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

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

INITIAL DETERMINATION ORDER AND ORDER TO SHOW CAUSE

Adopted: June 29, 2026 **Released: June 29, 2026**

By the Chief, Enforcement Bureau:

I. INTRODUCTION

1. By this Initial Determination Order and Order to Show Cause (Order), the Enforcement Bureau (Bureau) issues its initial determination 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 for voice service providers. This Order follows the Bureau's April 2, 2026, Notification of Suspected Illegal Traffic and Additional Notification of Robocall Mitigation Database (RMD) Certification Deficiency (Digital Solutions Notice or Notice).[2] Digital Solutions now has 14 days to respond to the Order with a final response to the Bureau's initial finding and to demonstrate compliance with the Commission's rules.[3] If Digital Solutions fails to provide an adequate response within 14 days or continues to originate onto the U.S. network substantially similar illegal traffic, the Bureau will issue a Final Determination Order.[4] Any provider immediately downstream from Digital Solutions will then be required to block and cease accepting all traffic received directly from Digital Solutions beginning 30 calendar days after release of the Final Determination Order.[5] In addition, this Order directs Digital Solutions to show cause as to why it should not be removed from the Commission's RMD for failing to authenticate all Session Initiation Protocol (SIP) calls it originates on its network, contrary to its certification in the RMD. Failure to cure this deficiency within 14 days will result in removal of the Company's certification from the RMD, in which case all voice service providers and intermediate providers will be required to cease accepting calls directly from Digital Solutions.[6] This Order follows the Bureau's April 2, 2026, Notification of Suspected Illegal Traffic and Additional Notification of Robocall Mitigation Database Certification Deficiency (Digital Solutions Notice or Notice).

---

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

[3] 47 CFR § 64.1200(n)(2)(ii).

[4] *Id.* § 64.1200(n)(2)(iii).

[5] *Id.* § 64.1200(n)(3).

[6] 47 CFR § 64.6305(g); *Call Authentication Trust Anchor*, WC Docket No. 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, 38 FCC Rcd 2573, 2604, para. 60 (2023) (*Sixth Caller ID Authentication Order)*.

II. BACKGROUND

A. Voice Service Provider Mandatory Blocking Rules[7]

2. Protecting consumers in the United States from the dangers and risks of unwanted and illegal robocalls is the Commission's top consumer protection priority.[8] Voice service providers can—and sometimes do—facilitate, or even protect, bad-actor callers.[9] When bad-actor callers are shielded by bad-actor voice service providers, it is significantly more difficult to stop the calls.[10] To address the problem, the Commission requires voice service providers to block illegal traffic in some cases.[11] 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.[12] On May 18, 2023, the Commission expanded the mandatory call blocking framework created in the *Gateway Provider Order* to all voice service providers.[13]

3. Mandatory call blocking pursuant to sections 64.1200(n)(2) and (n)(3) can entail a three-step process if the notified provider fails to take action as directed by the Bureau.[14] *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.[15] *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.[16] The provider then has an opportunity to respond.[17] *Third*, if the Bureau determines that the provider's response to the Initial Determination Order is inadequate (including

---

[7] 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.

[8] FCC, *Stop Unwanted Robocalls and Texts*, https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts (last visited Apr. 28, 2026) (explaining that "Unwanted calls – including illegal and spoofed robocalls – are the FCC's top consumer complaint and our top consumer protection priority.").

[9] *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*).

[10] *Id.*

[11] *Id.* at 5415, para. 29.

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

[13] *Seventh Call Blocking Order*, 37 FCC Rcd at 5415-17, paras. 29-36 (requirements codified at 47 CFR § 64.1200(n)(2)-(3)).

[14] 47 CFR § 64.1200(n)(2)-(3).

[15] *Id.* § 64.1200(n)(2)(i)(A).

[16] *Id.* § 64.1200(n)(2)(ii).

[17] *Id.*

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.[18] Downstream providers may choose to initiate blocking sooner than 30 calendar days from the release of the Final Determination Order if, prior to initiating blocking, they provide the Commission with notice and a brief summary of the basis for their determination that the provider failed to effectively mitigate illegal traffic within 48 hours of being notified by the Commission or failed to implement effective measures to prevent new and renewing customers from using its network to originate illegal calls.[19]

B. RMD Rules and Removal Procedure

4. The FCC established the RMD in 2021 to promote transparency and effective robocall mitigation.[20] Voice service providers, gateway providers, and non-gateway intermediate providers must file a certification in the RMD.[21] 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 processing illegal robocall traffic as part of its robocall mitigation program.[22] 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.[23] 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.[24] 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.[25] The submission of false or inaccurate information makes a certification deficient and may result in an enforcement action against the filer, including

[18] *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).

