



Federal Communications Commission
Washington, D.C. 20554

January 05, 2024

DA 24-18

SMALL ENTITY COMPLIANCE GUIDE

**The Commission's Rules Regarding Caller ID Authentication,
Call Blocking, and Appeals of the STIR/SHAKEN Governance Authority Token
Revocation Decisions**

FCC 23-18; WC Docket No. 17-97; Adopted March 16, 2023
FCC 22-37; WC Docket No. 17-97 & CG Docket No. 17-59; Adopted May 19, 2022
FCC 21-122; WC Docket No. 17-97; Adopted December 9, 2021
FCC 21-93; WC Docket Nos. 17-97 & 21-291; Adopted August 5, 2021

In accordance with Section 212 of the Small Business Regulatory Enforcement Fairness Act of 1996, this Small Entity Compliance Guide (Guide) is intended to help small entities—small businesses, small organizations (non-profits), and small governmental jurisdictions—comply with the rules adopted in the above-referenced Federal Communications Commission (FCC or Commission) rulemaking dockets. This Guide is not intended to replace or supersede these rules, but to facilitate compliance with the rules. Although we have attempted to cover all parts of the rules that might be especially important to small entities, the coverage may not be exhaustive. This Guide cannot anticipate all situations in which the rules apply. Furthermore, the Commission retains the discretion to adopt case-by-case approaches, where appropriate, that may differ from this Guide. Any decision regarding a particular small entity will be based on the statute and any relevant rules.

In any civil or administrative action against a small entity for a violation of rules, the content of the Guide may be considered as evidence of the reasonableness or appropriateness of proposed fines, penalties, or damages. Interested parties are free to file comments regarding this Guide in the above-referenced proceeding and the appropriateness of its application to a particular situation. The Commission will then consider whether the recommendations or interpretations in the Guide are appropriate in that situation. The Commission may decide to revise this Guide without public notice to reflect changes in its approach to implementing a rule or it may clarify or update the text of the Guide. Direct your comments, recommendations, or request for further assistance to the FCC's Consumer Center:

1-888-CALL-FCC (1-888-225-5322);
Videophone: 1-844-4-FCC-ASL (1-844-432-2275)
Fax: 1-866-418-0232

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	OBJECTIVES OF THE MARCH 2023 PROCEEDING	1
III.	BACKGROUND	1
IV.	COMPLIANCE REQUIREMENTS.....	2
A.	Definitions.....	2
B.	Traceback Request Responses by Gateway Providers.....	3
C.	Know Your Upstream Provider Requirements	3
D.	Gateway Provider Blocking Requirements Upon Notification of Illegal Traffic	4
E.	Gateway Provider Blocking Requirements Based on a Do-Not-Originate (DNO) List	5
F.	Caller ID Authentication by Intermediate Providers	6
G.	Caller ID Authentication in Non-IP Networks.....	6
H.	Extension of STIR/SHAKEN Implementation Deadline.....	6
I.	Robocall Mitigation	7
J.	Certification in the Robocall Mitigation Database.....	7
K.	Intermediate and Voice Service Provider Obligations	9
L.	Review of Governance Authority Decision to Revoke an SPC Token.....	10
M.	Public Safety Safeguards	11
N.	Enforcement Tools and Obligations	11
V.	RECORDKEEPING AND REPORTING REQUIREMENTS	12
VI.	EFFECTIVE DATES.....	13
VII.	INTERNET LINKS	13

I. INTRODUCTION

This Small Entity Compliance Guide (Guide) summarizes rules and technological standards the Federal Communications Commission (Commission) adopted in the following orders that were released between August 2021 and March 2023 in its efforts to combat illegal robocalls: 1) *Sixth Report and Order and Further Notice of Proposed Rulemaking (Sixth Report and Order)* adopted March 2023; 2) *Call Authentication Trust Anchor Third Report and Order* adopted in August 2021; 3) *Call Authentication Trust Anchor Fourth Report and Order (Small Provider Order)* adopted in December 2021; and 4) *Call Authentication Trust Anchor Fifth Report and Order (Gateway Provider Order)* adopted in May 2022.

In the *Sixth Report and Order*, the Commission adopted additional requirements that strengthen and expand the STIR/SHAKEN caller ID authentication framework. Widespread deployment of the STIR/SHAKEN framework will reduce the effectiveness of illegal call spoofing, allow law enforcement to identify bad actors more easily, and help phone companies identify calls with illegally spoofed caller ID information before those calls reach their subscribers. The *Sixth Report and Order* builds upon previous Commission orders summarized below, with the goal of protecting consumers from illegally spoofed robocalls. Links to each order can be found in Section VII of this Guide.

II. OBJECTIVES OF THE MARCH 2023 PROCEEDING

The *Sixth Report and Order* strengthens and expands caller ID authentication requirements in the STIR/SHAKEN ecosystem by requiring non-gateway intermediate providers that receive unauthenticated calls directly from an originating provider to use STIR/SHAKEN to authenticate those calls. Second, the *Sixth Report and Order* expands robocall mitigation requirements for all providers, including those that have not yet implemented STIR/SHAKEN because they lack the necessary infrastructure or are subject to an implementation extension. Third, the Commission defines and clarifies the STIR/SHAKEN obligations of satellite providers. Finally, the *Sixth Report and Order* empowers the Enforcement Bureau with new tools to impose penalties that will hold providers accountable for failing to comply with the Commission's rules.

