
This content is from the eCFR and is authoritative but unofficial.

Title 47 —Telecommunication

Chapter I —Federal Communications Commission

Subchapter B —Common Carrier Services

Part 64 —Miscellaneous Rules Relating to Common Carriers

Subpart HH —Caller ID Authentication

Source: 85 FR 22043, Apr. 21, 2020, unless otherwise noted.

Authority: 47 U.S.C. 151, 152, 154, 201, 202, 217, 218, 220, 222, 225, 226, 227, 227b, 228, 251(a), 251(e), 254(k), 255, 262, 276, 403(b)(2)(B), (c), 616, 620, 716, 1401-1473, unless otherwise noted; Pub. L. 115-141, Div. P, sec. 503, 132 Stat. 348, 1091; Pub. L. 117-338, 136 Stat. 6156.

Source: 28 FR 13239, Dec. 5, 1963, unless otherwise noted.

§ 64.6305 Robocall mitigation and certification.

(a) *Robocall mitigation program requirements for voice service providers.*

- (1)** Each voice service provider shall implement an appropriate robocall mitigation program.
- (2)** Any robocall mitigation program implemented pursuant to paragraph (a)(1) of this section shall include reasonable steps to avoid originating illegal robocall traffic and shall include a commitment to respond within 24 hours 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.

(b) *Robocall mitigation program requirements for gateway providers.*

- (1)** Each gateway provider shall implement an appropriate robocall mitigation program with respect to calls that use North American Numbering Plan resources that pertain to the United States in the caller ID field.
- (2)** Any robocall mitigation program implemented pursuant to paragraph (b)(1) of this section shall include reasonable steps to avoid carrying or processing illegal robocall traffic and shall include a commitment to respond fully and within 24 hours 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.

(c) *Robocall mitigation program requirements for non-gateway intermediate providers.*

- (1)** Each non-gateway intermediate provider shall implement an appropriate robocall mitigation program.
- (2)** Any robocall mitigation program implemented pursuant to paragraph (c)(1) of this section shall include reasonable steps to avoid carrying or processing illegal robocall traffic and shall include a commitment to respond within 24 hours 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.

(d) *Certification by voice service providers in the Robocall Mitigation Database.*

- (1) A voice service provider shall certify that all of the calls that it originates on its network are subject to a robocall mitigation program consistent with paragraph (a) of this section, that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and to one of the following:
 - (i) It has fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it originates are compliant with § 64.6301(a)(1) and (2);
 - (ii) 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 § 64.6301(a)(1) and (2); or
 - (iii) It has not implemented the STIR/SHAKEN authentication framework on any portion of its network.
- (2) A voice service provider shall include the following information in its certification in English or with a certified English translation:
 - (i) Identification of the type of extension or extensions the voice service provider received under § 64.6304, if the voice service provider is not a foreign voice service 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;
 - (ii) The specific reasonable steps the voice service provider has taken to avoid originating illegal robocall traffic as part of its robocall mitigation program, including a description of how it complies with its obligation to know its customers pursuant to § 64.1200(n)(4), any procedures in place to know its upstream providers, and the analytics system(s) it uses to identify and block illegal traffic, including whether it uses any third-party analytics vendor(s) and the name(s) of such vendor(s);
 - (iii) A statement of the voice service provider's commitment to respond within 24 hours 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; and
 - (iv) State whether, at any time in the prior two years, the filing entity (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.
- (3) All certifications made pursuant to paragraphs (d)(1) and (2) of this section shall:
 - (i) Be filed in the appropriate portal on the Commission's website; and
 - (ii) Be signed by an officer in conformity with 47 CFR 1.16.

