3060-1285
September 2022

Compliance with the Non-IP Call Authentication Solution Rules;
Robocall Mitigation Database (RMD)

SUPPORTING STATEMENT

This revised information collection is being submitted to obtain approval from the Office of Management and Budget (OMB) for new and revised information collection requirements due to a recent Federal Communications Commission (Commission or FCC) Order, as explained below. There is a change in the title of this information collection from Compliance with the Non-IP Call Authentication Solution Rules; Robocall Mitigation Database; Certification to Verify Exemption from Caller ID Authentication Implementation Mandate to Compliance with the Non-IP Call Authentication Solution Rules; Robocall Mitigation Database (RMD) to reflect that one of the original requirements of this collection has been fulfilled and the burden associated with that requirement is no longer part of this collection.

A. Justification

1. *Circumstances that make the collection necessary*. On December 30, 2019, Congress enacted the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act. The TRACED Act directs the Commission to require, no later than 18 months from enactment, all voice service providers to implement STIR/SHAKEN in the IP portions of their networks and implement an effective caller ID authentication framework in the non-IP portions of their networks. Among other provisions, the TRACED Act also directs the Commission to create extension and exemption mechanisms for voice service providers. To implement the TRACED Act's provisions related to call authentication, the Commission adopted a Report and Order and Further Notice of Proposed Rulemaking on March 30, 2020 and a Second Report and Order on September 29, 2020. *See Call Authentication Trust Anchor*, *Implementation of TRACED Act Section 6(a)—Knowledge of Customers by Entities with Access to Numbering Resources*, WC Docket Nos. 17-97 and 20-67, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3241 (Mar. 31, 2020) (*Report and Order and Further Notice*); *Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, 36 FCC Rcd 1859 (Sept. 30, 2020) (*Second Report and Order*).

   The Commission subsequently proposed and sought comment on imposing similar and additional obligations on gateway providers on September 30, 2021 and adopted many of these proposed obligations on May 19, 2022. *See Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Fifth Further Notice of Proposed Rulemaking *et al*., FCC 21-105 (adopted Oct. 1, 2021) (*Fifth Further Notice et al*.); *Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Sixth Report and Order *et al*., FCC 22-27 (adopted May 19, 2022) (*Sixth Report and Order et al*.).

   Section 4(b)(1)(B) of the TRACED Act directs the Commission to require that providers of voice service, no later than June 30, 2021, take reasonable measures to implement an effective caller ID authentication framework in the non-IP portions of their networks. In the *Second Report and Order*, adopting the proposal from the March *Further Notice*, the Commission interpreted this language to require that a voice service provider be actively working to implement a caller ID authentication framework on the non-IP portions of its network, either by (1) upgrading its non-IP networks to IP so that the STIR/SHAKEN authentication framework may be implemented, or (2) by working to develop a non-IP authentication solution. Furthermore, the Commission adopted the proposal from the March *Further Notice* that to satisfy this latter option, a voice service provider would have to, upon request, provide the Commission documented proof that it is participating, either on its own or

through a representative, as a member of a working group or consortium that is working to develop a non-IP solution, or actively testing such a solution.

Section 4(b)(2) of the TRACED Act requires the Commission to free a voice service provider from the obligation to implement STIR/SHAKEN on the IP portions of its network and an effective call authentication system on the non-IP portions its network if the Commission determines, by December 30, 2020, that the provider: (A) in its IP networks (i) "has adopted the STIR/SHAKEN authentication framework for calls on the [IP] networks of the provider of voice service; (ii) has agreed voluntarily to participate with other providers of voice service in the STIR/SHAKEN authentication framework; (iii) has begun to implement the STIR/SHAKEN authentication framework; and (iv) will be capable of fully implementing the STIR/SHAKEN authentication framework not later than [June 30, 2021]"; and (B) in its non-IP networks (i) "has taken reasonable measures to implement an effective call authentication framework; and (ii) will be capable of fully implementing an effective call authentication framework not later than [June 30, 2021]." The *Second Report and Order* implemented section 4(b)(2) of the TRACED Act by establishing two exemptions: one exemption for a voice service provider's IP networks if it meets all four statutory criteria for all calls it originates or terminates in Session Internet Protocol (SIP), and one exemption for a voice service provider's non-IP networks if it meets both statutory criteria for all non-SIP calls it originates or terminates.