III. BACKGROUND

In 2020, the Commission adopted the first two orders implementing its call authentication rules pursuant to the Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED) Act,¹ including requiring voice service providers to adopt caller ID authentication technological standards known as "STIR/SHAKEN."² The Commission issued subsequent orders, summarized below, that strengthened and expanded these rules starting in 2021 with the *Call Authentication Trust Anchor Third Report and Order*, followed by the *Small Provider Order* and the *Gateway Provider Order*.

¹ Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105 (2019) (codified in 47 U.S.C. § 227b) (TRACED Act).

² Secure Telephone Identity Revisited (STIR) and Signature-based Handling of Asserted Information Using toKENs (SHAKEN) standards. 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 (2020) (*Caller ID Authentication First Report and Order*); *Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, 36 FCC Rcd 1859 (2020) (*Caller ID Authentication Second Report and Order*).

Call Authentication Trust Anchor Third Report and Order.³ The August 2021 *Call Authentication Trust Anchor Third Report and Order (Third Report and Order)* established a procedure for voice service providers and intermediate providers to appeal to the Commission when their Service Provider Code (SPC) token has been revoked by the private Governance Authority (GA) that oversees the STIR/SHAKEN framework. The *Third Report and Order* also set rules for when a provider must update its Robocall Mitigation Database submission to reflect a revocation. Rules adopted in the *Third Report and Order* became effective September 30, 2021.

Call Authentication Trust Anchor Fourth Report and Order (Small Provider Order).⁴ In December 2021, the *Small Provider Order* shortened the STIR/SHAKEN implementation deadline for small voice service providers with 100,000 or fewer subscriber lines by one year, i.e., no later than June 30, 2022, based on evidence that non-facilities-based small voice service providers were originating a high and increasing share of illegal robocalls relative to their subscriber base.⁵ In addition, voice service providers suspected of originating illegal robocalls must implement STIR/SHAKEN within 90 days of an Enforcement Bureau determination following a summary process. Rules adopted in the *Small Provider Order* became effective February 24, 2022.

Call Authentication Trust Anchor Fifth Report and Order (Gateway Provider Order).⁶ The May 2022 *Gateway Provider Order* required all gateway providers, not subject to certain continuing extensions in the Commission's rules, to authenticate with STIR/SHAKEN all Session Initiation Protocol (SIP) calls carrying U.S. North American Numbering Plan (NANP) numbers in the caller ID field by June 30, 2023. The *Gateway Provider Order* also required gateway providers to adopt specific robocall mitigation practices, such as responding to traceback requests within 24 hours, blocking substantially similar traffic when notified by the Commission of illegal traffic as well as calls from numbers on a "reasonable" do-not-originate list, and implementing "know-your-upstream provider" procedures. Rules adopted in the *Gateway Provider Order* became effective September 23, 2022.

IV. COMPLIANCE REQUIREMENTS

The Commission adopted definitions, key components, and dates for the compliance requirements in the *Third Report and Order*, *Small Provider Order*, *Gateway Provider Order*, and the *Sixth Report and Order*. The order that adopted or modified each rule is denoted in parentheses following each rule.

A. Definitions (47 CFR §§ 64.1200; 64.6300) (amended in the *Small Provider Order*, *Gateway Provider Order*, and *Sixth Report and Order*)

The Commission adopted several new definitions applicable to the Restrictions on Telemarketing, Telephone Solicitation, and Facsimile Advertising (Subpart L), and to Caller ID Authentication (Subpart HH) of part 64 of the Commission's rules:

³ *Call Authentication Trust Anchor, Appeals of the STIR/SHAKEN Governance Authority Token Revocation Decisions*, WC Docket Nos. 17-97 and 21-291, *Third Report and Order*, 36 FCC Rcd 12878 (2021) (*Caller ID Authentication Third Report and Order*).

⁴ *Call Authentication Trust Anchor*, WC Docket No. 17-97, *Fourth Report and Order*, 36 FCC Rcd 17840 (2021) (*Small Provider Order*).

⁵ *Call Authentication Trust Anchor, Third Further Notice of Proposed Rulemaking*, WC Docket No. 17-97, 36 FCC Rcd 8827, 8830-32, paras. 6, 8-10 (2021) (citing data submitted in the record and Federal Trade Commission enforcement actions).

⁶ *Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, *Sixth Report and Order* in CG Docket No. 17-59, *Fifth Report and Order* in WC Docket No. 17-97, *Order On Reconsideration* in WC Docket No. 17-97, *Seventh Further Notice of Proposed Rulemaking* in CG Docket No. 17-59, and *Fifth Further Notice of Proposed Rulemaking* in WC Docket No. 17-97, FCC 22-37 (2022) (*Gateway Provider Order*).