- (4) A voice service provider filing a certification shall submit the following information in the appropriate portal on the Commission's website:
 - (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;
 - (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;
 - (vi) Whether the voice service provider is:
 - (A) A voice service provider with a STIR/SHAKEN implementation obligation directly serving end users;
 - (B) A voice service provider with a STIR/SHAKEN implementation obligation acting as a wholesale provider originating calls on behalf of another provider or providers; or
 - (C) A voice service provider without a STIR/SHAKEN implementation obligation; and
 - (vii) The voice service provider's OCN, if it has one.
 - (5) A voice service provider shall update its filings within 10 business days of any change to the information it must provide pursuant to paragraphs (d)(1) through (4) of this section.
 - (i) A voice service provider or intermediate provider that has been aggrieved by a Governance Authority decision to revoke that voice service provider's or intermediate provider's SPC token need not update its filing on the basis of that revocation until the sixty (60) day period to request Commission review, following completion of the Governance Authority's formal review process, pursuant to § 64.6308(b)(1) expires or, if the aggrieved voice service provider or intermediate provider files an appeal, until ten business days after the Wireline Competition Bureau releases a final decision pursuant to § 64.6308(d)(1).
 - (ii) If a voice service provider or intermediate provider elects not to file a formal appeal of the Governance Authority decision to revoke that voice service provider's or intermediate provider's SPC token, the provider need not update its filing on the basis of that revocation until the thirty (30) day period to file a formal appeal with the Governance Authority Board expires.
- (e) ***Certification by gateway providers in the Robocall Mitigation Database.***
- (1) A gateway provider shall certify that all of the calls that it carries or processes on its network are subject to a robocall mitigation program consistent with paragraph (b)(1) of this section, that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and to one of the following:
 - (i) It has fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it carries or processes are compliant with § 64.6302(b);
 - (ii) It has implemented the STIR/SHAKEN authentication framework on a portion of its network and calls it carries or processes on that portion of its network are compliant with § 64.6302(b); or

- (iii) It has not implemented the STIR/SHAKEN authentication framework on any portion of its network for carrying or processing calls.
- (2) A gateway provider shall include the following information in its certification made pursuant to paragraph (e)(1) of this section, in English or with a certified English translation:
 - (i) Identification of the type of extension or extensions the gateway provider received under § 64.6304 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;
 - (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 a description of how it complies with its obligation to know its upstream providers pursuant to § 64.1200(n)(5), the analytics system(s) it uses to identify and block illegal traffic, and whether it uses any third-party analytics vendor(s) and the name(s) of such vendor(s);
 - (iii) A statement of the gateway provider's commitment to respond fully and within 24 hours 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; and
 - (iv) State whether, at any time in the prior two years, the filing entity (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.
- (3) All certifications made pursuant to paragraphs (e)(1) and (2) of this section shall:
 - (i) Be filed in the appropriate portal on the Commission's website; and
 - (ii) Be signed by an officer in conformity with 47 CFR 1.16.
- (4) A gateway provider filing a certification shall submit the following information in the appropriate portal on the Commission's website:
 - (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 foreign voice service provider;
 - (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;
 - (vi) Whether the gateway provider is:

- (A) A gateway provider with a STIR/SHAKEN implementation obligation; or
- (B) A gateway provider without a STIR/SHAKEN implementation obligation; and
- (vii) The gateway provider's OCN, if it has one.

(5) A gateway provider shall update its filings within 10 business days to the information it must provide pursuant to paragraphs (e)(1) through (4) of this section, subject to the conditions set forth in paragraphs (d)(5)(i) and (ii) of this section.

(f) *Certification by non-gateway intermediate providers in the Robocall Mitigation Database.*

(1) A non-gateway intermediate provider shall certify that all of the calls that it carries or processes on its network are subject to a robocall mitigation program consistent with paragraph (c) of this section, that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the Robocall Mitigation Database by the Commission, and to one of the following:

- (i) It has fully implemented the STIR/SHAKEN authentication framework across its entire network and all calls it carries or processes are compliant with § 64.6302(b);
- (ii) It has implemented the STIR/SHAKEN authentication framework on a portion of its network and calls it carries or processes on that portion of its network are compliant with § 64.6302(b); or
- (iii) It has not implemented the STIR/SHAKEN authentication framework on any portion of its network for carrying or processing calls.

