

FCC Significantly Expands Robocall Obligations for Broad Universe of Providers

March 21, 2023

At its March 16, 2023 Open Meeting, the Federal Communications Commission (FCC or Commission) adopted a Sixth Report and Order and Further Notice of Proposed Rulemaking (Order and FNPRM, respectively), which significantly expands robocall regulatory obligations on all providers, including intermediate providers and providers that have fully deployed the STIR/SHAKEN call authentication standard. The Order also establishes new enforcement frameworks, including additional penalties for noncompliance and an expedited removal procedure for facially deficient Robocall Mitigation Database (RMD) filings. The FNPRM seeks targeted comments relating to the deployment of the STIR/SHAKEN call authentication standard. With the Commission's adoption of the Order, several new obligations and filing deadlines for providers throughout the voice ecosystem will become effective in the weeks and months ahead. A brief summary of the key portions of the Order and FNPRM is provided below.

STIR/SHAKEN Deployment Obligations. The Order amends the FCC's rules to require any non-gateway intermediate provider that receives an unauthenticated Session Initiation Protocol (SIP) call directly from an originating provider to authenticate the call. In other words, the first intermediate provider in the path of an unauthenticated SIP call will now be subject to a mandatory requirement to authenticate the call, subject to limited exceptions. The FCC declined to apply the STIR/SHAKEN deployment obligation on all intermediate providers, concluding that such an obligation "could subject intermediate providers to significant costs."

Authors

Kevin G. Rupy
Partner
202.719.4510
krupy@wiley.law
Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law
Stephen J. Conley
Associate
202.719.4572
sconley@wiley.law
Kelly Laughlin
Associate
202.719.4666
klaughlin@wiley.law

Practice Areas

Communications Enforcement & Compliance
Telecom, Media & Technology

The Order states that the authentication requirement would arise only in “limited circumstances,” such as where an originating provider failed to comply with their own authentication obligation or where the call is sent directly to an intermediate provider from the limited subset of originating providers that lack an authentication obligation. The Order states that the first intermediate provider in the call path could completely avoid the obligation if it implements contractual provisions with its upstream originating providers stating that it will only accept authenticated traffic. The Order sets a December 31, 2023 deadline for the new authentication obligations.

“Reasonable Steps” Mitigation Standard Applies to All Providers. The Order requires all non-gateway intermediate providers, as well as voice service providers that have fully implemented STIR/SHAKEN, to meet the same “reasonable steps” general mitigation standard that is currently applied to gateway providers and voice service providers that have not fully implemented STIR/SHAKEN under the FCC’s rules. The Order also requires that voice service providers without the facilities necessary to implement STIR/SHAKEN must mitigate illegal robocalls and meet this same mitigation standard. Providers newly covered by the general mitigation standard must meet it within 60 days following Federal Register publication of the Order, which may take several weeks or even months.

Universal RMD Filing Obligations. The Order expands the obligation to file a robocall mitigation plan along with a certification in the RMD to *all* providers regardless of whether they are required to implement STIR/SHAKEN—including non-gateway intermediate providers and providers without the facilities necessary to implement STIR/SHAKEN—and expands the downstream blocking duty to providers receiving traffic directly from non-gateway intermediate providers not in the RMD. Providers with a new RMD filing obligation must submit the same basic information as providers that had previously been required to file, but all providers must file additional information in certain circumstances, as explained below.

As part of their obligation to “describe with particularity” their robocall mitigation techniques, (1) **voice service providers** must describe how they are meeting their existing obligation to take affirmative, effective measures to prevent new and renewing customers from originating illegal calls; (2) **non-gateway intermediate providers** and voice service providers must, like gateway providers, describe any “know-your-upstream provider” procedures in place designed to mitigate illegal robocalls; and (3) **all providers** must describe any call analytics systems they use to identify and block illegal traffic, including whether they use a third-party vendor or vendors and the name of the vendor(s).

All providers newly obligated to submit a certification to the RMD must also submit the following information: (1) whether it has fully, partially, or not implemented the STIR/SHAKEN authentication framework in the IP portions of its network; (2) the provider’s business name(s) and primary address; (3) other business name(s) in use by the provider; (4) all business names previously used by the provider; (5) whether the provider is a foreign provider; and (6) the name, title, department, business address, telephone number, and email address of one person within the company responsible for addressing robocall mitigation-related issues. The certification must be signed by an officer of the company.

Finally, all providers must also: (1) submit additional information regarding their role(s) in the call chain; (2) assert whether they do not have an obligation to implement STIR/SHAKEN to include more detail regarding the basis of that assertion; (3) certify that they have not been prohibited from filing in the RMD; and (4) state whether they have been subject to a “formal” FCC, law enforcement, or regulatory agency action or investigation within the last two years due to suspected unlawful robocalling or spoofing and provide information concerning such actions or investigations.

Providers newly subject to RMD filing obligations must submit a certification and mitigation plans to the RMD by the later of: (1) 30 days following publication in the Federal Register of notice of approval by the Office of Management and Budget (OMB) of any associated Paperwork Reduction Act (PRA) obligations; or (2) any deadline set by the Wireline Competition Bureau through Public Notice.

