

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of	)	
	)	
Digital Solutions Inc.	)	EB-TCD-25-00039386 ¹
	)	EB Docket No. 22-174
	)	

FINAL DETERMINATION ORDER AND REMOVAL ORDER

Adopted: October 5, 2026

Released: October 5, 2026

By the Chief, Enforcement Bureau:

I. INTRODUCTION

1. By this Final Determination Order and Removal Order, the Enforcement Bureau (Bureau) finds that Digital Solutions Inc. (Digital Solutions or Company) has not complied with section 64.1200(n)(2) of the Federal Communications Commission's (Commission or FCC) rules.² Voice service providers immediately downstream of Digital Solutions must block and cease accepting all traffic from Digital Solutions beginning 30 calendar days after the release of this Final Determination Order.³ Providers may block and cease accepting traffic from Digital Solutions before the expiration of this 30-calendar-day period if they provide the Commission with notice and a brief summary of the basis for their determination that Digital Solutions has failed to effectively mitigate illegal traffic or failed to implement effective measures to prevent new and renewing customers from using its network to originate illegal calls.⁴ Furthermore, by this Removal Order, the Bureau removes Digital Solutions' certification from the Robocall Mitigation Database (RMD). Removal of Digital Solutions certification from the RMD requires all intermediate providers and voice service providers to cease accepting calls directly from the Company.⁵ Digital Solutions shall not re-file an RMD certification without the prior approval of the Bureau and the Wireline Competition Bureau (WCB).

2. The Bureau has twice addressed Digital Solutions in this proceeding: on April 2, 2026, the Bureau issued a Notification of Suspected Illegal Traffic and Additional Notification of Robocall

¹ The investigation began under File No. EB-TCD-25-00038998 and was subsequently assigned File No. EB-TCD-25-00039386. Any future correspondence with the Commission concerning this matter should reflect the new case number.

² See 47 CFR § 64.1200(n)(2)(iii) ("If the provider does not provide an adequate response to the Initial Determination Order within the timeframe permitted in that Order or continues to originate substantially similar traffic onto the U.S. network, the Enforcement Bureau shall issue a Final Determination Order finding that the provider is not in compliance with this section.").

³ See *id.* § 64.1200(n)(3).

⁴ See *id.* § 64.1200(k)(4).

⁵ See *id.* § 64.6305(g). Notwithstanding this requirement, "[a] provider may not block a voice call under any circumstances if the call is an emergency call placed 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." *Id.* § 64.6304(g)(5).

Mitigation Database Certification Deficiency (Notice),⁶ and on June 29, 2026, the Bureau issued an Initial Determination Order and Order to Show Cause (Initial Determination Order).⁷ Digital Solutions' response to the Notice omitted information required by the Commission's rules⁸ with respect to the suspected illegal traffic the Company originated,⁹ and, while the Company cured one of two deficiencies in its RMD certification, it left the other uncured.¹⁰ The Initial Determination Order afforded the Company a final opportunity to supply the missing information and cure the remaining deficiency.¹¹ The Company did neither. Therefore, we take this final step of mandating call blocking and removing Digital Solutions from the RMD.

II. BACKGROUND

A. Voice Service Provider Mandatory Blocking Rules¹²

3. Protecting consumers in the United States from the dangers and risks of unwanted and illegal robocalls is the Commission's top consumer protection priority.¹³ Voice service providers can—and sometimes do—facilitate, or even protect, bad-actor callers.¹⁴ When bad-actor callers are shielded by bad-actor voice service providers, it is significantly more difficult to stop the calls.¹⁵ To address the problem, the Commission requires voice service providers to block illegal traffic in some cases.¹⁶ On May 19, 2022, the Commission adopted the *Gateway Provider Order*, which built upon the Commission's prior, permissive call blocking rules to require gateway providers to block illegal traffic when notified of such traffic by the Commission.¹⁷ On May 18, 2023, the Commission expanded the

⁶ Letter from Patrick Webre, Chief, FCC Enforcement Bureau, to Richard Anderson, Chief Executive Officer, Digital Solutions Inc., 2026 WL 1015536 (Apr. 2, 2026), <https://docs.fcc.gov/public/attachments/DOC-420553A1.pdf> (Notice).

⁷ *Digital Solutions Inc.*, EB Docket No. 22-174, Initial Determination Order and Order to Show Cause, DA 26-643, 2026 WL 1907538 (EB June 29, 2026), <https://docs.fcc.gov/public/attachments/DA-26-643A1.pdf> (Initial Determination Order).

⁸ See 47 CFR 64.1200(n)(2) (describing a voice service provider's obligations “[u]pon receipt of a Notice of Suspected Illegal Traffic”).

⁹ Notice, *supra* note 6, at 1-2 & Attach. A (identifying calls that the Company originated).

¹⁰ Initial Determination Order, *supra* note 7, at 7, paras. 13, 15.

¹¹ *Id.* at 7-8, paras. 14, 16.

¹² For purposes of this section, the term “voice service provider” refers to that term as used in section 64.1200 of the Commission's rules, which is based on the definition of “voice service” in 47 CFR § 64.1600(r) and includes intermediate providers.

¹³ *Stop Unwanted Robocalls and Texts*, Fed. Comm'n's Comm'n, <https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts> (last visited July 1, 2026) (“Stopping illegal robocalls is the Federal Communication Commission's (FCC) top consumer protection priority.”).

¹⁴ *Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, WC Docket No. 17-97, Seventh Report and Order in CG Docket 17-59 and WC Docket 17-97, Eighth Further Notice of Proposed Rulemaking in CG Docket 17-59, and Third Notice of Inquiry in CG Docket 17-59, 38 FCC Rcd 5404, 5410, para. 15 (2023) (*Seventh Call Blocking Order*).

