terrestrial systems and capable of transmitting telecommunications to, and receiving telecommunications from, satellite systems. Establishments providing Internet services or voice over Internet protocol (VoIP) services via client-supplied telecommunications connections are also included in this industry. The SBA has

developed a small business size standard for "All Other Telecommunications", which consists of all such firms with annual receipts of $35 million or less. For this category, U.S. Census Bureau data for 2012 show that there were 1,442 firms that operated for the entire year. Of those firms, a total of 1,400 had annual receipts less than $25 million and 15 firms had annual receipts of $25 million to $49,999,999. Thus, the Commission estimates that the majority of "All Other Telecommunications" firms potentially affected by our action can be considered small.

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

139. The FNPRM proposes to impose several obligations on gateway providers, many of whom may be small entities. Specifically, we propose to require gateway providers to authenticate and employ robocall mitigation techniques on all SIP calls that they allow into the United States from abroad that display a U.S. number in the caller ID field. The FNPRM also proposes that gateway providers should engage in robocall mitigation by (1) responding to all traceback requests from the Commission, law enforcement, and the industry traceback consortium within 24 hours; (2) complying with mandatory call blocking requirements; (3) complying with enhanced know-your-customer obligations; (4) complying with a general duty to mitigate illegal robocalls; and (5) filing a certification in the Robocall Mitigation Database. The FNPRM also proposes one blocking requirement for intermediate and terminating providers immediately downstream from the gateway provider, which would require those providers to block all traffic from a gateway provider that fails to block or effectively mitigate illegal traffic when notified of such traffic by the Commission. This proposal may also cover small entities.

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

140. 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. The FNPRM seeks comment on the particular impacts that the proposed rules may have on small entities. The FNPRM seeks comment on whether the costs of the proposed gateway provider authentication requirement may vary by provider, including those providers that have not yet implemented STIR/SHAKEN, such as small voice service providers. The FNPRM also seeks comment on the burdens on "small gateway providers" of a 24-hour traceback requirement. It also seeks comment on the impact on small businesses whose traffic may be blocked under our proposed blocking rules and know your customer obligations. The FNPRM also seeks comment on whether a general mitigation approach may make compliance more difficult for small entities.

F. Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rules

142. None**.**

V. PROCEDURAL MATTERS

143. *Initial Regulatory Flexibility Analysis*. As required by the Regulatory Flexibility Act, the Commission has prepared an Initial Regulatory Flexibility Analysis (IRFA) of the possible significant economic impact on small entities of the policies and rules addressed in this FNPRM. Written public comments are requested on the IRFA. Comments must be filed by the deadlines for comments on the FNPRM 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 FNPRM, including the IRFA, to the Chief Counsel for Advocacy of the SBA.

144. *Paperwork Reduction Act*. The FNPRM contains proposed new 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.

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

VI. ORDERING CLAUSES

146. Accordingly, IT IS ORDERED, 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), 403, that this Further Notice of Proposed Rulemaking IS ADOPTED.

147. 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 (IRFA), to the Chief Counsel for Advocacy of the Small Business Administration.

List of Subjects in 47 CFR Part 64

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

FEDERAL COMMUNICATIONS COMMISSION

Katura Jackson,

Federal Register Liaison Officer.

For the reasons discussed in the preamble, the Federal Communications Commission proposes to amend 47 CFR part 64 as follows:

1. The authority for part 64 continues to read as follows:

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

2. Amend § 64.1200 by adding new paragraph (f)(19), revising paragraphs (n)(1) through (3), adding paragraphs (o) and (p) to read as follows:

§ 64.1200 Delivery restrictions.

* * * * *

(f) * * *

(19) The term *gateway provider* means 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.

* * * * *

(n) * * *

(1) Respond fully and in a timely manner to all traceback requests from the Commission, civil law enforcement, criminal law enforcement, and the industry traceback consortium. Where the voice service provider is a gateway provider, it must respond within 24 hours of receipt of such a request;

(2) Take affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal traffic; and,

(3) Take steps to effectively mitigate illegal traffic when it receives actual written notice of such traffic from the Commission through its Enforcement Bureau.