Section 4(b)(5) of the TRACED Act requires the Commission to provide extensions of the June 30, 2021 implementation deadline to certain categories of providers. In the *Second Report and Order*, the Commission provided: (1) a two-year extension to small, including small rural, voice service providers; (2) an extension to voice service providers that cannot obtain a certificate due to the Governance Authority's token access policy until such provider is able to obtain a certificate; (3) a one-year extension to services scheduled for section 214 discontinuance; and (4) an extension for the parts of a voice service provider's network that rely on technology that cannot initiate, maintain, and terminate SIP calls until a solution for such calls is reasonably available. As required by section 4(b)(5)(C)(i) of the TRACED Act, the Commission further adopted rules that require those voice service providers that receive an extension to implement a robocall mitigation program to protect their customers on the parts of their networks not subject to protection from STIR/SHAKEN.

The *Second Report and Order* also established the certification process that the Commission proposed in the March *Further Notice* as necessary to permit the Commission to meet the TRACED Act's statutory deadline. Because the section 4(b)(2)(A) and (B) exemptions are based on a voice service provider's prediction of its future ability to meet the June 30, 2021 implementation deadline, the *Second Report and Order* adopted the proposal from the March *Further Notice* that applicable voice service providers be required to file a second certification after June 30, 2021, to verify that they met the criteria to receive their exemption. Because these certification requirements have been fulfilled, the burden associated with these requirements is no longer part of this information collection.

In order to promote transparency, in the *Second Report and Order*, the Commission required that all voice service providers file certifications with the Commission in the Robocall Mitigation Database (RMD), stating that: (i) the voice service provider has fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it originates are compliant with 47 CFR 64.6301(a)(1)-(2); (ii) the voice service provider has implemented the STIR/SHAKEN authentication framework on a portion of its network and calls it originates on that portion are compliant with paragraphs 47 CFR 64.6301(a)(1)-(2), and the remainder of the calls that originate on its network are subject to a robocall mitigation program; or (iii) the voice provider has not implemented the STIR/SHAKEN authentication framework on any portion of its network, and all of the calls that originate on its network are subject to a robocall mitigation program. Pursuant to the

rules adopted in the *Second Report and Order*, each voice service provider must also include in its filing: (i) the voice service provider's business name(s) and primary address; (ii) other business names in use by the voice service provider; (iii) all business names previously used by the voice service provider; (iv) whether the voice service provider is a foreign voice service provider; and (v) the name, title, department, business address, telephone number, and email address of one person within the company responsible for addressing robocall mitigation-related issues. Voice service providers are required to update any of the data in the RMD within 10 business days of any change to the information filed. The certification must be signed by an officer of the voice service provider. The Commission subsequently clarified that voice service providers were required to submit all information in English or with a certified English translation. (OMB approved the non-substantive change request to the collection associated with this requirement on June 2, 2022, ICR 202205-3060-018.)

The *Second Report and Order* further required that any voice service provider certifying all or part of its network is covered by a robocall mitigation program, include in its certification: (i) identification of the type of extension or extensions the voice service provider received under 47 CFR 64.6304, if the voice service provider is not a foreign voice service provider; (ii) the specific reasonable steps the voice service provider has taken to avoid originating illegal robocall traffic as part of its robocall mitigation program; and (iii) a statement of the voice service provider's commitment to respond fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

The *Sixth Report and Order et al.,* adopts many of the proposals in the *Fifth Further Notice et al*. to extend many of the foregoing voice service provider obligations to gateway providers and, in some cases, to impose additional requirements on gateway providers. The *Sixth Report and Order et al*. defines a gateway provider 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.

Like the existing requirements for voice service providers, the *Sixth Report and Order et al*. requires gateway providers to be actively working to implement a caller ID authentication framework on the non-IP portions of their networks, either by (1) upgrading their non-IP networks to IP so that the STIR/SHAKEN authentication framework may be implemented, or (2) by working to develop a non-IP authentication solution. Furthermore, to satisfy this latter option, a gateway provider would have to, upon request, provide the Commission documented proof that it is participating, either on its own or through a representative, as a member of a working group or consortium that is working to develop a non-IP solution, or actively testing such a solution.

A gateway provider is required to authenticate all unauthenticated calls it receives and will exchange with another provider as a SIP call. A gateway provider must do so by June 30, 2023 unless it is subject to one of the following conditional extensions: (1) for gateway providers that cannot obtain a certificate due to the Governance Authority's token access policy, until such provider is able to obtain a certificate; or (2) for the parts of a gateway provider's network that rely on non-IP technology and that cannot authenticate calls, until a solution for authenticating such calls is reasonably available.