- Gateway provider is 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.”
- U.S.-based is defined as a provider with “facilities in the United States, including a point of presence capable of processing the call.”
- Receives a call directly is defined as the “foreign provider directly upstream of the gateway provider in the call path sent the call to the gateway provider, with no providers in-between.”
- Intermediate provider is defined as “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.”
- Non-facilities-based small voice service provider is defined as “a small voice service provider that is offering voice service to end-users solely using connections that are not sold by the provider or its affiliates.”
- Non-gateway Intermediate provider is defined as “any entity that is an intermediate provider” and “that is not a gateway provider” as those terms are defined above.

B. Traceback Request Responses by Gateway Providers (47 CFR § 64.1200(n)(1)) (amended in the *Gateway Provider Order*)

Gateway providers must (1) cooperatively participate with the industry traceback consortium; and (2) respond fully within 24 hours to all traceback requests it receives from the Commission, civil and criminal law enforcement, and the industry traceback consortium regarding calls for which it acts as a gateway provider.

The 24-hour clock does not start outside of business hours, and requests received during that time are deemed received at 8:00 a.m. on the next business day. If the 24-hour response period would end on a non-business day, either a weekend or a federal legal holiday, the 24-hour clock does not run for the weekend or holiday in question, and restarts at 12:01 a.m. on the next business day following when the request would otherwise be due. Business hours is defined as 8:00 a.m. to 5:30 p.m. on a business day. All times are local time for the office that is required to respond to the request.

C. Know Your Upstream Provider Requirements (47 CFR § 64.1200(n)(4)) (adopted in the *Gateway Provider Order*)

Gateway providers must take reasonable and effective steps to ensure that the immediate upstream foreign provider is not using the gateway provider to carry or process a high volume of illegal traffic onto the U.S. network.⁷

⁷ A subsequent item, *Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Seventh Report and Order, FCC 23-37 (May 19, 2023) (*Seventh Report and Order*), redesignates this requirement as 47 CFR § 64.1200(n)(5) as part of other rule modifications. These changes will be covered in a subsequent Small Entity Compliance Guide.

D. Gateway Provider Blocking Requirements Upon Notification of Illegal Traffic (47 CFR § 64.1200(n)(5)-(6))⁸ (adopted in the *Gateway Provider Order*)

Gateway providers properly notified must block illegal traffic and any substantially similar traffic on an ongoing basis (unless its investigation determines that the traffic is not illegal) when it receives actual written notice of such traffic by the Commission through its Enforcement Bureau. The gateway provider will not be held liable under the Communications Act or the Commission's rules if they inadvertently block lawful traffic as part of the requirement to block substantially similar traffic so long as it is blocking consistent with these requirements.

Notifications of Suspected Illegal Traffic. These notices shall: (1) identify with as much particularity as possible the suspected illegal traffic; (2) provide the basis for the Enforcement Bureau's reasonable belief that the identified traffic is unlawful; (3) cite the statutory or regulatory provisions the suspected illegal traffic appears to violate; and (4) direct the provider receiving the notice that it must comply with section 64.1200(n)(5) of the Commission's rules.

- Notifications shall specify a timeframe of no fewer than 14 days for an identified gateway provider to comply with the notice.
- Each notified provider must promptly investigate the identified traffic and report the results of that investigation to the Enforcement Bureau within the timeframe specified in the Notification.
- If the investigation determines that the provider serves as a gateway provider for the identified traffic, it must block the identified traffic within the timeframe specified in the Notification and include in its report to the Enforcement Bureau:
 - Certification that it is blocking the identified traffic and will continue to do so; and
 - A description of its plan to identify and block substantially similar traffic on an ongoing basis.
- If the provider's investigation determines that the identified traffic is not illegal, it shall provide an explanation as to why the provider reasonably concluded that the identified traffic is not illegal and what steps it took to reach that conclusion. Absent such a showing, or if the Enforcement Bureau determines based on the evidence that the traffic is illegal despite the provider's assertions, the identified traffic will be deemed illegal.
- If the notified provider determines during this investigation that it did not serve as the gateway provider for any of the identified traffic, it shall provide an explanation as to how it reached that conclusion and, if it is a non-gateway intermediate or terminating provider for the identified traffic, it must identify the upstream provider(s) from which it received the identified traffic and, if possible, take lawful steps to mitigate this traffic.
- If the notified provider determines that it is the originating provider for the identified traffic, or the traffic otherwise comes from a source that does not have direct access to the U.S. public switched telephone network, the notified provider must comply with 47 CFR

⁸ The *Seventh Report and Order* redesignates 47 CFR § 64.1200(n)(5) as 47 CFR § 64.1200(n)(2) and 47 CFR § 64.1200(n)(6) as 47 CFR § 64.1200(n)(3) as part of other rule modifications. These changes will be covered in a subsequent Small Entity Compliance Guide.

§ 64.1200(n)(2) by effectively mitigating the identified traffic and report to the Enforcement Bureau any steps the provider has taken to effectively mitigate the identified traffic.

- If the Enforcement Bureau finds that an approved plan is not blocking substantially similar traffic, the identified provider shall modify its plan to block such traffic.
- If the Enforcement Bureau finds that the identified provider continues to allow suspected illegal traffic onto the U.S. network, it may proceed under § 64.1200(n)(5)(ii) or (iii) as appropriate.