¹⁵ *Id.*

¹⁶ *Id.* at 5415, para. 29.

¹⁷ *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 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, Order, 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, 37 FCC Rcd 6865, 6898, para. 75 (2022) (*Gateway Provider Order*); see 47 CFR § 64.1200(k)(1)-(3) (listing

(continued....)

mandatory call blocking framework created in the *Gateway Provider Order* to all voice service providers.¹⁸

4. Mandatory call blocking pursuant to sections 64.1200(n)(2) and (n)(3) of the Commission's rules can entail a three-step process if the notified provider fails to take action as directed by the Bureau.¹⁹ *First*, a provider will receive a notification of suspected illegal traffic from the Bureau requiring the provider to investigate the suspected illegal traffic, report the results of the investigation to the Bureau, and block the identified traffic and substantially similar traffic unless it determines the identified traffic is not illegal.²⁰ *Second*, if the provider fails to respond to the notification, the Bureau determines that the response is insufficient, the Bureau determines that the provider is continuing to originate substantially similar traffic, or the Bureau determines that the traffic is illegal despite assertions by the provider to the contrary, then the Bureau will issue an initial determination order.²¹ The provider then has an opportunity to respond.²² *Third*, if the Bureau determines that the provider's response to the Initial Determination Order is inadequate (including if the provider fails to respond), or if it continues to transmit substantially similar traffic, the Bureau may issue a final determination order mandating all immediate downstream providers block and cease accepting all traffic from the provider starting 30 calendar days from release of the final determination order.²³ Downstream providers may choose to initiate blocking before expiration of this 30-calendar-day period if they provide the Commission with notice and a brief summary of the basis for their determination that the provider has failed to effectively mitigate illegal traffic or failed to implement effective measures to prevent new and renewing customers from using its network to originate illegal calls.²⁴

B. RMD Certification Rules and Removal Procedures

5. The FCC established the RMD in 2021 to promote transparency and effective robocall mitigation.²⁵ Voice service providers, gateway providers, and non-gateway intermediate providers must file a certification in the RMD.²⁶ A provider must include in its RMD certification, among other things, a description of the specific reasonable steps the provider has taken to avoid originating, carrying, or

permissive blocking scenarios such as Do-Not-Originate lists, invalid and unallocated numbers, and reasonable analytics).

¹⁸ *Seventh Call Blocking Order*, 37 FCC Rcd at 5415, para. 29 (requirements codified at 47 CFR § 64.1200(n)(2)–(3)).

¹⁹ 47 CFR § 64.1200(n)(2)–(3).

²⁰ *Id.* § 64.1200(n)(2)(i)(A).

²¹ *Id.* § 64.1200(n)(2)(ii).

²² *Id.*

²³ *Id.* § 64.1200(n)(2)(iii) (permitting issuance of a Final Determination Order up to one year after release of the Initial Determination Order); *id.* § 64.1200(n)(3); *One Eye LLC Final Determination Order*, EB Docket No. 22-174, 38 FCC Rcd 4211, 4214, para. 8 (EB 2023) (finding that One Eye's failure to respond to the Initial Determination Order was an inadequate response).

²⁴ 47 CFR § 64.1200(n)(2)(iii); *see id.* § 64.1200(k)(4).

²⁵ *See Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, 36 FCC Rcd 1859, 1902-03, paras. 82-83 (2020) (*Second Caller ID Authentication Order*); *Wireline Competition Bureau Announces Opening of Robocall Mitigation Database and Provides Filing Instructions and Deadlines*, WC Docket No. 17-97, Public Notice, 36 FCC Rcd 7394 (WCB 2021) (announcing the immediate opening of the RMD on April 20, 2021).

²⁶ 47 CFR § 64.6305(d)–(f). Paragraph (d) applies to voice service providers; paragraph (e) applies to gateway providers; and paragraph (f) applies to non-gateway intermediate providers. For purposes of this section, the term “voice service provider” is based on the definition of “voice service” in section 64.6300 of the Commission's rules, which applies to the RMD requirements in section 64.6305. *See* 47 CFR § 64.6300(o). As such, the term “voice service provider” excludes intermediate providers (*i.e.*, gateway providers and non-gateway intermediate providers), as those terms are defined in section 64.6300. *See id.* § 64.6300(d), (g), (i).

processing illegal robocall traffic as part of its robocall mitigation program.²⁷ Providers must also certify whether they have fully or partially implemented STIR/SHAKEN on their networks and whether the calls that they originate, carry, or process are compliant with the applicable STIR/SHAKEN caller ID authentication rules in section 64.6301 or 64.6302 of the Commission's rules.²⁸ The RMD certification must also include a statement of the provider's commitment to respond 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 initiate calls.²⁹ An officer of the provider filing a certification in the RMD must declare, under penalty of perjury, that the information included in the certification is true and correct.³⁰ The submission of false or inaccurate information makes a certification deficient and may result in an enforcement action against the filer, including removal of the filing from the RMD.³¹

6. The Commission may remove a provider's filing from the RMD that it finds "deficient in some way."³² To do so, the Commission will first contact the provider to notify it that its filing is deficient, explain the nature of the deficiency, and provide 14 days for the provider to cure the deficiency.³³ If the provider fails to cure the deficiency, the Bureau will release an order to show cause concluding that the provider's filing is deficient based on the available evidence. The order will direct the provider to—within 14 days—cure the deficiency in its filing and explain why the Bureau should not remove the provider's certification from the RMD.³⁴ If the provider fails to cure the deficiency or provide a sufficient explanation why its filing is not deficient within that 14-day period, the Bureau will release an

²⁷ 47 CFR § 64.6305(d)(2)(ii), (e)(2)(ii), (f)(2)(ii) (requiring the description to include how the provider complies with its obligations to know its customers and upstream providers pursuant to 64.1200(n)(4) and (n)(5) 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 vendors).

