

FCC Proposes New Robocall Mitigation Regulations on Gateway Providers

October 2021

Privacy In Focus®

At the September 30, 2021 Open Meeting, the Federal Communications Commission (FCC or Commission) adopted a Fifth Further Notice of Proposing Rulemaking (FNPRM) that proposes additional regulatory requirements on the gateway providers that are the point of entry for foreign-originated illegal robocalls into the United States. The FNPRM also proposes increased administrative obligations for voice providers registered in the FCC's Robocall Mitigation Database (RMD), to include their filing of additional identifying information. With respect to gateway providers, the FNPRM proposes to require them to apply STIR/SHAKEN caller ID authentication to, and perform robocall mitigation on, foreign-originated calls with U.S. numbers. The FNPRM also proposes and seeks 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, including mandatory blocking mechanisms and a general robocall mitigation standard for gateway providers. Finally, the FNPRM has deferred enforcement of its foreign provider prohibition adopted in the FCC's *Fourth Report and Order*.

The FNPRM provides that comments will be due 30 days following publication of the notice in the Federal Register and that reply comments will be due 60 days following that publication date. As of October 25, the FNPRM has not been published in the Federal Register.

Authors

Kevin G. Rupy
Partner
202.719.4510
krupy@wiley.law
Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

Privacy, Cyber & Data Governance
Telecom, Media & Technology
The Telephone Consumer Protection Act (TCPA)

As the Commission continues its focus on stopping illegal robocalls, it is critical for providers to be aware of the changing regulatory landscape. Below, we outline how the new FNPRM would impact this fast-evolving space – for gateway providers as well as for voice service providers.

The FNPRM Proposes Increased Regulation on Gateway Providers.

The FNPRM proposes a series of additional regulatory obligations for so-called “gateway providers” – which the FCC proposes to define 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.” FNPRM ¶ 33. Most notably, the FNPRM proposes requiring these companies to both apply STIR/SHAKEN caller ID authentication to, and perform robocall mitigation on, all foreign-originated calls with U.S. numbers. FNPRM ¶¶ 38-51. The FNPRM also proposes a series of additional obligations that include:

- Requiring gateway providers to respond to traceback requests within 24 hours;
- Implementing mandatory blocking requirements for both gateway providers and the U.S.-based provider that receives the call from the gateway provider, including requirements based on the Commission’s existing effective mitigation requirement, bad-actor provider blocking safe harbor, and reasonable analytics blocking safe harbor;
- Requiring gateway providers to confirm that a foreign call originator that uses a U.S. telephone number to originate a call is authorized to use that number; and
- Adopting a general mitigation standard for gateway providers.

Requiring Gateway Providers to Respond to Traceback Requests Within 24 Hours.

The FNPRM proposes 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.” FNPRM ¶ 52. The FNPRM notes that this requirement would be “stricter than [the FCC’s] general obligation, which requires that voice service providers (including intermediate providers) respond to traceback requests ‘in a timely manner.’” FNPRM ¶ 52. Although the FNPRM seeks comment on this proposal, the FCC believes it presents a “minimal burden on gateway providers,” since they must already respond in a “timely manner.” FNPRM ¶ 53. The FNPRM proposes 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. FNPRM ¶ 55.

Establishing a Mandatory Blocking Framework.

Although the FNPRM acknowledges that the FCC has “generally taken a permissive approach to call blocking,” it seeks 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. FNPRM ¶ 56. The FNPRM seeks comment on four specific approaches to possible mandatory blocking, as well as other blocking considerations.

- **Gateway Provider Blocking Based on Commission Notification of Illegal Calls.** First, the FNPRM seeks comment on whether to affirmatively require gateway providers to block calls upon receipt of notification from the FCC through its Enforcement Bureau. FNPRM ¶ 57. Specifically, the FCC proposes to require gateway providers, following “a prompt investigation” by the gateway provider to determine whether the traffic identified in the Bureau’s notice is illegal, to “promptly block all traffic associated with the traffic pattern identified in that notice.” Given the heightened risk of foreign-originated illegal robocalls, the FNPRM further asks whether gateway providers should block calls “*prior* to investigation.” FNPRM ¶ 58 (emphasis added). The FNPRM also asks whether gateway providers should be afforded some discretion in blocking the calls. FNPRM ¶ 58.
- **Requiring Downstream Providers to Block Calls from Bad-Actor Gateway Providers.** Next, the FNPRM seeks comment on a complementary approach to require the voice service provider or intermediate provider downstream from the gateway provider to block traffic where the FCC determines a particular gateway provider is a bad actor. FNPRM ¶ 60. The FNPRM states that such an approach could “provide a strong incentive for the gateway provider to avoid having its traffic blocked by ensuring that it complies with our rules.” FNPRM ¶ 60.