Initial Determination Order. The Enforcement Bureau may issue an Initial Determination Order to the gateway provider stating the gateway provider is not in compliance with section 64.1200(n)(5) in the following circumstances:

- The provider fails to respond to the Notification of Suspected Illegal Traffic;
- The Enforcement Bureau determines that the response is insufficient,
- The gateway provider is continuing to allow substantially similar traffic onto the U.S. network after the timeframe specified in the Notification of Suspected Illegal Traffic, or
- Based on the evidence, the traffic is illegal despite the provider's assertions.

The Initial Determination Order shall include the Enforcement Bureau's reasoning for its determination and give the gateway provider a minimum of 14 days to provide a final response prior to the Enforcement Bureau making a final determination on whether the provider is in compliance with this section.

Final Determination Order. If the gateway provider does not provide an adequate response to the Initial Determination Order within the timeframe permitted in that Order or continues to allow substantially similar traffic onto the U.S. network, the Enforcement Bureau shall issue a Final Determination Order finding that the gateway provider is not in compliance with this section.

The Final Determination Orders shall be published in EB Docket No. 22-174 at [https://www.fcc.gov/ecfs/search/search-filings/results?q=\(proceedings.name:\(\"22-174\"\)\)](https://www.fcc.gov/ecfs/search/search-filings/results?q=(proceedings.name:(\). A Final Determination Order may be issued up to one year after the release date of the Initial Determination Order, and may be based on either an immediate failure to comply with this rule or a determination that the gateway provider has failed to meet its ongoing obligation under this rule to block substantially similar traffic.

When the Commission's Enforcement Bureau has notified a gateway provider that it issued a Final Determination Order finding that the gateway provider failed to block as required under section 64.1200(n)(5), any provider immediately downstream from the gateway provider must block and cease accepting all traffic received directly from the identified gateway provider.

The Enforcement Bureau will publish the Final Determination Order in EB Docket No. 22-174 at [https://www.fcc.gov/ecfs/search/search-filings/results?q=\(proceedings.name:\(\"22-174\"\)\)](https://www.fcc.gov/ecfs/search/search-filings/results?q=(proceedings.name:(\). Providers must monitor EB Docket No. 22-174 and initiate blocking no later than 30 days from the release date of the Final Determination Order. A provider that chooses to initiate blocking sooner than 30 days from the release date may do so consistent with section 64.1200(k)(4).

E. Gateway Provider Blocking Requirements Based on a Do-Not-Originate (DNO) List (47 CFR § 64.1200(o)) (adopted in the *Gateway Provider Order*)

Gateway providers must block calls purporting to originate from a number on at least one reasonable DNO list. Reasonable DNO lists may include only:

- Numbers for which the subscriber to which the number is assigned has requested that calls purporting to originate from that number be blocked because the number is used for inbound calls only;
- NANP numbers that are not valid;
- Valid NANP numbers that are not allocated to a provider by the NANP Administrator; and
- Valid NANP numbers that are allocated to a provider by the NANP Administrator, but are unused, so long as the provider blocking the calls is the allocatee of the number and confirms that the number is unused or has obtained verification from the allocatee that the number is unused at the time of blocking.

Reasonable DNO lists must include at a minimum any inbound-only government numbers where the government entity has requested the number be included and private inbound-only numbers that have been used in imposter scams, when a request is made by the private entity assigned such a number. Gateway providers, or those managing DNO lists, should ensure that entities can reasonably request inclusion on the list.

F. Caller ID Authentication by Intermediate Providers (47 CFR § 64.6302(c) adopted in the *Gateway Provider Order*, 47 CFR § 64.6302(d) adopted in the *Sixth Report and Order*)

By June 30, 2023, unless subject to an extension, a gateway provider must have authenticated caller identification information for all calls it receives using NANP resources that pertain to the U.S. in the caller ID field and for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call.

By December 31, 2023, unless subject to an extension, a non-gateway intermediate provider must authenticate caller identification information for all calls it receives directly from an originating provider and for which the caller identification information has not been authenticated and which it will exchange with another provider as a SIP call.

G. Caller ID Authentication in Non-IP Networks (47 CFR § 64.6303(b) adopted in the *Gateway Provider Order*, 47 CFR § 64.6303(c) adopted in the *Sixth Report and Order*)

For the non-IP portions of their network, gateway providers and non-gateway intermediate providers must either (1) upgrade to IP and implement STIR/SHAKEN throughout its network, or (2) work to develop a non-IP caller ID authentication solution. If a provider wishes to comply by meeting the second option, it must maintain and be ready to provide the Commission, on request, documented proof that it is participating (on its own or through a representative, including a third-party representative) as a member of a working group, industry standards group, or consortium that is working to develop or is actively testing a non-IP caller ID authentication solution.

