wiley

ALERT

FCC Rulemaking Targets the Non-IP Caller ID Authentication Gap

May 1, 2025

In a move designed to close a gap in its robocall mitigation efforts, the Federal Communications Commission (FCC or Commission) adopted a Notice of Proposed Rulemaking (NPRM) at its April 29 Open Meeting that seeks comment on proposals to require call authentication on non-Internet Protocol (IP) networks. The NPRM proposes to repeal the caller ID authentication exemption for non-IP networks and to modify the FCC's rule interpreting the Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act's "reasonable measures" requirement by interpreting that to mean that providers must "either upgrade their networks to IP or implement non-IP caller ID authentication frameworks." Comments and reply comments will be due 30 and 60 days after Federal Register publication, respectively.

Specifically, the NPRM proposes to:

- Adopt criteria for determining whether effective non-IP caller identification frameworks exist;
- Find that certain authentication frameworks satisfy these criteria;
- Create a streamlined authentication approval process;
- Make targeted revisions to certain of its rules to implement non-IP caller ID authentication; and
- Implement a two-year timeline for providers that continue to maintain non-IP infrastructure to "either complete their IP transitions or fully implement one or more of the available non-IP caller ID authentication frameworks in their non-IP networks."

Authors

Kevin G. Rupy
Partner
202.719.4510
krupy@wiley.law

Kelly Laughlin
Associate
202.719.4666
klaughlin@wiley.law

Practice Areas

Telecom, Media & Technology

The Telephone Consumer Protection Act (TCPA)

Overview of the ATIS Non-IP Standards

The NPRM seeks comment on three non-IP caller ID authentication standards published by the Alliance for Telecommunication Industry Solutions (ATIS): ATIS-1000095.v002, *Extending STIR/SHAKEN over TDM* ("In-Band Authentication"); ATIS-1000096, *Out-of-Band PASSporT Transmission Involving TDM Networks* ("Out-of-Band Multiple STI-CPS Authentication"); and ATIS-1000105, *Out-of-Band PASSporT Transmission Involving TDM Networks* ("Out-of-Band Agreed STI-CPS Authentication").

- ***In-Band Authentication*** allows providers to transmit some of the same information as STIR/SHAKEN, including PASSporTs, with the call over the non-IP portions of the phone network. The standard enables directly connected providers that exchange calls to share "information about what it knows about the caller and its right to use the phone number along with the call." The standard relies on bilateral agreements being in place between every directly connected provider using the standard at each non-IP network-to-network interface (NNI) in a call path.
- ***Out-of-Band Multiple STI-CPS Authentication*** allows providers to send the same information about a call as STIR/SHAKEN "on a separate track that is sent in tandem to the non-IP call signaling." When a provider originates a call, it "publishes" STIR/SHAKEN call information, including PASSporTs to a Secure Telephone Identity Call Placement Service (STI-CPS), which is hosted on the internet. The next provider in the call path then "retrieves" the published information from an STI-CPS. The Out-of-Band Multiple STI-CPS Authentication standard would involve more than one STI-CPS, each sharing information with one another, enabling a terminating provider to retrieve call information from an STI-CPS other than the one to which the information was originally published.
- ***Out-of-Band Agreed STI-CPS Authentication*** allows publication and retrieval of some STIR/SHAKEN call information, including PASSporTs, out-of-band through an STI-CPS – like Out-of-Band Multiple STI-CPS Authentication. However, the solution would require *all* directly connected providers across each non-IP NNI in the call path to agree on the specific STI-CPS to be used for publishing and retrieving call information. Additionally, unlike the two other non-IP standards, *all* providers that interconnect with non-IP portions of the call path must utilize Out-of-Band Agreed STI-CPS Authentication for the call information to be received intact by the terminating provider.

NPRM Proposes "Reasonable Measures" Definition

The NPRM explains that the TRACED Act mandates that providers take "reasonable measures" to implement an effective call authentication framework in their non-IP networks and the Commission therefore proposes that the available non-IP authentication frameworks meet the TRACED Act requirements. The Commission's NPRM proposes to mandate that voice service providers, gateway providers, and non-gateway intermediate providers receiving calls directly from an originating provider implement one or more non-IP caller ID authentication frameworks in their non-IP networks.