[19] 47 CFR § 64.1200(n)(2)(iii); *see id.* § 64.1200(k)(4).

[20] *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).

[21] 47 CFR § 64.6305(d), (e), (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 our 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).

[22] 47 CFR § 64.6305(d)(2)(ii), (e)(2)(ii), (f)(2)(ii) (requiring the description to include how it 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).

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

[24] *Id.* § 64.6305(d)(2)(iii), (e)(2)(iii), (f)(2)(iii).

[25] *Id.* § 64.6305(d)(3)(ii), (e)(3)(ii), (f)(3)(ii); *id.* § 1.16; *see also Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2595, para. 42.

removal of the filing from the RMD.[26]

5. The Commission may remove a provider's filing from the RMD that it finds "deficient in some way."[27] 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.[28] 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.[29] 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 order removing the provider from the RMD.[30]

6. 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.[31] 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.[32]

C. Digital Solutions' Origination of Suspected Illegal Robocalls and RMD Certification Deficiencies

7. The Bureau identified 51 calls placed to wireless telephone numbers between May 6, 2025, and July 8, 2025, that featured prerecorded messages and were placed without the requisite consent of the called party, in apparent violation of section 227(b)(1)(A) of the Communications Act of 1934, as

[26] *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*, 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)).

[27] *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).

[28] *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2604, para. 60.

[29] *Id.* (quoting *Global UC Inc*, Removal Order, 37 FCC Rcd 13376, 13378, para. 5 (EB 2022) (*Global UC Removal Order*)).

[30] *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2604, para. 60.

[31] 47 CFR § 64.6305(g).

[32] *See id.*

amended, and the Commission's rules.[33] Nineteen of the 51 identified calls told recipients that they were "prequalified" or "eligible" for financial relief programs purporting to be from someone on a "loan processing team."[34] The message told the recipient to "press '2'" to "speak with someone from underwriting" to "finalize" the terms of the loan.[35]

8. The Industry Traceback Group (ITG) investigated the identified calls and determined that Digital Solutions originated the suspected illegal robocalls.[36] The ITG notified Digital Solutions of these calls and 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."[37] The traceback requests directed Digital Solutions to investigate the suspected illegal traffic and "[i]f, in investigating the call, the end user originating the traffic claims that the traffic complies with applicable U.S. laws and regulations, provide the identity of the end user, a description of the traffic, and the basis of the claim that the traffic complies with U.S. laws and regulations."[38] Digital Solutions confirmed that it originated the calls and identified three of its customers as the sources of all of the calls.[39]

9. On April 2, 2026, the Bureau sent the Notice to Digital Solutions via certified mail.[40] 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.[41] The Digital Solutions Notice directed the Company to take the following actions: (i) promptly investigate the identified suspected illegal traffic; (ii) block the identified traffic within 14 days (and continue to block the identified traffic as well as substantially similar traffic on an ongoing basis) unless it determined that the traffic was not illegal; and (iii) report the results of the Company's investigation to the Bureau within 14 days.[42] The Notice also included specific instructions for the report. If the Company's investigation did not conclude that the identified traffic was legal, the report had to include (i) a certification that the Company was blocking the identified traffic and would continue to do so, and (ii) a description of the Company's plan to identify and block or cease accepting substantially similar traffic on an ongoing basis.[43] The Notice warned Digital Solutions that a failure to comply with those obligations could result in the Bureau requiring all immediate downstream providers to block its traffic pursuant to sections 64.1200(n)(2) and (3) of the Commission's rules.[44] The Notice further warned Digital Solutions that failure to respond to the Notice would be grounds for issuing an initial determination order, and ultimately could lead to issuance of a final determination order that would require all downstream providers to block and cease accepting traffic directly from the Company.[45]

---

[33] *Id.* at 1 & Attachment A (identifying calls that the Company originated); 47 U.S.C. § 227(b)(1)(A) (requiring callers obtain consent before placing certain types of pre-recorded calls); 47 CFR § 64.1200(a)(1)-(2) (same).

[34] Digital Solutions Notice at 1.

[35] *Id.*

[36] *Id.* at 2.