H. Extension of STIR/SHAKEN Implementation Deadline (47 CFR § 64.6304) (adopted in the *Small Provider Order*, amended in the *Gateway Provider Order* and the *Sixth Report and Order*)

Non-facilities-based small voice service providers were required to comply with the caller ID authentication and related requirements in section 64.6301 by June 30, 2022. The small voice service provider will no longer be exempt from the requirements of STIR/SHAKEN implementation beginning 90 days after the Enforcement Bureau determines that: 1) it notified the small voice service provider of suspected illegal calls and the Enforcement Bureau determines that provider failed to respond in a timely manner or with information requested (including credible evidence that the robocall traffic identified by the Enforcement Bureau is not illegal); 2) the small voice service provider failed to or demonstrate it has

taken steps to effectively mitigate the traffic; or 3) if the Enforcement Bureau determines the small voice service provider violated section 64.1200(n)(2). If the exemption would have terminated earlier than 90 days after the Enforcement Bureau determination, then that earlier termination date will apply.

Like voice service providers, gateway providers and non-gateway intermediate providers that are incapable of obtaining an SPC token due to the GA's token access policy have a STIR/SHAKEN implementation extension that runs until the gateway provider is capable of obtaining an SPC token as long as the provider diligently pursues obtaining the token.⁹ Similarly, gateway providers and non-gateway intermediate providers that rely on technology that cannot initiate, maintain, carry, process, and terminate SIP calls are subject to a continuing extension. Small voice service providers that originate calls via satellite using NANP numbers have a continuing STIR/SHAKEN implementation extension.

I. Robocall Mitigation (47 CFR § 64.6305(a)-(c)) (amended in the *Small Provider Order*, *Gateway Provider Order*, and *Sixth Report and Order*)

All providers (i.e., voice service providers, gateway providers, and non-gateway intermediate providers) shall implement an appropriate robocall mitigation program. The program must include:

- Reasonable steps to avoid originating (for a voice service provider), or carrying or processing (for gateway providers and non-gateway intermediate providers) illegal robocall traffic;
- A commitment to respond fully and in a timely manner (for voice service providers and non-gateway intermediate providers) or within 24 hours (for gateway providers) to all traceback requests from the Commission, law enforcement, and the industry traceback consortium; and
- A commitment to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls (for voice service providers) or carry or process calls (for gateway providers and non-gateway intermediate providers).

J. Certification in the Robocall Mitigation Database (47 CFR § 64.6305(d)-(e)) (adopted in the *Gateway Provider Order*, amended in the *Sixth Report and Order*)

All providers must certify in the Robocall Mitigation Database that all of the calls it originates on its network (if it is a voice service provider) or that it carries or processes on its network (if it is a gateway provider or non-gateway intermediate provider) are subject to a robocall mitigation program, that any prior certification has not been removed by Commission action, that the Commission has not prohibited it from filing in the Robocall Mitigation Database, and to one of the following:

- It has fully implemented the STIR/SHAKEN framework across its entire network, and all the calls it originates are compliant with sections 64.6301(a)(1) and (2) (if it is a voice service provider); or that all the calls it carries or processes are compliant with section 64.6302(b) if (it is a gateway provider or non-gateway intermediate provider);
- It has implemented the STIR/SHAKEN authentication framework on a portion of its network, and all calls it originates on that portion of its network are compliant with sections 64.6301(a)(1) and (2) (if it is a voice service provider), or that all calls that it carries or processes on that portion of its network are compliant with section 64.6302(b) (if it is a gateway provider or non-gateway intermediate provider); or
- It has not implemented STIR/SHAKEN on any portion of its network.

All providers must include the following information in its certification in English or with a certified English translation:

⁹ *Gateway Provider Order*, para. 61; *Caller ID Authentication Sixth Report and Order*, para. 48.

- Identification of the type of extension or extensions the provider received under section 64.6304, if the provider is not a foreign provider, and the basis for the extension or extensions, or an explanation of why it is unable to implement STIR/SHAKEN due to a lack of control over the network infrastructure necessary to implement STIR/SHAKEN;
- The specific reasonable steps the provider has taken to avoid originating (if it is a voice service provider), or carrying or processing (if it is a gateway provider or non-gateway intermediate provider), illegal robocalls as part of its robocall mitigation program.
 - If it is a voice service provider, how it complies with its obligation to know its customers and take affirmative, effective measures to prevent new and renewing customers from originating illegal calls under section 64.1200(n). If it is a gateway provider, how it complies with its obligation to know its upstream providers under section 64.1200(n).
 - To comply with the requirement to describe their “new and renewing customer” and “know your upstream provider” procedures, providers must “describe any contractual provisions with end-users or upstream providers designed to mitigate illegal robocalls.”¹⁰
 - All providers must describe any procedures in place to know its upstream providers, and the analytics systems it uses to identify and block illegal traffic, including whether it uses any third-party analytics vendors and the names of such vendors.
- A statement of the provider’s commitment to respond fully and in a timely manner (if it is a voice service provider or non-gateway intermediate provider) and within 24 hours (if it is a gateway provider) 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 (if it is a voice service provider) or to carry or process calls (if it is a gateway or non-gateway intermediate provider); and
- A statement whether, at any time in the prior two years, the entity submitting the certification (and/or any entity for which the filing entity shares common ownership, management, directors, or control) has been the subject of a formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to the filing entity transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or mitigation program description; and, if so, provide a description of any such action or investigation, including all law enforcement or regulatory agencies involved, the date that any action or investigation was commenced, the current status of the action or investigation, a summary of the findings of wrongdoing made in connection with the action or investigation, and whether any final determinations have been issued.
 - This requirement is limited to reporting formal actions and investigations that have been commenced or issued pursuant to a written notice or other instrument containing findings by the law enforcement or regulatory agency that the filing entity has been or is suspected of the illegal activities itemized above, including, but not limited to, notices of apparent liability, forfeiture orders, state or federal civil lawsuits or criminal indictments, and cease-and-desist notices.¹¹

All providers must also file the following information in the Robocall Mitigation Database:

¹⁰ *Caller ID Authentication Sixth Report and Order*, para. 40.

