

FCC Shifts Regulatory Landscape for Gateway Providers; Proposed Rules Signal Further Changes

June/July 2022

Privacy In Focus®

On May 19, 2022, the Federal Communications Commission (FCC or Commission) adopted a Report and Order, Order on Reconsideration, Order, and Further Notice of Proposed Rulemaking that significantly expands obligations on so-called gateway providers, which are the entry points for foreign calls into the United States, and proposes new rules that could impact a broad range of providers (the “Report and Order,” “Order on Reconsideration,” “Order,” and “FNPRM,” respectively). Collectively, the items adopted by the Commission raise a host of new regulatory obligations for foreign and domestic voice providers, and propose new rules that, if adopted, could vastly change the Commission’s existing robocall regulatory framework.

Summary of the Items

The Report and Order requires gateway providers to play a more active role in the fight against illegal robocalls originating from overseas by, among other things, requiring them to apply STIR/SHAKEN caller-ID to all Session Initiation Protocol (SIP) calls carrying a U.S. number, submit certifications and mitigation plans to the Robocall Mitigation Database (RMD), and institute mandatory blocking in certain instances. Gateway providers will also be subject to a 24-hour response time to traceback requests from the Industry Traceback Group (ITG), a “know your upstream provider” requirement, and a general mitigation duty for illegal robocalls. The Order on Reconsideration requires domestic providers to block calls

Authors

Kevin G. Rupy
Partner
202.719.4510
krupy@wiley.law
Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law
Scott Bouboulis
Associate
202.719.4434
sbouboulis@wiley.law

Practice Areas

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

with U.S. numbers from foreign providers if the latter are not registered in the RMD. Finally, the FNPRM seeks comment on a host of issues, including extending the STIR/SHAKEN authentication requirement to all intermediate providers, extending certain mitigation duties to all domestic providers, and significantly expanding the Commission's enforcement rules, including those related to delisting voice providers from the RMD.

The Report and Order Subjects Gateway Providers to a Host of New Requirements

The Report and Order imposes several new obligations on gateway providers, which are defined as "a U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider." The scope of the FCC's new requirements is limited to foreign-originated calls carrying a U.S. number in the caller ID field.

First, the Report and Order requires gateway providers to submit a certification and mitigation plan to the RMD. Although gateway providers were originally automatically registered in the RMD as intermediate providers, the FCC's new requirement places an affirmative obligation on gateway providers to register and certify. The certification and mitigation plans will work in tandem with new obligations that will prohibit downstream providers from accepting traffic from a gateway provider not listed in the RMD. Gateway providers must submit a certification to the RMD by 30 days following publication in the *Federal Register* of notice of approval by Office of Management and Budget (OMB) of any associated Paperwork Reduction Act (PRA) obligations.

Second, gateway providers must also implement the STIR/SHAKEN framework within their networks and authenticate SIP calls carrying a U.S. number in the caller ID field. Consistent with the FCC's initial order establishing the STIR/SHAKEN framework, gateway providers can satisfy the requirements by adhering to three ATIS standards: ATIS-1000074, ATIS-1000080, and ATIS-1000084. The compliance deadline for this new requirement is June 30, 2023.

Third, gateway providers must respond to traceback requests from the ITG within 24 hours, although the FCC clarified that the 24-hour clock does not start outside of the business hours of the local time for the responding office. The traceback requirement does not require gateway providers to identify the caller or originating provider within 24 hours, unless the originating provider is the provider from which the gateway provider received the call. The compliance deadline is 30 days after publication notice of OMB approval.

Fourth, the FCC created new mandatory blocking requirements for gateway providers. Unlike the FCC's existing, permissive blocking framework, gateway providers will be required to block illegal traffic in two discrete instances: 1) when notified by the Commission of unlawful traffic transiting their networks; and 2) as an ongoing obligation to block calls based on any reasonable do-not originate (DNO) list. Further, providers "immediately downstream" from the gateway provider must block all traffic from the gateway provider if the FCC notifies the downstream providers that such gateway provider did not block illegal traffic upon request by the FCC. Regarding the second blocking category, gateway providers are permitted to use any reasonable

DNO list, which contains a list of numbers that should never be used to originate calls. The FCC declined to mandate the use of a specific list but will permit gateway providers to use any DNO list so long as the list is reasonable. The FCC also declined to adopt a safe harbor for providers that block according to the adopted rules. The FCC will require gateway and downstream providers to comply with the requirements to block upon FCC notification no later than 60 days after publication of the Report and Order in the *Federal Register*. Gateway providers must comply with the DNO blocking requirement no later than 30 days after publication of notice of OMB approval under PRA.