[37] *Id.*

[38] *Id.*

[39] ITG Subpoena Response (Nov. 17, 2025) (on file at EB-TCD-25-00039386) (ITG Subpoena Response).

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

[41] Email from Enforcement Bureau, FCC, to Richard Anderson, Digital Solutions (Apr. 2, 2026, 10:03 AM EDT) (on file at EB-TCD-25-00039386).

[42] Digital Solutions Notice at 5; *see also* 47 CFR § 64.1200(n)(2)(i)(A).

[43] *Id.*

[44] *Id.*

[45] *Id.* at 5-6; *see also* 47 CFR § 64.1200(n)(2)(ii)-(iii), (3).

10. The Notice also identified two deficiencies related to the truthfulness and accuracy of its certification: (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 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 latter, the Notice explained that in August 2025 Digital Solutions did not authenticate the calls identified in Attachment B that it originated despite having certified that all calls originating on its network are authenticated in compliance with section 64.6301.[47] It also noted that "[t]his failure to authenticate all calls that it originates indicates that Digital Solutions' certification of 'Complete STIR/SHAKEN Implementation' in the RMD is inaccurate, and thus its certification is deficient." The Notice then explained how the Company could cure these two deficiencies:

> To cure these deficiencies, we direct Digital Solutions to (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 [10] calls.[48]

11. On April 3, 2026, the Company filed a revised robocall mitigation plan in the RMD. The revised document states that "DIGITAL SOLUTIONS INC. has fully implemented the STIR/SHAKEN caller authentication framework across its IP-based network."[49]

12. On May 5, 2026, Digital Solutions responded to the Commission 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."[50] Digital Solutions further claimed that "[w]ith regards to the clerical matters in the RMD database we have already taken action and addressed the issues in the RMD."[51] Digital Solutions did not provide any other information required by the Notice, including the results of its investigation of the suspected illegal traffic, its plan to block substantially similar illegal traffic on an ongoing basis, and an explanation as to why the Company did not authenticate the calls listed in Attachment B that it had originated, despite certifying that all calls originating on its network are authenticated in compliance with section 64.6301.

---

[46] *See* Digital Solutions Notice at 3.

[47] *See id*. at 6 & Attach. B.

[48] *Id.* at 6. Ten calls are listed in Attachment B to the Notice.

[49] Digital Solutions Inc (No. RMD0027372), Fed. Commc'ns Comm'n, Robocall Mitigation Database, https://fccprod.servicenowservices.com/rmd?id=rmd_form&table=x_g_fmc_rmd_robocall_mitigation_database&sys_id=4a11fac887b8e650e1cc75d9cebb3518&view=sp (filed Apr. 3, 2026) (Digital Solutions RMD Certification), Attachment at 1 (attachment can be viewed by clicking on the "Download PDF" button) (on file at EB-TCD-25-00039386).

[50] Email from DavidA@gdstelecom.net, signed as "Digital Solutions Inc Compliance Dept", to Enforcement Bureau, FCC (May 5, 2026, 9:49 PM EDT) (on file at EB-TCD-25-00039386) (Digital Solutions May 5 email).

[51] *Id.*

III. DISCUSSION

A. Digital Solutions May Be Subject to Mandatory Call Blocking

13. The Company is in apparent violation of section 64.1200(n)(2) of our rules because Digital Solutions has not provided a complete response to the Notice. Although the Company's May 5 email response claims that it is in compliance with our rules, the Company did not fully comply with the instructions in the Notice relating to section 64.1200(n)(2). Even if Digital Solutions completed an investigation into the identified traffic (which the email implies it did a "long time ago"), the Company failed to report the results of this investigation to the Bureau. The Company's email does not state whether it concluded that the calls were illegal. It states that the Company "vacated those customer profiles and as a result we have been compliant and without any complaint for over 9 months,"[52] which suggests that the Company terminated the customers who were responsible for the identified calls. However, the Company failed to include a certification that it is blocking the identified traffic and will continue to do so, as required by the Notice.[53] The Company also failed to explain how it plans to identify and block similar traffic on an ongoing basis, which again was required by the Notice.[54] Therefore, the Company's response to the Notice is insufficient.