¹¹ *Id.* at para. 47.

- The provider's business name and primary address.
- Other business names in use by the provider.
- All business names previously used by the provider.
- Whether the provider and/or its affiliate is a foreign voice service provider.
- The name, title, department, business address, telephone number, and email address of one person within the company responsible for addressing robocall-mitigation related issues.
- Whether the provider is:
 - A voice service provider with a STIR/SHAKEN implementation obligation directly serving end users.
 - A voice service provider with a STIR/SHAKEN implementation obligation acting as a wholesale provider originating calls on behalf of another provider or providers.
 - A voice service provider, gateway provider, or non-gateway intermediate provider without a STIR/SHAKEN implementation obligation.
 - A gateway provider or non-gateway intermediate provider with a STIR/SHAKEN implementation obligation.
- The provider's Operating Company Number (OCN), if it has one.
- Information regarding the provider's principals, affiliates, subsidiaries, and parent companies in sufficient detail to facilitate the Commission's ability to determine whether the provider has been prohibited from filing in the Robocall Mitigation Database.¹²

All providers shall update their filings within 10 business days of any change to the foregoing information and update their filing following an SPC token revocation by the GA by the later of:

- the expiration of the 30-day period for appeal to the GA;
- following the completion of GA's final review process;
- the expiration of the 60-day period for appeal to the Commission; or
- 10 business days after the Wireline Competition Bureau releases a final decision.

All certifications shall be filed in the Robocall Mitigation Database and signed by a company officer pursuant to 47 CFR § 1.16. A provider who previously submitted plans with respect to STIR/SHAKEN rules that were not in English or submitted with an English translation must have updated its plans no later than January 26, 2023.¹³ Providers may request confidential treatment of their filings, consistent with the Commission's existing confidentiality requirements.¹⁴

K. Intermediate and Voice Service Provider Obligations (47 CFR § 64.6305(g)(2)-(g)(4)) (adopted in the *Sixth Report and Order*)

Providers shall accept calls directly from a domestic voice service provider, only if that voice service provider's filing appears in the Robocall Mitigation Database and that filing has not been de-listed pursuant to an enforcement action.

¹² *Id.* at para. 46.

¹³ *Gateway Provider Order*, para. 38.

¹⁴ *Id.* para. 36; *Caller ID Authentication Sixth Report and Order*, para. 49.

Providers shall accept calls directly from a foreign voice service provider or foreign intermediate provider that uses NANP resources that pertain to the United States in the caller ID field to send voice traffic to residential or business subscribers in the United States only if that foreign provider's filing appears in the Robocall Mitigation Database and that filing has not been de-listed from the Robocall Mitigation Database due to an enforcement action.

Providers shall accept calls directly from a gateway provider, only if the gateway provider's filing appears in the Robocall Mitigation Database showing that the gateway provider has affirmatively submitted the filing, and that filing has not been de-listed pursuant to an enforcement action.

Providers shall accept calls directly from a non-gateway intermediate provider, only if that non-gateway intermediate provider's filing appears in the Robocall Mitigation Database showing that the non-gateway intermediate provider affirmatively submitted the filing, and that filing has not been de-listed pursuant to an enforcement action. The compliance date of this obligation for non-gateway intermediate providers will be no sooner than 90 days following the deadline established by the Wireline Competition Bureau notice for non-gateway intermediate providers to file a certification in the Robocall Mitigation Database.¹⁵

L. Review of Governance Authority Decision to Revoke an SPC Token (47 CFR §§ 64.6308, 0.91(r)) (adopted in the *Third Report and Order*)

Any provider (i.e., a voice service provider or intermediate provider) aggrieved by a Governance Authority (GA) decision to revoke that provider's token must first seek review from the GA and exhaust that process prior to seeking Commission review. A provider requesting Commission review of a GA decision shall file such a request within 60 days of the GA's final decision upholding a token revocation, and such request must be filed electronically in WC Docket No. 21-291 through the Commission's Electronic Comment Filing System (ECFS), and must be captioned "In the matter of Request for Review by (name of party seeking review) of Decision of the GA to Revoke an SPC Token." The process for filing oppositions and replies to oppositions to the appeal must follow 47 CFR § 1.45.

A copy of the request for review with the Commission must be served on the GA by the provider requesting review at sti-ga@atis.org or in accordance with any alternative delivery mechanism the GA establishes in its procedures. The request for review must contain:

- A statement setting forth the provider's asserted basis for appeal of the GA revocation decision;
- A full statement of the relevant, material facts with supporting affidavits and documentation, including any background information the provider deems useful to the Commission's review; and
- The question presented for review, with reference, where appropriate, to any underlying Commission rule or GA policy.