²⁸ *Id.* § 64.6305(d)(1), (e)(1), (f)(1); *see also id.* §§ 64.6301, 6302.

²⁹ *Id.* § 64.6305(d)(2)(iii), (e)(2)(iii), (f)(2)(iii).

³⁰ *Id.* § 64.6305(d)(3)(ii), (e)(3)(ii), (f)(3)(ii); *id.* § 1.16; *see also Call Authentication Trust Anchor*, WC Docket No. 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd 2573, 2595, para. 42 (2023) (*Sixth Caller ID Authentication Order*).

³¹ *See Second Caller ID Authentication Order*, 36 FCC Rcd at 1903, para. 83 (noting that if a certification "is deficient in some way," the Commission may take enforcement action as appropriate, including "removing a defective certification from the database after providing notice to the voice service provider and an opportunity to cure the filing"); *Gateway Provider Order*, 37 FCC Rcd at 6882, para. 40 (discussing the same enforcement actions against gateway providers); *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2603, para. 57 (discussing the same enforcement actions against non-gateway intermediate providers). The Commission may also impose a forfeiture on filers that submit false or inaccurate information in the RMD. *See Improving the Effectiveness of the Robocall Mitigation Database, Amendment of Part 1 of the Commission's Rules, Concerning Practice and Procedure, Amendment of CORES Registration System*, WC Docket No. 24-213, MD Docket No. 10-234, Report and Order, 40 FCC Rcd 599, 606-07, para. 18 (2025) (adopting a \$10,000 base forfeiture for submitting false or inaccurate information to the RMD); *see also Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2590, para. 31 ("[A] provider's program is 'sufficient if it includes detailed practices that can reasonably be expected to significantly reduce' the carrying or processing (for intermediate providers) or origination (for voice service providers) of illegal robocalls. Each provider 'must comply with the practices' that its program requires, and its program is insufficient if the provider 'knowingly or through negligence' carries or processes calls (for intermediate providers) or originates (for voice service providers) unlawful robocall campaigns." (citations omitted)).

³² *Second Caller ID Authentication Order*, 36 FCC Rcd at 1903, para. 83 (regarding voice service provider filings); *see also Gateway Provider Order*, 37 FCC Rcd at 6882, para. 40 (adopting the same approach for gateway provider filings); *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2603, para. 57 (adopting the same approach for non-gateway intermediate provider filings).

³³ *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2604, para. 60.

³⁴ *Id.*

order removing the provider from the RMD.³⁵

7. Under the Commission's rules, intermediate providers and voice service providers shall accept calls directly from a domestic voice service provider, gateway provider, or non-gateway intermediate provider only if that provider's certification appears in the RMD.³⁶ Removal of a provider's certification from the RMD therefore requires all intermediate providers and voice service providers to cease accepting all calls directly from the provider, except calls to 911 and other emergency communications numbers.³⁷

C. Digital Solutions' Origination of Illegal Robocalls

8. The Bureau identified 51 calls placed to wireless telephone numbers between May 6, 2025, and July 8, 2025, that delivered prerecorded messages without the consent of the called parties, in apparent violation of section 227(b)(1)(A) of the Communications Act of 1934, as amended, and the Commission's implementing rules.³⁸ Nineteen of the identified calls purported to be from someone on the "loan processing team" and stated that the called party's "application" had been "preapproved for up to 41,000 dollars with estimated monthly payments of around 610 dollars depending on the terms you select."³⁹ Four of the identified calls stated "we finally have an approval for you" and "to review your offer and select your terms, press 2 now."⁴⁰ The remaining calls for which the Bureau has an audio recording stated that the "new administration has introduced updated IRS relief programs," and that the recipient is qualified for one of these programs that "could significantly reduce or even eliminate" their tax balance.⁴¹

9. The Industry Traceback Group (ITG)⁴² investigated the identified calls and determined that Digital Solutions originated the suspected illegal robocalls.⁴³ The ITG notified Digital Solutions of these calls, provided the Company with supporting data identifying each call, and explained that the basis for the traceback was "[e]vidence of lack of consent for prerecorded message."⁴⁴ Digital Solutions confirmed that it originated the calls and identified three of its customers as the sources of all of the calls.⁴⁵

D. Digital Solutions' Deficient RMD Certification

10. While investigating the above-described suspected illegal traffic, the Bureau identified

³⁵ *Id.*

³⁶ 47 CFR § 64.6305(g).

³⁷ *See id.*

³⁸ Notice, *supra* note 6, at 1 & Attach. A (identifying calls that the Company originated); 47 U.S.C. § 227(b)(1)(A) (requiring callers to obtain consent before placing calls using an artificial or prerecorded voice to certain types of numbers); 47 CFR § 64.1200(a)(1)-(2) (same).

³⁹ Notice, *supra* note 6, at 1.

⁴⁰ *Id.*

⁴¹ *Id.* at 1-2.

⁴² The ITG is the registered industry consortium selected pursuant to the TRACED Act to conduct tracebacks. *See Implementing Section 13(d) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act (TRACED Act)*, EB Docket No. 20-22, Report and Order, 38 FCC Rcd 7561, 7561-62, para. 1 (EB 2023); *see also* Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, Pub. L. No. 116-105, § 13(d), 133 Stat. 3274, 3287-88 (2019).