Fifth, gateway providers are required to follow new “know your upstream provider” rules, which require them to “take reasonable and effective steps” to ensure that their upstream foreign provider is not using the gateway provider to process a high volume of illegal traffic. The rules do not mandate any specific steps for this requirement, and the compliance deadline is 180 days after publication in the *Federal Register*.

Finally, gateway providers must follow a general mitigation standard that requires them to take “reasonable steps to avoid carrying or processing illegal robocall traffic.” While no specific steps are mandated by the FCC, gateway providers must “comply with the practices” of their robocall mitigation plans. The compliance deadline is 30 days of the effective date of the Order.

The Order on Reconsideration Lifts the Stay on the Foreign Provider Provision

The FCC now requires that domestic providers only accept calls from a foreign provider if the foreign provider is registered in the RMD. This requirement, which was originally adopted in a 2020 Report and Order, was subject to a stay of enforcement in 2021, and the FCC’s Order on Reconsideration has ended the deferral. Under the now-enforceable rules, domestic providers must block foreign service providers that are not registered in the RMD. The original rule only applied to calls from foreign-originating providers, but the Commission has expanded the rules to include foreign intermediate providers. Enforcement will begin 90 days after the deadline for gateway providers to submit certifications to the Robocall Mitigation Database.

The FNPRM Proposes a Broad Range of Rules That if Adopted Could Impact Broad Industry Segments

The FNPRM considers a broad range of proposed rules, including expanding the gateway provider rules to include all intermediate providers. Among other things, the proposed rules would require *all* intermediate providers to authenticate caller ID information using STIR/SHAKEN, and the FNPRM seeks comment on a six-month implementation deadline. The proposed rules also include the following:

- Expanding the 24-hour traceback requirement to *all* domestic providers (currently limited to gateway providers);
- Requiring all domestic providers in the call path to block, rather than simply effectively mitigate, illegal traffic when notified of such traffic by the FCC, regardless of whether that traffic originates abroad or domestically (currently limited to gateway providers);
- Clarifying through additional guidance the FCC’s existing rule requiring providers to take affirmative, effective measures to prevent new and renewing customers from using a voice provider’s network to

originate illegal calls;

- Requiring intermediate and terminating providers to block traffic from bad-actor providers, regardless of whether or not the bad actor is a gateway provider; and
- Extending a general mitigation standard to voice service providers that have implemented STIR/SHAKEN in the IP portions of their networks and to all intermediate providers.

The FNPRM also seeks comment on requiring all intermediate providers to submit filings to the RMD describing their robocall mitigation practices. The FNPRM also proposes to require voice service providers that have already filed a certification to submit a robocall mitigation plan to the extent they previously were not required to do so due to fully implementing STIR/SHAKEN.

The Commission also proposes a number of new enforcement measures that include:

- Imposing forfeitures for failures to block calls on a per-call basis and establish a maximum forfeiture amount for such violations;
- Imposing the highest available forfeiture for failures to appropriately certify in the RMD;
- Establishing additional bases for removal from the RMD, including by establishing a “red light” feature to notify the FCC when a newly-filed certification lists a known bad actor as a principal, parent company, subsidiary, or affiliate; and
- Subjecting repeat offenders to proceedings to revoke their Section 214 operating authority and to ban offending companies and/or their individual company owners, directors, officers, and principals from future significant association with entities regulated by the Commission.

The Commission also seeks comment on several other issues that if adopted could impact a broad range of providers. These include whether the TRACED Act applies to satellite providers, and if it does, whether such providers should be granted an implementation extension; adopting restrictions on the use of domestic numbering resources for calls that originate outside of the United States for termination in the United States; and whether the FCC should allow a third party to authenticate caller identification information to satisfy the originating provider’s obligation.

In sum, the FCC’s most recent action on illegal robocalls has dramatically changed the agency’s regulatory framework for domestic and foreign providers, and its proposed rules could significantly alter regulatory obligations for a broad range of providers.

© 2022 Wiley Rein LLP