14. Given the insufficiency of the Company's response, the Bureau now issues this Initial Determination Order and directs Digital Solutions to file a final response before the Bureau makes a final determination on whether the Company is in compliance with section 64.1200(n)(2). The response must include the specific information enumerated on page 5 of the Notice.[55] Digital Solutions shall file its response with the Bureau within 14 calendar days of the date of this Initial Determination Order. Failure to respond to this Initial Determination Order or submit the information enumerated on page 5 of the Notice will result in the Bureau issuing a Final Determination Order.[56] The Final Determination Order will be published in EB Docket No. 22-174 and serve as notification to all immediate downstream providers that they must block and cease accepting all traffic received directly from Digital Solutions beginning 30 days after release of the Final Determination Order.[57]

B. Digital Solutions' RMD Certification Remains Deficient

15. We find that the Company's April 3, 2026 revisions to its robocall mitigation plan have cured the first RMD certification deficiency identified in the Notice concerning full implementation of the STIR/SHAKEN framework.[58] However, although the Company's May 5 email states that it has "addressed the issues in the RMD," we see no evidence that the Company has taken any action to cure the second certification deficiency identified in the Notice, namely that while the Company has certified that it authenticates the caller ID information for all SIP calls it originates on its network, ITG traceback data indicates that it has not done so for at least the calls identified in Attachment B to the Notice. The Notice directed the Company that, in order to cure this second deficiency, it must "provide authentication information for the calls listed in Attachment B . . . and explain why it did not provide authentication information for each of the . . . calls."[59] The Company's May 5 email response did neither.

16. Accordingly, the Bureau directs Digital Solutions to cure this remaining deficiency or explain why the Bureau should not remove the Company's certification from the RMD. This Order

---

[52] Digital Solutions May 5 email.

[53] *See* Digital Solutions Notice at 5; *see also* 47 CFR § 64.1200(n)(2)(ii)(A)(1).

[54] *See* Digital Solutions Notice at 5; *see also* 47 CFR § 64.1200(n)(2)(ii)(A)(2)

[55] *See* Digital Solutions Notice at 5; *see also* 47 CFR § 64.1200(n)(2)(ii).

[56] *Id.* § 64.1200(n)(2)(iii).

[57] *Id.* § 64.1200(n)(3).

[58] *See supra* para. 11.

[59] Digital Solutions Notice at 6.

affords Digital Solutions a final opportunity to cure its deficiency by responding fully to the Notice in accordance with its certification and the Commission's rules.[60] Alternatively, the Company may explain why its certification is not deficient.

17. Digital Solutions shall file its response with the Bureau within 14 calendar days of the date of this Order.[61] Failure 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 and accompanying filing.[62] Removal of Digital Solutions' certification from the RMD will require all voice service providers, gateway providers, and intermediate providers to cease accepting calls directly from Digital Solutions.[63] If Digital Solutions' certification is removed from the RMD, it shall not be permitted to refile unless and until both the Bureau and the Commission's Wireline Competition Bureau consent.

IV. ORDERING CLAUSES

18. 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)(2) of the Commission's rules, 47 CFR §§ 0.111, 0.311, 1.1, 1.102(b)(1), 64.1200(n)(2), and the *Sixth Caller ID Authentication Order*,[64] Digital Solutions Inc. **SHALL FILE** any written final response to this Initial Determination Order and Show Cause Order **within 14 calendar days** from the release date of this Initial Determination Order and Show Cause Order. The response must include the specific information identified in paras. 15 and 16 above.[65]

19. Any response must be mailed to the Office of the Secretary, Federal Communications Commission, 45 L Street NE, Washington, DC 20554, ATTN: Enforcement Bureau – Telecommunications Consumers Division. The response must also be emailed to Daniel Stepanicich, Division Chief, Telecommunications Consumers Division, at Daniel.Stepanicich@fcc.gov, and Samuel Hanks, Attorney Advisor, Telecommunications Consumers Division, at Samuel.Hanks@fcc.gov.

20. **IT IS FURTHER ORDERED** that, pursuant to section 1.102(b)(1) of the Commission's rules, 47 CFR § 1.102(b)(1), this Initial Determination Order and Order to Show Cause **SHALL BE EFFECTIVE** upon release.

21. **IT IS FURTHER ORDERED** that copies of this Initial Determination Order and Order to Show Cause 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.

[60] *See* 47 CFR § 64.6301; *see also Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2604, para. 60.

[61] *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2604, para. 60.

[62] *Id.*

[63] 47 CFR § 64.6305(g).

[64] *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2604, paras. 60-62.

[65] 47 CFR § 64.1200(n)(2)(ii).

FEDERAL COMMUNICATIONS COMMISSION

_____
Patrick Webre
Chief
Enforcement Bureau