⁴³ Notice, *supra* note 6, at 2.

⁴⁴ *Id.*

⁴⁵ *Id.*; *see also* ITG Subpoena Response (July 24, 2025) (on file at EB-TCD-25-00039386) (ITG July Response).

deficiencies with Digital Solutions' RMD certification. Specifically:

(1) the Company certified that it has fully implemented STIR/SHAKEN across its entire network, but its robocall mitigation plan indicates that it has not implemented STIR/SHAKEN on a portion of its network; and (2) the Company has certified that it authenticates the caller ID information for all Session Initiation Protocol (SIP) calls it originates on its network, but ITG traceback data indicates that it has not done so for at least some calls.⁴⁶

With regard to the second deficiency, the Notice identified in Attachment B ten calls that the Bureau determined were authenticated by providers other than Digital Solutions.⁴⁷ The Notice cited evidence that the Bureau had obtained from Verizon, the terminating provider (or "end point") for these ten calls.⁴⁸ The evidence showed that the calls carried SIP Identity headers containing PASSporTs that had been signed using Secure Telephone Identity (STI) certificates issued to providers other than Digital Solutions.⁴⁹ The ITG traceback data similarly showed that the STI certificates used to sign the calls were issued to providers other than Digital Solutions.⁵⁰

E. Digital Solutions' Inadequate Response to the Notice

11. On April 2, 2026, the Bureau sent the Notice to Digital Solutions via certified mail.⁵¹ The Bureau also sent an email containing the Notice, with the subject line "Official Correspondence from the Federal Communications Commission," to Digital Solutions' official contact listed in the RMD.⁵² The Notice and the Commission's rules required Digital Solutions to investigate the identified traffic and report the results of its investigation to the Bureau within 14 days (*i.e.*, on or before April 16, 2026).⁵³ The Notice required the report to include both a certification that it is blocking the identified traffic and will continue to do so⁵⁴ and a description of its plan to identify and block or cease accepting substantially similar traffic on an ongoing basis.⁵⁵ Alternatively, if Digital Solutions reasonably concluded either that the identified traffic was not illegal or that it did not serve as the gateway or originating provider for any

⁴⁶ Notice, *supra* note 6, at 3.

⁴⁷ *Id.* at Attach. B.

⁴⁸ Verizon Subpoena Response (Jan. 8, 2026) (on file at EB-TCD-25-00039386) (Verizon Subpoena Response).

⁴⁹ *Id.*; Notice, *supra* note 6, at 6 n.52 (citing the Verizon Subpoena Response and noting that it "show[ed] the intermediate providers that signed each of the calls in Attachment B"); *see also Call Authentication Trust Anchor*, WC Docket No. 17-97, Eighth Report and Order, 39 FCC Rcd 12894, 12897, paras. 6-7 & n.25 (2024) (*Eighth Caller ID Authentication Order*) (discussing the STIR/SHAKEN process and the use of STI certificates to sign an encrypted Personal Assertion Token (PASSporT) that travels with the call and is then verified and decrypted by the terminating provider).

⁵⁰ ITG Subpoena Response (Nov. 17, 2025) (on file at EB-TCD-25-00039386) (ITG November Response).

⁵¹ *See* Certified Mail Receipt (Apr. 2, 2026) (on file at EB-TCD-25-00039386).

⁵² Email from Enforcement Bureau, FCC, to Richard Anderson, Chief Executive Officer, Digital Solutions Inc. (Apr. 2, 2026, 10:03 AM EDT) (on file at EB-TCD-25-00039386). The Bureau also sent the Notice via certified mail and first class mail to Digital Solutions' Denver, Colorado address of record contained in the RMD. Both mailings were returned to sender and marked "NOT DELIVERABLE AS ADDRESSED UNABLE TO FORWARD." Envelopes from Telecommunications Consumers Division, FCC Enforcement Bureau, to Digital Solutions Inc., 1050 Curtis Street, Denver, CO 80202 postmarked Apr. 17, 2026 (on file at EB-TCD-25-00039386).

⁵³ Notice, *supra* note 6, at 5; *see generally* 47 CFR § 64.1200(n)(2)(i)(A) ("The . . . Notification of Suspected Illegal Traffic shall give the identified provider a minimum of 14 days to comply with the notice.").

⁵⁴ Notice, *supra* note 6, at 5; *see also* 47 CFR § 64.1200(n)(2)(i)(A)(1).

⁵⁵ Notice, *supra* note 6, at 5; *see also* 47 CFR § 64.1200(n)(2)(i)(A)(2).

of the traffic, its report was required to explain the basis for that conclusion.⁵⁶ If Digital Solutions concluded that it was not the gateway or originating provider for any of the identified traffic, but instead was a non-gateway intermediate or terminating provider for such traffic, it was required to provide an explanation as to how it reached that conclusion and “identify the upstream provider(s) from which the Company received the identified traffic and, if possible, take steps to mitigate the traffic.”⁵⁷ The Notice warned Digital Solutions that its failure to comply would be grounds for the Bureau to issue an initial determination order and, if the noncompliance continued, a final determination order requiring all immediate downstream providers to block its traffic under sections 64.1200(n)(2)(iii) and (n)(3) of the Commission’s rules.⁵⁸

12. The Notice also addressed Digital Solutions RMD certification, describing the certification’s deficiencies identified above and explaining how the Company could cure them:

- (a) provide an explanation for the discrepancy between the Company’s RMD certification and statements in its mitigation plan regarding its level of STIR/SHAKEN implementation, and update its certification and mitigation plan accordingly; and (b) provide authentication information for the calls listed in Attachment B within 14 days from the date of this Order and explain why it did not provide authentication information for each of the 13 calls.⁵⁹