In order to promote transparency, in the *Sixth Report and Order et al.*, the Commission requires that all gateway providers file a certification with the Commission stating that: (i) the gateway provider has fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it processes and carries are compliant with 47 CFR 64.6301(a)(1)-(2); (ii) the gateway provider has implemented the STIR/SHAKEN authentication framework on a portion of its network and calls

it processes and carries on that portion are compliant with paragraphs 47 CFR 64.6301(a)(1)-(2); or (iii) the gateway provider has not implemented the STIR/SHAKEN authentication framework on any portion of its network. The gateway provider must also certify that all calls that it processes and carries are subject to a robocall mitigation program. Each gateway provider must also include in its certification: (i) the gateway provider's business name(s) and primary address; (ii) other business names in use by the gateway provider; (iii) all business names previously used by the gateway provider; (iv) whether the gateway provider or any affiliate is also a foreign voice service provider; and (v) the name, title, department, business address, telephone number, and email address of one person within the company responsible for addressing robocall mitigation-related issues. Gateway providers are also required to update any data submitted to the RMD within 10 business days of any change to the information filed. Certifications must be filed in English or with a certified English translation and signed by an officer of the gateway provider.

The *Sixth Report and Order et al.* further requires gateway providers to include in their certifications: (i) identification of the type of extension or extensions the gateway provider received under 47 CFR 64.6304; (ii) the specific reasonable steps the gateway provider has taken to avoid carrying or processing illegal robocall traffic as part of its robocall mitigation program, including how it is complying with the newly-adopted "know-your-upstream provider" requirement; and (iii) a statement of the gateway provider's commitment to respond fully and in a timely manner to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls.

The *Sixth Report and Order et al*. delegates to the Wireline Competition Bureau the form and format of gateway provider submissions to the RMD, including whether gateway providers that are also voice service providers must file a separate certification as a gateway provider or amend their current voice service provider certification. Two separate certifications will have a greater combined burden than an initial voice service provider certification following by an amendment specific to its gateway provider operations. We assume gateway providers that are also voice service providers will make separate certifications for the purpose of the burden estimates below.

New requirements for which we are seeking OMB approval:

There are two new information collection requirements created under the newly adopted rules of the *Sixth Report and Order et al.*[1]

First, in order to comply with the requirement that a gateway provider has taken reasonable steps to implement an effective call authentication system in the non-IP portions of its network by June 30, 2023, it must either upgrade its network to IP or maintain and be ready to provide the Commission upon request with documented proof that it is participating, either on its own or through a representative, including third party representatives, as a member of a working group, industry standards group, or consortium that is working to develop a non-Internet Protocol caller identification authentication solution, or actively testing such a solution.

Second, to promote transparency in the robocall mitigation programs, gateway providers are required to submit a certification to the RMD. The Commission will modify the RMD to tailor the system to accept their filings. The certification will indicate the gateway provider's STIR/SHAKEN

[1] Other requirements adopted in the *Sixth Report and Order et al.* do not include information collections or are part of other information collections for which the Commission will request separate approval.

implementation status, describe its robocall mitigation program, and include other information described above.

Statutory authority for this information collection is contained in 47 U.S.C. §§ 227b, 251(e), and 227(e) of the Communications Act of 1934.

This information collection does not affect individuals or households; thus; there is no impact under the Privacy Act.

2. *Use of information*. The Commission will use the information to determine which voice service providers and gateway providers: (1) satisfy the requirement that they take reasonable measures to implement an effective call authentication system in the non-IP portions of their networks; and (2) comply with the requirements of the Robocall Mitigation Database.

3. *Technology collection techniques*. First, regarding a request under section 64.6303(a) and (b) for a provider to submit to the Commission documented proof that it is participating, either on its own or through a representative, including third party representatives, as a member of a working group, industry standards group, or consortium that is working to develop a non-Internet Protocol caller identification authentication solution, the applicable provider will respond to the Commission in the method specified in the Commission's request. Second, all submissions to the Robocall Mitigation Database under section 64.6305(c) and (d) will be made electronically into a database set up specifically for this purpose.

4. *Efforts to identify duplication*. For each of these two requirements, the information to be collected is unique to each provider, and there are no similar collection requirements.

5. *Impact on small entities*. The Commission worked to minimize the amount of information each certification will require.

6. *Consequences if information is not collected*. If this information is not collected from voice service providers, the Commission will be unable to meet its statutory obligations under the TRACED Act and will be unable to implement its rules and protections meant to stop illegal robocalls. If the information is not collected from gateway providers, significant foreign sources of illegal robocalls will continue to be able to reach and harm U.S. consumers.