The Wireline Competition Bureau has authority to rule on the request for review in accordance with 47 CFR § 0.91(r) and the provider can seek review of the Wireline Competition Bureau's decision pursuant to 47 CFR § 1.115. Except in extraordinary circumstances, the Wireline Competition Bureau's decision should be expected no later than 180 days from the date the request for review is filed in ECFS. The Wireline Competition Bureau has discretion to pause the 180-day period in situations where actions outside of its control are responsible for delaying the review. The Wireline Competition Bureau must conduct *de novo* review of the GA decision.

¹⁵ *Caller ID Authentication Sixth Report and Order*, para. 50.

Following a GA token revocation decision, a provider will not be considered out of compliance with the Commission's caller ID authentication rules until the later of:

- the expiration of the 30-day period for appeal to the GA;
- completion of the GA's final review process upholding the revocation; or
- where the provider has sought timely Commission review of a GA decision to revoke the provider's SPC token, until and unless the Wireline Competition Bureau has upheld or otherwise decided not to overturn the GA's decision.

The effective date of Commission action may not be stayed without an order by the Wireline Competition Bureau or Commission pursuant to 47 CFR §§ 1.102(b) and 1.106(n). Following revocation by the GA, and unless and until the revocation is reversed, the provider may not maintain possession and use of its token, and will not be able to continue to exchange STIR/SHAKEN-authenticated traffic during the pendency of an appeal.¹⁶ A provider that relies on a delegated token from another entity may seek a waiver for a limited period if the token that it relies upon is revoked.¹⁷

M. Public Safety Safeguards (47 CFR §§ 64.1200(k)(5), (k)(6), and 64.6305(g)(5)) (amended in the *Gateway Provider Order, Sixth Report and Order*)

Providers must follow public safety safeguards when blocking calls under 47 CFR §§ 64.1200(k)(1)-(4), (1), (n)(5)-(6), (o) and 64.6305(e). A provider may not block a voice call if the call is an emergency call to 911 and must make all reasonable efforts to ensure that it does not block any calls from public safety answering points and government emergency numbers.

N. Enforcement Tools and Obligations (47 CFR §§ 1.80, 0.111) (amended in the *Small Provider Order, Gateway Provider Order, Sixth Report and Order*)

In the *Gateway Provider Order* and *Caller ID Authentication Sixth Report and Order*, the Commission adopted a number of several enforcement tools and obligations on providers. Specifically, it:

- Established a per-call maximum forfeiture amount of \$23,727 for violations of the robocall blocking rules.¹⁸
- Concluded that gateway providers and non-gateway intermediate providers can be removed from the Robocall Mitigation Database or subject to other penalties if they file a deficient robocall mitigation plan, knowingly or negligently carry or process illegal robocalls, or accept calls from a provider not listed in the Robocall Mitigation Database or that has been de-listed through enforcement action.¹⁹
- Established a process for removal of all providers' filings from the Robocall Mitigation Database where they are found to be "facially deficient."²⁰
 - Under that process, if the Enforcement Bureau believes that a filing is facially deficient, it will: (1) issue a notice to the provider explaining the basis for its conclusion and provide

¹⁶ *Id.* at para. 28.

¹⁷ *Id.* at para. 14

¹⁸ 47 CFR § 1.80(b)(9)-(12).

¹⁹ *Gateway Order*, para. 40; *Caller ID Authentication Sixth Report and Order*, para. 50; 47 CFR § 0.111(a)(28).

²⁰ *Caller ID Authentication Sixth Report and Order*, paras. 59-64.

an opportunity for the provider to cure the deficiency or explain why its certification is not deficient within 10 days; and

- (2) if the deficiency is not cured or the provider fails to establish that there is no deficiency within that 10-day period, the Enforcement Bureau will issue an order removing the provider from the Robocall Mitigation Database.
- Concluded that it may use its existing authority to revoke section 214 operating authority, or other provider authorizations, licenses, and/or instruments, for repeated violations of the robocall mitigation rules.²¹
 - The robocall mitigation rules include the specific obligations to:
 - Implement a robocall mitigation program that includes specific “reasonable steps” to mitigate illegal robocalls and comply with the steps outlined in the plan;
 - Submit a certification describing the mitigation program to the Robocall Mitigation Database;
 - Not accept traffic from providers not in the Robocall Mitigation Database; and
 - Authenticate calls under the Commission’s caller ID authentication rules.
- Once an authorization, license, and/or instrument is revoked, the Commission will consider the public interest impact of that revocation when deciding whether to grant other future Commission authorizations, licenses, or certifications to that same entity, as well as the individual company owners, directors, officers, and principals (either individuals or entities) of such entities.

V. RECORDKEEPING AND REPORTING REQUIREMENTS

The *Gateway Provider Order* and the *Caller ID Authentication Sixth Report and Order* contain rules with new or modified information collection and reporting requirements as discussed in Section IV above. Both orders require each gateway or non-gateway intermediate provider to: (1) upgrade its non-IP networks to IP so that the STIR/SHAKEN authentication framework may be implemented, or (2) work to develop a non-IP authentication solution. To satisfy the latter option, a provider must, 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.