Although the FCC’s *Third Call Blocking Order and Further Notice* encouraged – but did not require – such blocking, the FNPRM proposes that, should a gateway provider fail to comply with those requirements, the FCC, through the 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 public safety answering point (PSAP) calls. FNPRM ¶ 60. The FNPRM also seeks 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, and how much time to permit downstream providers to begin blocking calls from the identified gateway provider. FNPRM ¶¶ 62-63.

The FNPRM also seeks comment on how best to notify downstream providers when blocking is required. For example, the FCC asks whether it should directly notify all downstream providers, or work through the industry traceback consortium. FNPRM ¶ 64. Finally, recognizing 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,” the FNPRM seeks comment on whether to adopt additional due process steps or requirements to ensure that any rules “are not erroneously applied to gateway providers.” *Id.* ¶ 65.

- **Blocking by Gateway Providers Based on Reasonable Analytics.** Consistent with the safe harbor established in the *Fourth Call Blocking Order* that permits terminating voice providers to block calls based on reasonable analytics, the FNPRM proposes 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. FNPRM ¶ 66. In the event the FCC adopts such a requirement, the FNPRM also proposes 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 nondiscriminatory, competitively neutral manner. FNPRM ¶ 66.

The FNPRM notes that, unlike terminating voice service provider blocking, consumers will have no recourse for erroneous gateway provider blocking. The FNPRM asks how the FCC should address this potential problem, such as requiring 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. FNPRM ¶¶ 67-68.

- **Gateway Provider Do Not Originate.** The FNPRM also seeks comment on whether to require gateway providers to block some, or all, of the four categories of calls permitted to be blocked by voice providers. Specifically, the FNPRM asks whether gateway providers should be required to block where: 1) the subscriber to the number indicated that that number should never be used to originate calls; 2) the number is unallocated; 3) the number is unused; and/or 4) the number is invalid. FNPRM ¶¶ 71-72. In the event the FCC approves such blocking, it seeks comment on management of any list containing the relevant telephone numbers associated with such blocking. FNPRM ¶ 73.
- **Other Blocking Considerations.** Finally, the FCC seeks comment on alternative mandatory blocking frameworks for gateway providers. Among other things, it seeks comment on associated risks and burdens with such approaches, and the specifics associated with each approach. FNPRM ¶ 74. Acknowledging the risks associated with the blocking of legal calls, the FNPRM also seeks comment on appropriate transparency and redress options that could accompany mandatory blocking requirements for gateway providers, and what transparency and redress requirements the FCC should adopt. FNPRM ¶ 75.

The FNPRM also asks if the FCC adopts mandatory blocking requirements, should it also establish a safe harbor for gateway providers engaged in such blocking. The FNPRM asks whether it should provide a blanket safe harbor under the Act and the Commission's rules for such blocking or limit that protection to actions taken to comply in good faith. It also asks if the FCC establishes a good faith requirement, should the agency define good faith, and, if so, how. FNPRM ¶ 77. Finally, the FCC seeks comment on its proposal 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. FNPRM ¶ 79.

'Know Your Customer' Requirements for Gateway Providers.

The FNPRM also proposes and seeks 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. The FNPRM then seeks 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. FNPRM ¶¶ 80-86.

While acknowledging that there are valid reasons for some U.S. numbers to originate calls internationally, the FNPRM proposes and seeks 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. *Id.*, ¶ 81. Among other things, the FNPRM seeks comment on how a gateway provider can best comply with this requirement, and how it could reliably gather this information prior to calls being placed. If such information is not available until after some calls have been placed, the FNPRM asks whether the FCC should 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. FNPRM ¶ 82.

The FNPRM asks whether the FCC should instead 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.” FNPRM ¶ 84. The FNPRM seeks comment on defining the provider immediately upstream from the gateway provider to be the gateway provider’s “customer,” and, if that definition is adopted, it seeks comment on what the gateway provider should “know” to be able to reasonably claim it “knows” its customer. FNPRM ¶ 84.

As a final alternative, the FNPRM seeks comment on whether the FCC should consider the call originator the gateway provider’s “customer” for purposes of such a requirement. FNPRM ¶ 85. Although the FNPRM acknowledges that in “many cases” the gateway provider “may have no direct relationship with the originator,” it seeks comment on considering the call originator the “customer” for purposes of a know-your-customer requirement. The FCC also seeks comment on what would be sufficient for a gateway provider to reasonably claim that it “knows” this “customer,” and any barriers gateway providers might face in obtaining necessary information from call originators. FNPRM ¶ 85. The FCC proposes 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.