The Notice warned Digital Solutions that failure to cure all deficiencies in its RMD certification would result in removal from the RMD, requiring all intermediate providers and voice service providers to cease accepting all calls directly from Digital Solutions.⁶⁰ The Notice also warned Digital Solutions that failure to respond to the Notice and to correct the noticed deficiencies with its RMD certification may be used as evidence that the Company’s certification is also deficient with respect to its commitment to cooperate with the Commission.⁶¹

13. On April 3, 2026, Digital Solutions filed a revised robocall mitigation plan in the RMD. The revised plan states that “DIGITAL SOLUTIONS INC. has fully implemented the STIR/SHAKEN caller authentication framework across its IP-based network.”⁶² This revision cured the first RMD certification deficiency identified in the Notice—the Company’s submission of contradictory information regarding its STIR/SHAKEN implementation status.⁶³ The Company did not, however, cure the second RMD certification deficiency: it failed to “provide authentication information for the calls listed in Attachment B . . . and explain why it did not provide authentication information for each of the . . . calls.”⁶⁴ Thus, despite being put on notice, the Company failed to explain how it fulfilled its responsibility under section 64.6301 to authenticate the calls (e.g., by engaging third parties to sign the calls). Thus, Digital Solutions’ certification that “it has fully implemented the STIR/SHAKEN authentication framework across its entire network” and that all calls it originates are compliant with

⁵⁶ Notice, *supra* note 6, at 5; *see also* 47 CFR § 64.1200(n)(2)(i)(B).

⁵⁷ Notice, *supra* note 6, at 5; *see also* 47 CFR § 64.1200(n)(2)(i)(B).

⁵⁸ Notice, *supra* note 6, at 4–6.

⁵⁹ *Id.* at 6. Although the text of the Notice referred to “13 calls,” only 10 calls were identified in Attachment B. *See id.* at Attach. B. Digital Solutions’ second RMD certification deficiency is thus based on its failure to provide call authentication for the 10 calls identified in Attachment B.

⁶⁰ *Id.* at 6–7 (citing 47 CFR § 64.6305(g)).

⁶¹ *Id.* at 6–7.

⁶² Digital Solutions Inc (RMD0027372), Fed. Commc’ns Comm’n, Robocall Mitigation Database, Attach. at 1 (filed Apr. 3, 2026) (Digital Solutions RMD Certification) (on file at EB-TCD-25-00039386). Digital Solutions submitted an additional RMD certification on July 12, 2026.

⁶³ Initial Determination Order, *supra* note 7, at 7, para. 15.

⁶⁴ *Id.* (quoting Notice, *supra* note 6, at 6).

section 64.6301, as well as the statement in its robocall mitigation plan, remain inaccurate.

14. On May 5, 2026—more than two weeks after the April 16 deadline set by the Notice—Digital Solutions responded to the Bureau by email, stating briefly that it had “taken action [a] long time ago and vacated those customer profiles and as a result we have been compliant and without any complaint for over 9 months,” and that “there has [sic] not been any more [of] such calls after Aug 12th 2025.”⁶⁵ Digital Solutions provided none of the other information required by the Notice, including the results of its investigation of the suspected illegal traffic, a certification that it is blocking the identified traffic and will continue to do so, or a description of its plan to identify and block or cease accepting substantially similar traffic on an ongoing basis.⁶⁶ Digital Solutions’ insufficient response, together with its still-deficient RMD certification, was the basis of the Initial Determination Order.⁶⁷

F. Digital Solutions’ Response to the Initial Determination Order

15. On June 29, 2026, the Bureau issued the Initial Determination Order to Digital Solutions requiring Digital Solutions to respond within 14 days of the release date of the order demonstrating compliance with the Commission’s rules.⁶⁸ The Initial Determination Order warned Digital Solutions that if it failed to provide “the specific information enumerated on page 5 of the Notice” within 14 days or continued to originate traffic substantially similar to the traffic identified in Attachment A of the Notice onto the U.S. network, the Bureau would issue this Final Determination Order.⁶⁹ Furthermore, this Final Determination Order would require any provider immediately downstream from Digital Solutions to block and cease accepting all traffic received directly from Digital Solutions.⁷⁰

16. The Initial Determination Order also afforded Digital Solutions a final opportunity to cure the remaining deficiency in its RMD certification or to explain why the certification is not deficient.⁷¹ The Bureau warned Digital Solutions that “[f]ailure to respond and correct the deficiency, or provide a sufficient explanation for why Digital Solutions should retain its certification in the RMD will result in removal of the certification.”⁷² Upon removal, all intermediate providers and voice service providers would be required to cease accepting all calls directly from the Company.⁷³

17. On July 12, 2026, Digital Solutions submitted an additional RMD certification again selecting Option 1, “Complete STIR/SHAKEN Implementation,” electronically signed by CEO Richard

⁶⁵ Email from DavidA@gdstelecom.net, signed as “Digital Solutions Inc Compliance Dept,” to Enforcement Bureau, FCC (May 5, 2026, 21:49 EDT) (on file at EB-TCD-25-00039386) (Digital Solutions First Response).

⁶⁶ Initial Determination Order, *supra* note 7, at 6, para. 12.

⁶⁷ See 47 CFR § 64.1200(n)(2)(ii) (“If the provider fails to respond to the Notification of Suspected Illegal Traffic [or] the [Bureau] determines that the response is insufficient, . . . the [Bureau] shall issue an Initial Determination Order to the provider stating the Bureau’s initial determination that the provider is not in compliance with this section.”).