(2) A non-gateway intermediate provider shall include the following information in its certification made pursuant to paragraph (f)(1) of this section in English or with a certified English translation:

- (i) Identification of the type of extension or extensions the non-gateway intermediate provider received under § 64.6304, if the non-gateway intermediate 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;
- (ii) The specific reasonable steps the non-gateway intermediate provider has taken to avoid carrying or processing illegal robocall traffic as part of its robocall mitigation program, including a description of any procedures in place to know its upstream providers and the analytics system(s) it uses to identify and block illegal traffic, including whether it uses any third-party analytics vendor(s) and the name of such vendor(s);
- (iii) A statement of the non-gateway intermediate provider's commitment to respond within 24 hours 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; and
- (iv) State whether, at any time in the prior two years, the filing entity (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.

- (3) All certifications made pursuant to paragraphs (f)(1) and (2) of this section shall:
 - (i) Be filed in the appropriate portal on the Commission's website; and
 - (ii) Be signed by an officer in conformity with 47 CFR 1.16.
- (4) A non-gateway intermediate provider filing a certification shall submit the following information in the appropriate portal on the Commission's website:
 - (i) The non-gateway intermediate provider's business name(s) and primary address;
 - (ii) Other business names in use by the non-gateway intermediate provider;
 - (iii) All business names previously used by the non-gateway intermediate provider;
 - (iv) Whether the non-gateway intermediate provider or any affiliate is also foreign voice service provider;
 - (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;
 - (vi) Whether the non-gateway intermediate provider is:
 - (A) A non-gateway intermediate provider with a STIR/SHAKEN implementation obligation; or
 - (B) A non-gateway intermediate provider without a STIR/SHAKEN implementation obligation; and
 - (vii) The non-gateway intermediate service provider's OCN, if it has one.
- (5) A non-gateway intermediate provider shall update its filings within 10 business days of any change to the information it must provide pursuant to this paragraph (f) subject to the conditions set forth in paragraphs (d)(5)(i) and (ii) of this section.
- (g) **Intermediate provider and voice service provider obligations –**
 - (1) **Accepting traffic from domestic voice service providers.** Intermediate providers and voice service 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 in accordance with paragraph (d) of this section and that filing has not been de-listed pursuant to an enforcement action.
 - (2) **Accepting traffic from foreign providers.** Beginning April 11, 2023, intermediate providers and voice service providers shall accept calls directly from a foreign voice service provider or foreign intermediate provider that uses North American Numbering Plan 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 in accordance with paragraph (d) of this section and that filing has not been de-listed pursuant to an enforcement action.

- (3) **Accepting traffic from gateway providers.** Beginning April 11, 2023, intermediate providers and voice service providers shall accept calls directly from a gateway provider only if that gateway provider's filing appears in the Robocall Mitigation Database in accordance with paragraph (e) of this section, showing that the gateway provider has affirmatively submitted the filing, and that filing has not been de-listed pursuant to an enforcement action.
- (4) **Accepting traffic from non-gateway intermediate providers.** Intermediate providers and voice service 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 in accordance with paragraph (f) of this section, showing that the non-gateway intermediate provider affirmatively submitted the filing, and that filing has not been de-listed pursuant to an enforcement action.
- (5) **Public safety safeguards.** Notwithstanding paragraphs (g)(1) through (4) of this section:
 - (i) A provider may not block a voice call under any circumstances if the call is an emergency call placed to 911; and
 - (ii) A provider must make all reasonable efforts to ensure that it does not block any calls from public safety answering points and government emergency numbers.

[87 FR 42946, July 18, 2022, as amended at 88 FR 40119, June 21, 2023; 88 FR 43459, July 10, 2023]