7. *Special circumstances*. We do not foresee any special circumstances with this information collection.

8. *Federal Register notice; efforts to consult with persons outside the Commission*. A 60-day notice was published in the Federal Register as required by 5 CFR 1320.8(d) on June 28, 2022 (87 FR 38401). The Commission did not receive any comments as a result of this notice.

9. *Payments or gifts to respondents*. The Commission does not anticipate providing any payment or gifts to respondents.

10. *Assurances of confidentiality.* The Commission will consider the potential confidentiality of any information submitted, particularly where public release of such information could raise security concerns (e.g., granular location information). Respondents may request materials or information submitted to the Commission or to the Administrator be withheld from public inspection under 47 C.F.R. § 0.459 of the Commission's rules.

11. *Questions of a sensitive nature.* There are no questions of a sensitive nature with respect to the information collection described herein.

12. *Estimates of the hour burden of the collection to respondents.* The following represents the hour burden on the collection of information[2]:

(a) Compliance with requirement under section 64.6303(a) that a voice service provider have documented proof that it is working towards a solution for non-IP caller ID authentication

(1) Number of Respondents: Approximately 2,379 voice service providers.

(2) Frequency of Response: Upon request by the Commission.

(3) Total number of responses per respondent: 1.

(4) Estimated time per response: 30 minutes (0.5 hours).

(5) Total hour burden: 1,190 hours.

0.5 hours per response for per respondent for 2,379 voice service providers. Total annual hour burden is calculated as follows:

1,634 respondents x 1 response per respondent = 2,379 responses x 0.5 hours = **1,190 total hours.**

(6) Total estimate of in-house cost to respondents: $69,032 (1,190 hours x $58.01/hr.).

(7) Explanation of calculation: We estimate that each voice service provider will take, on average, 0.5 hours per response. We estimate that respondents use mid- to senior-level personnel to comply with the requirements comparable in pay to the Federal Government, approximately $58.01 per hour (equivalent to a GS-13, step 5 federal employee).

2,379 (number of responses) x 0.5 (hours to prepare response) x 1 (responses per respondent) x $58.01/hr. = $69,032

(b) Compliance with requirement under section 64.6303(b) that a gateway provider have documented proof that it is working towards a solution for non-IP caller ID authentication

(1) Number of Respondents: Approximately 184 gateway providers

(2) Frequency of Response: Upon request by the Commission.

(3) Total number of responses per respondent: 1.

(4) Estimated time per response: 30 minutes (0.5 hours).

[2] As noted above, because the exemption certification requirements have been fulfilled, the burden associated with these requirements is no longer part of this information collection

(5) Total hour burden: 92 hours.

0.5 hours per response for per respondent for 184 gateway providers. Total annual hour burden is calculated as follows:

184 respondents x 1 response per respondent = 184 responses x 0.5 hours = **92 total hours.**

(6) Total estimate of in-house cost to respondents: $5,337 (92 hours x $58.01/hr.).

(7) Explanation of calculation: We estimate that each voice service provider will take, on average, 0.5 hours per response. We estimate that respondents use mid- to senior-level personnel to comply with the requirements comparable in pay to the Federal Government, approximately $58.01 per hour (equivalent to a GS-13, step 5 federal employee).

184 (number of responses) x 0.5 (hours to prepare response) x 1 (responses per respondent) x $58.01. = $5,337

(c) Voice Service Provider Robocall Mitigation Database requirement under section 64.6305(c)

(1) Number of Respondents: Approximately 5,947 voice service providers.

(2) Frequency of Response: One-time reporting requirement, and on the occasion that information in the robocall mitigation database is updated.

(3) Total number of responses per respondent: 1.

(4) Estimated time per response: 3 hours.

(5) Total hour burden: 17,841 hours.

3 hours per response for 1 response per respondent for 5,947 voice service providers. Total annual hour burden is calculated as follows:

5,947 respondents x 1 response per respondent = 5,947 responses x 3 hours = **17,841 total hours.**

(6) Total estimate of in-house cost to respondents: $1,034,956 (17,841 hours x $58.01/hr.).

(7) Explanation of calculation: We estimate that each voice service provider will take, on average, 3 hours per response. We estimate that respondents use mid- to senior-level personnel to comply with the requirements comparable in pay to the Federal Government, approximately $58.01 per hour (equivalent to a GS-13, step 5 federal employee).