⁶⁸ Initial Determination Order, *supra* note 7 at 1, 7, paras. 1, 14; *see also* 47 CFR § 64.1200(n)(2)(ii) (requiring the Bureau to give the provider a minimum of 14 days to provide a final response). The Bureau sent an email containing the Initial Determination Order, with the subject line “Official Correspondence from the FCC Enforcement Bureau,” to Digital Solutions’ robocall mitigation contact listed in the RMD. Email from Enforcement Bureau, FCC, to Richard Anderson, Chief Executive Officer, Digital Solutions Inc. (June 29, 2026, 12:46 PM EDT) (on file at EB-TCD-25-00039386). On June 30, 2026, the Bureau sent the Initial Determination Order to Digital Solutions via certified mail. Certified Mail Receipt (June 30, 2026) (on file at EB-TCD-25-00039386).

⁶⁹ Initial Determination Order, *supra* note 7, at 1, 7, paras. 1, 14; *see also* 47 CFR § 64.1200(n)(2)(iii).

⁷⁰ Initial Determination Order, *supra* note 7, at 1, 7, paras. 1, 14; *see also* 47 CFR § 64.1200(n)(3).

⁷¹ *Id.* at 7–8, para. 16.

⁷² *Id.* at 8, para. 17.

⁷³ *Id.* (citing 47 CFR § 64.6305(g)).

Anderson, under penalty of perjury.⁷⁴ Despite the existence of the April 2, 2026 Notice, and the June 29, 2026 Initial Determination Order, Digital Solutions responded “no” to the question whether “the filing entity has, at any time in the prior two years, been the subject of a formal Commission . . . investigation with accompanying findings of actual or suspected wrongdoing” for transmitting illegal robocalls or a deficient RMD certification.⁷⁵

18. On July 13, 2026, Digital Solutions responded to the Bureau by email, but its response addressed only the calls listed in Attachment B of the Notice.⁷⁶ Again, Digital Solutions did not provide any of the specific information required by page 5 of the Notice, including the results of its investigation of the suspected illegal traffic identified in Attachment A of the Notice, a certification that it is blocking the identified traffic and will continue to do so, or a description of its plan to identify and block or cease accepting substantially similar traffic on an ongoing basis.

19. With regard to the remaining RMD certification deficiency, the Company again failed to provide call authentication information for the ten calls listed in Attachment B and again failed to explain how it fulfilled its responsibility under section 64.6301 to authenticate the calls (e.g., by engaging third parties to sign the calls). Instead, the Company raised a number of arguments as to why it could not provide that information or did not need to provide that information. *First*, as a procedural matter, the Company asserted that it received only a redacted version of Attachment B and thus was unable to identify the ten calls. *Second*, the Company stated that because its “downstream carrier would not have accepted an unauthenticated call” all calls originated by Digital Solutions must have been authenticated.⁷⁷ *Third*, Digital Solutions suggested that the absence of call authentication information for the identified calls may be due to a “technical problem” somewhere downstream in the call path: “if [the Bureau is] not able to identify the signing authentication token that should relate to a technical problem some where [sic] in the call flow downstream or at the end point.”⁷⁸ *Finally*, the Company asserted that “[w]e attempted to research any possible way to find the SIP call traces, however, due to the time passed we can not [sic] obtain any SIP call technical trace record.”⁷⁹

III. DISCUSSION

A. Digital Solutions Is Subject to Mandatory Call Blocking

20. When a provider fails to adequately respond to an initial determination order, the Commission’s rules require the Bureau to issue a final determination order finding that the provider is not in compliance with section 64.1200(n)(2) of the Commission’s rules.⁸⁰ As detailed above, Digital Solutions’ response to the Notice was inadequate: the Company failed to satisfy its obligations under the

⁷⁴ Digital Solutions Inc (RMD0027372), Fed. Commc’ns Comm’n, Robocall Mitigation Database, Attach. at 1 (filed July 12, 2026), https://fccprod.servicenowservices.com/rmd?id=rmd_form&table=x_g_fmc_rmd_robotcall_mitigation_database&sys_id=4a11fac887b8e650e1cc75d9cebb3518&view=sp (Digital Solutions July 2026 RMD Certification) (attachment can be viewed by clicking on the “Download PDF” button) (on file at EB-TCD-25-00039386).

⁷⁵ *Id.*

⁷⁶ Email from DavidA@gdstelecom.net, signed as “Digital Solutions Inc Compliance Dept,” to Enforcement Bureau, FCC (July 13, 2026, 07:27 EDT) (on file at EB-TCD-25-00039386) (Digital Solutions Second Response) (“With regards to your inquiry about calls in Attachment B . . .”).

⁷⁷ Digital Solutions Second Response, *supra* note 76.

⁷⁸ *Id.*

⁷⁹ *Id.*

⁸⁰ See 47 CFR § 64.1200(n)(2)(iii) (“If the provider does not provide an adequate response to the Initial Determination Order within the timeframe permitted in that Order or continues to originate substantially similar traffic onto the U.S. network, the Enforcement Bureau *shall* issue a Final Determination Order finding that the provider is not in compliance with this section.” (emphasis added)).

Commission's rules with respect to the suspected illegal traffic.⁸¹ The Initial Determination Order afforded the Company a final opportunity to come into compliance with the Commission's rules, but the Company's response was again inadequate. The Company still has not provided the Bureau results of its investigation of the suspected illegal traffic, a certification that it is blocking the identified traffic and will continue to do so, or a description of its plan to identify and block or cease accepting substantially similar traffic on an ongoing basis.