Increased Enforcement Frameworks. In addition to expanded regulatory obligations, the FCC also bolstered its robocall enforcement framework. Among other things, the Order adopted per-call forfeiture penalties and established expedited procedures for removal of certain RMD certifications. Highlights of the new enforcement frameworks are briefly summarized below.

- **\$23,727 Per Call Per-Call Forfeiture Penalty.** The Order authorizes a maximum forfeiture amount for each violation of the FCC’s mandatory blocking requirements of \$23,727 per call, which is the maximum forfeiture amount permitted under the FCC’s rules on non-common carriers. Although common carriers may be assessed a maximum forfeiture of \$237,268 for each violation, the FCC concluded that it should not impose a greater penalty on one class of providers than another for purposes of the mandatory blocking requirements. The Order also sets a base forfeiture amount of \$2,500 per call.
- **Required Removal of Intermediate Providers From the RMD.** The Order adopts rules providing for the removal of non-gateway intermediate providers from the RMD with a deficient certification. This would include instances where the non-gateway intermediate provider describes a program that is unreasonable, or if the FCC determines that the provider knowingly or negligently carries or processes illegal robocalls. The Order notes that the FCC’s enforcement action may include removing a certification from the RMD after providing notice to the intermediate provider and an opportunity to cure the filing, requiring the intermediate provider to submit to more specific robocall mitigation requirements, and/or proposing the imposition of a forfeiture.
- **Expedited Removal for Facially Deficient RMD Certifications.** In instances where the Enforcement Bureau determines that a provider’s filing is “facially deficient,” it may remove the provider from the RMD using an expedited two-step procedure, which entails providing notice and an opportunity to cure the deficiency. A certification will be deemed “facially deficient” where the provider fails to submit any information regarding the “specific reasonable steps” it is taking to mitigate illegal robocalls.
- **Consequences for Repeat Offenders of Robocall Rules.** The Order adopted rules enabling the FCC to revoke the section 214 operating authority of entities that engage in continued violations of the agency’s robocall mitigation rules. Non-common carriers are similarly subject to revocation of their authorizations and/or certifications. Under the new framework, the FCC will consider the public interest impact of granting other future FCC authorizations, licenses, or certifications to the entity that was

subject to the revocation, as well as individual company owners, directors, officers, and principals (either individuals or entities) of such entities.

Certain Satellite Providers Exempt From STIR/SHAKEN Obligations. The Order also concludes that satellite providers that do not use North American Numbering Plan Administrator (NANP) numbers to originate calls or only use such numbers to forward calls to non-NANP numbers are not “voice service providers” under the TRACED Act and therefore do not have a STIR/SHAKEN implementation obligation. It provides an indefinite extension from TRACED Act obligations to satellite providers that are small voice service providers and use NANP numbers to originate calls on the basis of a finding of undue hardship. Although small voice service satellite providers received an extension from STIR/SHAKEN implementation under the Order, they must still submit a certification to the RMD pursuant to the FCC’s existing rules and the new obligations adopted in the Order.

FNPRM Seeks Comment on Discrete STIR/SHAKEN Compliance Issues. Finally, the FCC adopted an FNPRM that seeks comment on two discrete issues pertaining to the STIR/SHAKEN call authentication framework.

First, the FNPRM seeks further comment on the use of third-party solutions to authenticate caller ID information and whether any changes should be made to the FCC’s rules to permit, prohibit, or limit their use. Among other things, the FNPRM seeks comment on the types of third-party solutions available to providers, and whether, and under what circumstances, a third party may authenticate calls on behalf of a provider with A- or B-level attestations consistent with the ATIS standards.

To the extent third parties may satisfy the criteria to sign calls with A- or B-level attestations, the FNPRM seeks comment on what information must be shared between originating providers and third parties for those attestation levels to be applied, and whether it implicates any legal or public interest concerns, including those relating to privacy and CPNI. The FNPRM also seeks comment on whether the FCC should amend its rules to explicitly authorize third-party authentication and what, if any, limitations it should place on that authorization to ensure compliance with authentication requirements and the reliability of the STIR/SHAKEN framework.

Second, the FNPRM seeks comment on whether to eliminate the STIR/SHAKEN implementation extension for providers that cannot obtain a service provider code (SPC) token. Given recent changes in access policy making it easier to obtain an SPC token, the FNPRM seeks comment on which, if any, providers are likely to qualify for the extension today, and under what circumstances. The FNPRM also asks if other ways exist for the FCC to account for providers unable to obtain an SPC token, apart from an implementation extension. Comments and reply comments will be due 30 and 60 days, respectively, from date of publication in the Federal Register.

In sum, the FCC’s new obligations under the Order will impact a broad range of domestic entities, including voice service providers, intermediate providers, and gateway providers. Some of these deadlines are fast approaching, and all providers must be prepared to comply with the FCC’s new requirements.

We have a deep and experienced robocalling bench, and our experts handle federal and state policy issues, compliance with federal and state requirements, and complex TCPA issues. For more information about the gateway provider obligations, please contact one of the authors listed on this alert.