Gateway Provider Order. In addition to the requirements above, all gateway providers must describe in the Robocall Mitigation Database the specific reasonable steps taken to avoid carrying or processing illegal robocalls including how they are meeting their obligation to know their upstream provider. Gateway providers are also required to submit similar information to the Robocall Mitigation Database as voice service providers with a Robocall Mitigation Database filing requirement. The Commission clarified that voice service providers and gateway providers are required to submit all information in English or with a certified English translation. All gateway providers must also respond to traceback requests fully and within 24 hours and block calls based on at least one reasonable DNO list.

Caller ID Authentication Sixth Report and Order. In addition to the requirements above, all providers, including those that had already fully implemented STIR/SHAKEN and those that lack control over the network infrastructure necessary to implement STIR/SHAKEN, are required to submit a certification and robocall mitigation plan to the Robocall Mitigation Database. All Robocall Mitigation

²¹ *Id.* at paras. 66-73; 47 CFR § 0.111(a)(29).

Database filers, including existing filers subject to new or modified requirements, must provide additional information on mitigation plans and make additional certifications with their filings.²²

VI. EFFECTIVE DATES

- The *Caller ID Authentication Third Report and Order* became effective on September 30, 2021.
- The *Small Provider Order* became effective on February 24, 2022.
- The *Gateway Provider Order* became effective on September 23, 2022. Compliance with certain rules from the *Gateway Provider Order* became effective upon Office of Management and Budget's (OMB) approval of information collection requirements under the Paperwork Reduction Act (PRA). This includes compliance with amendments to 47 CFR § 64.1200(n)(1), required by September 23, 2022, and compliance with 47 CFR § 64.1200(o), required by December 19, 2022. Compliance with amendments to 47 CFR §§ 64.6303(b), 64.6305(b), 64.6305(c)(2) and 64.6305(d) was required by January 11, 2023, and compliance with amendments to 47 CFR § 64.6305(e)(2) and (e)(3) was required by April 11, 2023.
- The *Caller ID Authentication Sixth Report and Order* became effective on August 21, 2023, except for the amendments to 47 CFR §§ 64.6303(c) and 64.6305(d), (e), (f), and (g), which are pending OMB's approval of information collection requirements under the PRA. These rules shall become effective after the Wireline Competition Bureau publishes a public notice in the Federal Register announcing OMB's approval and the relevant effective date(s).

VII. INTERNET LINKS

A copy of the *Caller ID Authentication Third Report and Order* is available at: <https://docs.fcc.gov/public/attachments/FCC-21-93A1.pdf>.

A copy of the Federal Register Summary of the *Caller ID Authentication Third Report and Order* is available at: <https://www.govinfo.gov/content/pkg/FR-2021-08-31/pdf/2021-18765.pdf>.

A copy of the *Small Provider Order* is available at: <https://docs.fcc.gov/public/attachments/FCC-21-122A1.pdf>.

A copy of the Federal Register Summary of the *Small Provider Order* is available at: <https://www.govinfo.gov/content/pkg/FR-2022-01-25/pdf/2022-01244.pdf>.

A copy of the *Gateway Provider Order* is available at: <https://docs.fcc.gov/public/attachments/FCC-22-37A1.pdf>.

A copy of the Federal Register Summary of the *Gateway Provider Order* is available at: <https://www.govinfo.gov/content/pkg/FR-2022-08-24/pdf/2022-18148.pdf>.
<https://www.govinfo.gov/content/pkg/FR-2022-07-18/pdf/2022-13878.pdf>

A copy of the Public Notice announcing compliance dates of the amendments to 47 CFR 64.6300 *et seq.* from the *Gateway Provider Order* that were pending PRA review is available at: <https://docs.fcc.gov/public/attachments/DA-22-1303A1.pdf>.

²² *Caller ID Authentication Sixth Report and Order*, paras. 38-49.

A copy of the Federal Register Notice announcing the compliance date of the amendments to 47 CFR 64.1200(n)(1) from the *Gateway Provider Order* that were pending PRA review is available at: <https://www.govinfo.gov/content/pkg/FR-2022-08-24/pdf/2022-18148.pdf>.

A copy of the Federal Register Notice announcing the compliance date of the amendments to 47 CFR 64.1200(o) from the *Gateway Provider Order* that were pending PRA review is available at: <https://www.govinfo.gov/content/pkg/FR-2022-11-18/pdf/2022-25148.pdf>.

A copy of the *Caller ID Authentication Sixth Report and Order* is available at: <https://docs.fcc.gov/public/attachments/FCC-23-18A1.pdf>.

A copy of the Federal Register Summary of the *Caller ID Authentication Sixth Report and Order* is available at: <https://www.govinfo.gov/content/pkg/FR-2023-06-21/pdf/2023-12142.pdf>.

A copy of the Caller ID Authentication Rules (47 CFR § 64.6300 *et seq.*) is available at: <https://www.ecfr.gov/current/title-47/chapter-I/subchapter-B/part-64#subpart-HH>.

A copy of the Call Blocking Rules (47 CFR 64.1200 *et seq.*) is available at: <https://www.ecfr.gov/current/title-47/chapter-I/subchapter-B/part-64/subpart-L>.