21. To date, Digital Solutions has provided only a single sentence describing any investigation into the calls identified in Attachment A of the Notice, stating in its initial response to the Notice that it had "taken action [a] long time ago and vacated those customer profiles [responsible for the identified calls]."⁸² The Commission has made clear, however, that "an originating provider may not assume, without evidence, that the caller only has one subscriber line from which it is placing calls and must maintain vigilance to ensure that the caller does not use different existing accounts or open new accounts, under the same or a different name, to continue to place illegal calls."⁸³ Compliance with this obligation necessarily requires an originating provider, as a first step, to identify the customer(s) responsible for the illegal calls. Absent such identification, the provider cannot implement a plan to block the customer(s) from continuing to place the identified traffic or placing substantially similar calls through different accounts or under different names. Digital Solutions has offered no evidence that it identified the customer(s) responsible for the calls at issue, when or how it "vacated" the associated customer profiles, or what steps, if any, it has taken to ensure that those same customer(s) have not continued—or will not continue—to originate the identified traffic or substantially similar calls through other existing or newly opened accounts. Digital Solutions has also failed to provide a certification that it is blocking the identified traffic and will continue to do so, as required by the Notice and the Commission's rules.⁸⁴ In addition, the Company has failed to provide any plan as to how it will identify and block or cease accepting substantially similar traffic—including from other customers—on an ongoing basis.⁸⁵

22. The Bureau finds that Digital Solutions has not complied with section 64.1200(n)(2) of the Commission's rules.⁸⁶ All voice service providers immediately downstream of Digital Solutions must block and cease accepting all traffic from the Company beginning 30 calendar days after the release of this Final Determination Order.⁸⁷ Providers may block and cease accepting such traffic before expiration of this 30-calendar-day period if they provide the Commission with notice and a brief summary of the basis for their determination that Digital Solutions has failed to effectively mitigate illegal traffic or failed to implement effective measures to prevent new and renewing customers from using its network to originate illegal calls.⁸⁸

B. Digital Solutions' Certification is Removed From the RMD

23. The Bureau finds that Digital Solutions' RMD certification remains deficient. The Initial Determination Order directed the Company that, in order to cure the remaining deficiency, it must "provide authentication information for the calls listed in Attachment B . . . and explain why it did not

⁸¹ See *supra* paras. 11–14.

⁸² Digital Solutions First Response, *supra* note 65.

⁸³ *Seventh Call Blocking Order*, 37 FCC Rcd at 5419, para. 41.

⁸⁴ See Notice, *supra* note 6, at 5; 47 CFR § 64.1200(n)(2)(i)(A)(1); see also SK Teleco LLC, EB Docket No. 22-174, Final Determination Order and Removal Order, DA 26-583, at 6-7, paras. 12-14 (EB June 12, 2026).

⁸⁵ See Notice, *supra* note 6, at 5; 47 CFR § 64.1200(n)(2)(i)(A)(2).

⁸⁶ See 47 CFR § 64.1200(n)(2).

⁸⁷ See *id.* § 64.1200(n)(3).

⁸⁸ See *id.* § 64.1200(k)(4).

provide authentication information for each of the . . . calls.”⁸⁹ Alternatively, the Initial Determination Order directed the Company to explain why the Bureau should not remove the Company’s certification from the RMD.⁹⁰ The Company has failed to provide the required call authentication information for the identified calls to cure the deficiency and it has not offered a credible explanation “why its [RMD] certification is not deficient.”⁹¹

24. We find unavailing the Company’s arguments as to why it is unable to provide the required call authentication information. *First*, the Company asserts that it received only a redacted version of Attachment B and thus was unable to identify the ten calls listed.⁹² The record, however, shows that the Bureau sent unredacted copies of Attachment B to Digital Solutions by email and certified mail.⁹³ *Second*, the Company asserts that “due to the time passed we can not [sic] obtain any SIP call technical trace record.”⁹⁴ That lack of records rests solely with the Company and provides no basis on which we can find that it has cured its certification deficiency. Moreover, the STIR/SHAKEN call authentication information obtained by the Bureau from Verizon for the ten identified calls demonstrates that the PASSporTs for these calls were signed using STI certificates issued to providers other than Digital Solutions.⁹⁵ We note that Digital Solutions holds its own STI certificate,⁹⁶ which it used to sign other calls the Company originated during the same period as the calls identified in Attachments A and B.⁹⁷ Had the Company signed the calls listed in Attachment B, presumably those calls too would have carried PASSporTs signed using its own certificate. They did not. Significantly, Digital Solutions does not assert that it relied on any third parties to authenticate the identified calls.⁹⁸

25. We also find unpersuasive the Company’s arguments that it signed the identified calls, notwithstanding its inability to provide any call authentication records. The Company asserts that its “downstream carrier would not have accepted an unauthenticated call,”⁹⁹ but this argument is speculative, lacking any support, and is contradicted by the call authentication records provided by Verizon, which demonstrate that the calls were signed by providers other than Digital Solutions. The Company also asserts “if [the Bureau is] not able to identify the signing authentication token that should relate to a

⁸⁹ Initial Determination Order, *supra* note 7, at 7, para. 15.

⁹⁰ *Id.* at 7, para. 16.

⁹¹ *Id.* at 8, para. 16.

⁹² See Digital Solutions Second Response, *supra* note 73.

⁹³ See *supra* notes 51 and 52. If the Company had misplaced its copy of the unredacted Notice, it could at any time have requested an additional copy from the Bureau by contacting any of the Bureau staff identified in the Notice or the Initial Determination Order.

⁹⁴ See Digital Solutions Second Response, *supra* note 73.

⁹⁵ Verizon Subpoena Response, *supra* note 48.

⁹⁶ See <https://authenticate.iconektiv.com/authorized-service-providers-authenticate> (listing authorized providers holding STI certificates).