5,947 (number of responses) x 3 (hours to prepare response) x 1 (responses per respondent) x $58.01/hr. = $1,034,956

(d) Gateway Provider Service Provider Robocall Mitigation Database requirement under section 64.6305(d)

(1) Number of Respondents: Approximately 460 gateway providers.

(2) Frequency of Response: One-time reporting requirement, and on the occasion that information in the robocall mitigation database is updated.

(3) Total number of responses per respondent: 1.

(4) Estimated time per response: 3 hours.

(5) Total hour burden: 1,380 hours.

3 hours per response for 1 response per respondent for 460 gateway providers. Total annual hour burden is calculated as follows:

460 respondents x 1 response per respondent = 460 responses x 3 hours = **1,380 total hours.**

(6) Total estimate of in-house cost to respondents: $80,054 (1,380 hours x $58.01/hr.).

(7) Explanation of calculation: We estimate that each voice service provider will take, on average, 3 hours per response. We estimate that respondents use mid- to senior-level personnel to comply with the requirements comparable in pay to the Federal Government, approximately $58.01 per hour (equivalent to a GS-13, step 5 federal employee).

460 (number of responses) x 3 (hours to prepare response) x 1 (responses per respondent) x $58.01 = $80,054

Total Number of Respondents: 2,379 + 184 + 5,947 + 460 = 8,970 unique respondents

Total Number of Responses: 2,379 + 184 + 5,947 + 460 = 8,970 responses

Total Hourly Burden: 1,190 + 92 + + 17,841 + 1,380 = 20,503 burden hours

Total In-House Costs to Respondents: $ 1,189,379

13. *Estimates for the cost burden of the collection to respondents*. The Commission believes that voice service providers and gateway providers have sufficient "in-house" staff to address all the information collection requirements using their "in-house" personnel rather than having to contract out this requirement. Thus:

    (a) Total annualized capital/startup costs: $0.00
    (b) Total annualized costs (O&M): $0.00
    (c) Total annualized cost requested: $0.00

14. *Estimates of the cost burden to the Commission.*

(a) Compliance with requirement under section 64.6303(b) that a voice service provider have documented proof that it is working towards a solution for non-IP caller ID authentication

Costs to the Commission will potentially be $58.01/hr (GS-13, step 5 federal employee) x .5 hrs (to request documented proof from voice service providers) x 2,379 voice service providers = $69,003.

(b) Compliance with requirement under section 64.6303(b) that a gateway provider have documented proof that it is working towards a solution for non-IP caller ID authentication

Costs to the Commission will potentially be $58.01/hr (GS-13, step 5 federal employee) x .5 hrs (to request documented proof from voice service providers) x 184 gateway providers = $5,337

(c) Voice Service Provider Robocall Mitigation Database requirement under section 64.6305(c)

The cost to the Commission estimated to be $58.01/hr (GS-13, step 5 federal employee) x 480 hrs (to stand up the Robocall Mitigation Database) x 3 employees = $83,534

(d) Gateway Provider Service Provider Robocall Mitigation Database requirement under section 64.6305(d)

Cost to the Commission estimated to be $58.01 (GS-13, step 5 federal employee) x 240 hrs (to modify Robocall Mitigation Database to account for new gateway provider filings) x 3 employees = $41,767

Total Cost to the Federal Government: $69,003 + $5,337 + $83,534 + $41,767 = $199,641

15. *Program changes or adjustments*. The Commission is reporting program changes/increases to this revised information collection. These increases to the total number of respondents of +2,435, total annual responses of +2,435 and total annual burden hours of +4,983 will be added to OMB's Active Inventory.

16. *Collections of information whose results will be published.* The filings that gateway providers and voice service providers submit into the Robocall Mitigation Database will be published to the public on that database. At this time, the Commission does not plan to publish to the public a voice service provider's response or a gateway provider's response to a request for documented proof that they are taking reasonable measures to implement a non-IP caller ID authentication solution.

17. *Display of expiration date for OMB approval of information collection.* There is no paper form associated with this information collection; it will be collected electronically through the Electronic Comment Filing System (ECFS), the Robocall Mitigation Database, or another electronic method. The Commission publishes a list of all OMB-approved information collections including their titles, OMB Control Numbers and OMB expiration dates in 47 CFR 0.408 of the Commission's rules.

18. *Exceptions to certification for Paperwork Reduction Act submissions*. There are no exceptions to the Certification Statement.

B. Collections of Information Employing Statistical Methods:

No statistical methods are employed.