If the NPRM's proposals are adopted, the Commission would repeal the continuing extension from caller ID authentication requirements granted to providers that rely on non-IP technology and modify its rule interpreting the TRACED Act's "reasonable measures" requirement to mandate that providers either upgrade their networks to IP or implement non-IP caller ID authentication frameworks.

NPRM Proposes Criteria for Determining Whether Effective Non-IP Caller ID Authentication Exists

The TRACED Act requires the Commission to provide a continuing extension from implementing non-IP caller ID authentication for providers materially reliant on non-IP networks until a call authentication protocol has been "developed for calls delivered over non-[IP] networks" and is also "reasonably available." The NPRM proposes to establish criteria, "based on the plain meaning" in the TRACED Act, for evaluating whether a given non-IP caller ID authentication framework meets these two requirements.

The FCC proposes to define "developed" and "available" using dictionary definitions and proposes to retain the two criteria established in the Second Caller ID Authentication Report and Order for evaluating whether a non-IP caller ID authentication framework satisfies the TRACED Act. In that item, the FCC determined that a framework must be (1) "fully developed and finalized by industry standards," and (2) reasonably available such that "the underlying equipment and software necessary to implement such protocol is available on the commercial market." And the NPRM proposes to consider the framework's implementation readiness and providers' ability to implement the framework. Among other things, the NPRM also proposes to consider the extent to which industry was involved in the development and approval of the framework, whether the framework is undergoing further development, and evidence that the framework is currently being marketed.

The Commission concludes that both In-Band Authentication and Out-of-Band Multiple STI-CPS Authentication meet the TRACED Act's requirement to be effective, and seeks comment on whether the newest standard (Out-of-Band Agreed STI-CPS Authentication) also meets the requirement. Although the Out-of-Band Agreed STI-CPS Authentication standard is developed, the Commission seeks comment on whether it is "reasonably available." Finally, the Commission also seeks comment on whether there are any other non-IP frameworks that it should consider, including any potential proprietary solutions.

NPRM Seeks Comment on Additional Frameworks for Non-IP Call Authentication

In addition to evaluating the three specific non-IP caller ID authentication frameworks, the NPRM also seeks comment about the following:

- ***Establishment of a Streamlined Evaluation Process.*** The Commission proposes to create a streamlined process to determine whether other non-IP caller ID authentication frameworks are "effective." This would involve delegating authority to the Wireline Competition Bureau to seek comment on possible new frameworks, evaluate the framework under the established criteria, and make final determinations about a framework's effectiveness.
- ***Repeal of Continuing Extensions for Certain Voice Service Providers.*** The NPRM asks whether to repeal the continuing extension from robocall mitigation obligations granted to providers that rely on non-IP technology. While the Commission proposes to delete the rules that pertain to extensions for small voice service providers (i.e., less than 100,000 subscribers), the Commission would retain the extension for small voice service providers that originate calls via satellite using North American

Numbering Plan numbers.

- ***Modification of "Reasonable Measures" Rule.*** The Commission seeks comment on modifying its rules to mandate that providers either upgrade their networks to IP or implement one or more non-IP caller ID authentication frameworks. The Commission proposes to add a rule stating that intermediate providers, including gateway providers, must pass any non-IP caller ID authentication information they receive, unaltered, to the subsequent provider in the call path, except where the intermediate provider reasonably believes the non-IP caller ID authentication information presents an imminent threat to its network security. The Commission also asks about the costs and benefits of requiring providers to either complete their IP transitions or implement a non-IP caller ID authentication framework, including whether removing the "reasonable measures" rule would disincentivize providers from participating in efforts to develop other non-IP caller ID authentication solutions.
- ***Conforming Robocall Mitigation Database Rules.*** The Commission proposes a new requirement for providers to certify in the Robocall Mitigation Database whether they have implemented a non-IP caller ID authentication framework in their non-IP networks.
- ***Establishment of Two-Year Compliance Deadline.*** The Commission proposes a two-year timeline for providers that continue to maintain non-IP infrastructure to either complete their IP transitions or fully implement one or more of the available non-IP caller ID authentication frameworks in their non-IP networks. The NPRM specifically asks how any remaining technical, financial, or other obstacles may affect the time needed to implement any of the discussed non-IP caller ID authentication frameworks.

***

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 or assistance with responding to the new NPRM, please contact one of the authors listed on this alert.