⁹⁷ See ITG November Response, *supra* note 50 (traceback no. 30937); ITG July Response, *supra* note 45 (traceback no. 29173, 29298).

⁹⁸ The Commission adopted rules regarding third-party authentication prior to the calls at issue here; however, those rules did not take effect until September 18, 2025. See 47 CFR 64.6301(b); *Eighth Caller ID Authentication Order*, 39 FCC Rcd at 12903-14, paras. 14-26; *Wireline Competition Bureau Announces Effective Date for STIR/SHAKEN Rules*, WC Docket No. 17-97, Public Notice, 40 FCC Rcd 5995, 5996 (WCB 2025). Specifically, the rules require the third party to sign calls using the voice service provider’s certificate, the voice service provider must make all attestation-level decision for each call, the parties must memorialize the agreement in writing, maintain the agreement for as long as the third-party arrangement exists, and retain a copy of the agreement for two years after termination of the agreement. 47 CFR § 64.6301(b).

⁹⁹ See Digital Solutions Second Response, *supra* note 76.

technical problem some where [sic] in the call flow downstream or at the end point.”¹⁰⁰ But this, too, is speculative. In fact, the Bureau has been able to identify which providers signed the identified calls based on the records provided by Verizon, and Digital Solutions was not one of those companies. In short, Digital Solutions has not “provide[d] authentication information for the calls listed in Attachment B . . . and explain[ed] why it did not provide authentication information for each of the . . . calls” as required by the Initial Determination Order¹⁰¹ Thus, the Bureau concludes that Digital Solutions has not fully implemented STIR/SHAKEN in compliance with section 64.6301 despite its certification to the contrary.

26. Moreover, Digital Solutions revised RMD certification, submitted July 12, 2026, the day before the Company responded via e-mail to the Bureau’s IDO, omits mention of the Notice and Initial Determination Order in responding to the question of whether the filing entity is “the subject of a formal Commission . . . investigation [concerning] facilitating illegal robocalls . . . or a deficient [RMD] certification.”¹⁰² Because it was corresponding with the Bureau at the time, the Company clearly was aware of Notice and the Initial Determination Order, a formal Commission proceeding that suspected the Company of illegal robocalling and RMD deficiencies. Nevertheless, the Company certified—falsely—that it was not the subject of any pending investigations. Whether the result of negligence or intentional misconduct, Digital Solutions’ failure to disclose this ongoing investigation concerning suspected illegal robocalls and RMD deficiencies in its revised RMD certification also renders its RMD filing deficient.

27. Therefore, Digital Solutions’ certification shall be removed from the RMD. All voice service providers and intermediate providers shall cease accepting calls directly from Digital Solutions within two business days of the release date of this Removal Order.¹⁰³ Digital Solutions shall not be permitted to refile unless and until both the Bureau and WCB consent.

IV. ORDERING CLAUSES

28. Accordingly, **IT IS ORDERED** that, pursuant to sections 4(i), 4(j), 227(b), 251(e), and 403 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 154(i), 154(j), 227(b), 251(e), 403; sections 0.111, 0.311, 1.1, 1.102(b)(1), and 64.1200(n)(3) of the Commission’s rules, 47 CFR §§ 0.111, 0.311, 1.1, 1.102(b)(1), and 64.1200(n)(3); and the *Sixth Caller ID Authentication Order*,¹⁰⁴ all immediate downstream providers **MUST BLOCK AND CEASE TO ACCEPT ALL TRAFFIC** directly from Digital Solutions **beginning no later than 30 calendar days** after the release date of this Final Determination Order and Removal Order.¹⁰⁵

29. **IT IS FURTHER ORDERED** that Digital Solutions is **IMMEDIATELY REMOVED** from the Robocall Mitigation Database as of the release date of this Final Determination Order and Removal Order.

30. **IT IS FURTHER ORDERED** that within **two business days** of the release of this Final Determination Order and Removal Order all intermediate providers and voice service providers **MUST CEASE ACCEPTING TRAFFIC** directly from Digital Solutions.

31. **IT IS FURTHER ORDERED** that Digital Solutions shall not refile in the Robocall Mitigation Database unless and until both the Wireline Competition Bureau and the Enforcement Bureau

¹⁰⁰ *Id.*

¹⁰¹ Initial Determination Order, *supra* note 7, at 7, para. 15 (quoting Notice, *supra* note 6, at 6).

¹⁰² See Digital Solutions July 2026 RMD Certification, *supra* note 74.

¹⁰³ See 47 CFR § 64.6305(g); *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2603, para. 58; *Global UC Removal Order*, 37 FCC Rcd at 13379, para. 8.

¹⁰⁴ *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2604-05, paras. 60-62.

¹⁰⁵ 47 CFR § 64.1200(n)(3). We note that downstream providers will be required to cease accepting traffic directly from Digital Solutions on a shorter timeframe pursuant to paragraphs 27 and 30 of this Final Determination Order and Removal Order.

consent.

32. **IT IS FURTHER ORDERED** that pursuant to section 1.102(b) of the Commission's rules, 47 CFR § 1.102(b), this Final Determination Order and Removal Order **SHALL BE EFFECTIVE** upon release.

33. **IT IS FURTHER ORDERED** that copies of this Final Determination Order and Removal Order shall be filed in EB Docket No. 22-174 and sent by certified mail, return receipt requested, to Richard Anderson, CEO, Digital Solutions Inc., 1050 Curtis Street, Denver, CO 80202, and by email to support@gdstelecom.net.

FEDERAL COMMUNICATIONS COMMISSION

Hunter P. Deeley
Chief
Enforcement Bureau