

FCC Extends STIR/SHAKEN Obligations to Intermediate Providers and Adopts New Requirements on All Providers

Kristine Laudadio Devine

On March 20, 2023, the FCC adopted a Sixth Report & Order and Sixth Further Notice of Proposed Rulemaking regarding implementation of the STIR/SHAKEN framework. In previous orders, the FCC required voice service providers to implement STIR/SHAKEN in their IP networks as well as requiring originating voice service providers to authenticate and verify caller ID information of calls originating on their networks, and extended the obligation to implement STIR/SHAKEN in IP networks to gateway providers. (Gateway providers are "U.S.-based intermediate providers that receive 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.") In this Report & Order, the FCC has adopted a new, mandatory authentication requirement for the first intermediate provider in the call path and expands robocall mitigation obligations on all providers. It also adopts new enforcement mechanisms and poses a number of questions regarding additional steps it can take to further strengthen the STIR/SHAKEN framework.

Caller ID Authentication Obligations

The FCC has taken the step of extending the obligation to authenticate and verify caller ID information to **the first intermediate (non-gateway) provider in the path of an unauthenticated SIP call**. (Intermediate providers are "any entity that carries or processes traffic that traverses or will traverse the public switched telephone network at any point insofar as that entity neither originates nor terminates that traffic.") These non-gateway intermediate providers must authenticate these calls, regardless of their mandatory obligation respond to traceback requests from the FCC, law enforcement, and the industry traceback consortium. These providers must meet this new authentication obligation by **December 31, 2023**. If any non-gateway intermediate provider is unable to implement STIR/SHAKEN, it may instead agree to only accept authenticated traffic from originating providers.

The new requirement does not impose an obligation on all intermediate providers in the call path, recognizing that a broader mandate might impose costly burdens on providers that are not justified by the incremental benefits. The FCC noted, however, that it may adopt such a requirement in the future.

Non-gateway intermediate providers are only required to implement STIR/SHAKEN according to the standards that were in effect at the time of their authentication obligation—which is, as noted above, December 31, 2023. Intermediate providers are not required to comply with versions of the standards that come into effect after the compliance deadline, but the FCC has delegated authority to the Wireline Competition Bureau to look into ways in which compliance with revised versions of the applicable standards might be accomplished.

Robocall Mitigation and Database Filing Obligations

The FCC has also taken the step of requiring all providers (including intermediate providers and voice providers that are in full compliance with STIR/SHAKEN) to (1) take reasonable steps to mitigate illegal robocalls (2) file certifications of STIR/SHAKEN compliance along with robocall mitigation plans in the RMD, and (3) for non-gateway intermediate providers, refuse to accept traffic from unlisted or delisted providers.

The “reasonable steps” mitigation standard now applies to all providers. The Report and Order does not mandate specific measures for robocall mitigation but notes that a mitigation program will be considered “sufficient if it includes detailed practices that can reasonably be expected to significantly reduce the carrying or processing or origination of illegal robocalls.” Compliance with this standard also requires providers to commit to timely response to all traceback requests (as is already required for intermediate providers). Providers newly subject to this mitigation standard must comply **within 60 days of publication of the Report and Order in the Federal Register**.

In addition to the general mitigation standard, all providers, regardless of whether they are required to implement STIR/SHAKEN, must file a robocall mitigation plan in the RMD, along with a certification in the RMD. Robocall mitigation plans must include the following elements:

- Description of the specific reasonable steps the provider has taken to avoid the origination, carrying, or processing of illegal robocalls.
- For voice service providers, description of how they meet their existing obligation to take affirmative, effective measures to prevent new and renewing customers from originating illegal robocalls.
- For voice service providers and non-gateway intermediate providers, description of how they have complied with the “know your upstream provider” requirements in order to mitigate illegal robocalls.
- For all providers, description of any call analytics used to identify and block illegal robocalls, including whether they use a third-party vendor (and if so, the name of that vendor).
- The “new and renewing customer” and “know your upstream provider” requirements must be supported by description of contractual provisions with end users and upstream providers that are designed to mitigate illegal robocalls.

With respect to certification obligations, in addition to the baseline requirements for certification, providers now must also submit with their certifications the following:

- Information describing their role in the call chain.
- If the provider asserts it is not obligated to implement STIR/SHAKEN, information supporting that assertion.
- A statement that they have not been prohibited from filing in the RMD.
- A statement whether they are subject to an FCC, law enforcement, or regulatory agency investigation or action due to suspected unlawful robocalling or spoofing, and information about any such investigation or action.

Providers newly subject to any of the certification obligations and existing filers that must amend their filings must meet those obligations by the later of (1) **30 days after publication in the Federal Register of OMB approval** or (2) any deadline set by the Wireline Competition Bureau through public notice. The requirement on non-gateway intermediate providers to refuse traffic from unlisted providers will take effect no sooner than 90 days following the deadline for those providers to submit a certification in the RMD.

Additional Obligations

The Report and Order also adopts new findings with respect to satellite providers, concluding that satellite providers that do not use 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 are not required to implement STIR/SHAKEN. It also adopts an indefinite extension on any obligations under the TRACED Act to satellite providers that do use NANP numbers to originate calls but are “small voice service providers” on the basis of undue hardship.

New Enforcement Mechanisms

To strengthen its ability to enforce these rules, the FCC has also adopted several new enforcement mechanisms:

- Adoption of a per-call forfeiture penalty for failure to block traffic as required by the rules, and setting a base forfeiture amount of \$2500 per call and a maximum forfeiture of \$23,727 per call for such violations.
- Requiring the removal of non-gateway intermediate providers from the RMD for rule violations, as is done for other categories of filers.
- Establishing an expedited process for provider removal from the RMD for facially deficient certifications.
- Establishing rules imposing consequences on repeat offenders of the robocall mitigation rules.

Sixth Further Notice of Proposed Rulemaking

The Sixth NPRM continues exploring issues related to the use of third-party authentication by providers required to implement STIR/SHAKEN, first by acknowledging that third-party authentication is occurring while noting that the record does not contain sufficient information to determine its impact on the STIR/SHAKEN ecosystem. The FCC therefore seeks additional comment on the use of third-party authentication and whether the FCC should adopt new rules permitting, prohibiting, or limiting its use.

The Sixth FNPRM also asks whether it should eliminate its current extension of time to implement STIR/SHAKEN for those providers that are unable to obtain an SPC token.

* * * *

For more information on our call authentication and STIR/SHAKEN compliance, please contact [Kristine Laudadio Devine](#).

This advisory is not meant to convey legal advice. It is circulated publicly as a convenience and does not reflect or create an attorney-client relationship.