(i) In providing notice, the Enforcement Bureau shall identify with as much particularity as possible the suspected traffic; provide the basis for the Enforcement Bureau's reasonable belief that the identified traffic is unlawful; cite the statutory or regulatory provisions the suspected traffic appears to violate; and direct the voice service provider receiving the notice that it must comply with this section;

(ii) Each notified provider must promptly investigate the identified traffic. Each notified provider must then promptly report the results of its investigation to the Enforcement Bureau, including any steps the provider has taken to effectively mitigate the identified traffic or an explanation as to why the provider has reasonably concluded that the identified calls were not illegal and what steps it took to reach that conclusion. Should the notified provider find that the traffic comes from an upstream provider with direct access to the U.S. Public Switched Telephone Network, that provider must promptly inform the Enforcement Bureau of the source of the traffic and, if possible, take steps to mitigate this traffic;

(iii) If the notified provider is a gateway provider, that provider must, after conducting the investigation described in paragraph (ii) of this section, promptly block all traffic associated with the traffic pattern identified in the Enforcement Bureau's notice; and

(iv) Should a gateway provider fail to comply with the requirements of paragraph (iii) of this section, the Commission, through its Enforcement Bureau, may send a notice to all providers immediately downstream from the gateway provider in the call path. Upon receipt of such notice, all providers must promptly block all traffic from the identified gateway provider.

(o) A gateway provider must block calls that it reasonably determines, based on reasonable analytics that include consideration of caller ID authentication information where available, that calls are part of a call pattern that is highly likely to be illegal.

(1) The gateway provider must manage this blocking with human oversight and network monitoring sufficient to ensure that it blocks only calls that are highly likely to be illegal, which must include a process that reasonably determines that the particular call pattern is highly likely to be illegal before initiating blocking of calls that are part of that pattern.

(2) The gateway provider ceases blocking calls that are part of the call pattern as soon as the gateway provider has actual knowledge that the blocked calls are likely lawful;

(3) All analytics are applied in a non-discriminatory, competitively neutral manner.

(p) A gateway provider must confirm that the originator of a high volume of foreign-originated calls that use a U.S. North American Numbering Plan number in the caller ID field is authorized to use that number to originate calls.

3. Amend § 64.6300 by redesignating paragraphs (d) through (l) as paragraphs (e) through (m) and adding new paragraph (d) to read as follows:

§ 64.6300 Definitions.

* * * * *

(d) *Gateway Provider.* The term "gateway provider" means 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.

* * * * *

4. Amend § 64.6305 by revising paragraph (a) introductory text, redesignating paragraphs (b) and (c) as paragraphs (c) and (e), respectively, and by adding new paragraphs (b) and (d) to read as follows:

§ 64.6305 Robocall mitigation and certification.

(a) *Robocall mitigation program requirements for voice service providers.*

* * * * *

(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.

(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.

(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:

(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)(2) 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.

(d) *Certification by gateway providers in the Robocall Mitigation Database.*

(1) Not later than March 1, 2023, a gateway provider shall certify that 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(a) and (c);

(2) A gateway provider shall include the following information in its certification:

(i) The specific reasonable steps the gateway provider has taken to avoid carrying or processing illegal robocall traffic as part of its robocall mitigation program; and

(ii) 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 paragraph (d)(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) 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)(2) through (4) of this section, subject to the conditions set forth in paragraphs (c)(5)(i)-(ii) of this section.

(e) *Intermediate provider and voice service provider obligations.*

(1) Beginning September 28, 2021, intermediate providers and voice service providers shall accept calls directly from a voice service provider, including a foreign voice service provider that uses North American Numbering Plan resources that pertain to the United States to send voice traffic to residential or business subscribers in the United States, only if that voice service provider's filing appears in the Robocall Mitigation Database in accordance with paragraph (c) of this section.

(2) *Additional intermediate provider and voice service provider obligations*. Beginning ninety 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.

[FR Doc. 2021-23164 Filed: 10/25/2021 8:45 am; Publication Date: 10/26/2021]