Mandating Contractual Provisions for Gateway Providers.

The FNPRM seeks comment on whether the FCC 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. North American Number Plan (NANP) numbers, and, in some cases, traffic from their foreign-end user customers. FNPRM ¶ 87-88. It seeks comment on what contractual provisions, if any, should be required. For example, the FNPRM asks whether gateway providers should contractually require their foreign partners to 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. FNPRM ¶ 88. The FNPRM also seeks comment on whether the FCC should require gateway providers to ensure that their foreign partners employ know-your-customer practices, or contractually obligate their foreign partners to submit a certification to the RMD. FNPRM ¶ 88. Consistent with the other proposals in the FNPRM, the FCC proposes to require gateway providers to comply with any contractual provisions 30 days after the effective date of an Order adopting such requirements.

Establishing a General Robocall Mitigation Standard for Gateway Providers.

The FNPRM also proposes to require gateway providers to meet a general obligation to mitigate illegal robocalls. FNPRM ¶¶ 91-93. Referencing its similar obligation for providers subject to a robocall mitigation program, the FCC reasoned that “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 its proposal, gateway providers would be required to take reasonable steps to avoid transiting illegal robocall traffic. FNPRM ¶ 91.

In the alternative, the FNPRM seeks comment on whether the FCC should 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.” FNPRM ¶ 92. The FCC seeks comment on an appropriate deadline for any general mitigation standard it adopts. The FCC states its belief that any compliance deadline it adopts 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.” FNPRM ¶ 93.

Requiring Gateway Providers to Register in the Robocall Mitigation Database.

Finally, the FNPRM proposes to require gateway providers to submit a certification to the RMD describing their robocall mitigation practices and stating that they are adhering to those practices. FNPRM ¶¶ 94-102. The FNPRM notes that adoption of the proposal would “situate gateway providers consistently with voice service providers under [the FCC’s] STIR/SHAKEN rules.” FNPRM ¶ 95. Although the FNPRM proposes to require gateway providers to submit certifications and robocall mitigation plans to the RMD, it asks whether it should alter or remove any of these obligations as applied to gateway providers. FNPRM ¶ 96. The FNPRM also proposes to extend the prohibition on accepting traffic from unlisted providers to gateway providers. FNPRM ¶ 98. The FNPRM proposes that the prohibition should go into effect 90 days following the effective date of the requirement for gateway providers to submit a certification to the RMD. FNPRM ¶ 98.

Proposed New RMD Filing Obligations for All Providers.

The FCC seeks comment on whether the FCC should require RMD 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. FNPRM ¶ 100. The FCC believes that requiring some additional identifying information may ease compliance by facilitating searches within the RMD and cross-checking information within the RMD against other sources.

The FNPRM also clarifies that even if a voice service provider (or, if its FNPRM is adopted, a gateway provider) is not listed in the RMD, 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. FNPRM ¶ 101. It also states that calls to 911 must not be blocked, even if originated by a voice service provider not in the RMD or otherwise subject to blocking. FNPRM ¶ 101. The FNPRM seeks comment

on whether the FCC should modify its rules to reflect this clarification. FNPRM ¶ 102.

Deferral on Enforcement of Foreign Provider Prohibition.

Finally, the FNPRM concludes that the public interest will be best served by not enforcing the foreign provider prohibition during the pendency of this proceeding. FNPRM ¶ 106. That prohibition was adopted by the FCC in its *Fourth Report and Order* released in late 2020 and prohibited providers of voice service and intermediate providers from accepting traffic from foreign voice service providers not listed in the RMD. The FNPRM states that the FCC will make a final decision regarding whether to eliminate, retain, or enhance the foreign provider prohibition as part of the agency's larger consideration of how best to address illegal robocalls originating abroad in the order issued pursuant to the 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 RMD. FNPRM ¶ 106.

* * *

The regulatory landscape applicable to voice providers, intermediate providers, and gateway providers is dynamic and changing in response to consumer and congressional pressure. The FCC and Federal Trade Commission (FTC) have been expanding their oversight and broadening regulatory obligations across the private sector, while also bringing enforcement actions. App developers, service providers, analytics engines, and others should heed the FCC's actions and prepare for more.

For more information about the various proceedings and deadlines launched under the Pallone-Thune TRACED Act, or any of the many proceedings in this area, please reach out to a member of our team. We have a deep and experienced robocalling and robotexting bench. Our experts handle federal and state policy issues; compliance with federal and state requirements; complex Telephone Consumer Protection Act (TCPA) issues, including political and charitable outreach; and TCPA enforcement actions and investigations.