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

In the Matter of	)	
	)	
National Cloud Communications, LLC	)	EB-TCD-23-00034928
	)	

ORDER

Adopted: October 16, 2023 **Released: October 16, 2023**

By the Chief, Enforcement Bureau:

I. INTRODUCTION

1. By this Order, we direct National Cloud Communications, LLC (National Cloud or Company) to demonstrate why the Enforcement Bureau of the Federal Communications Commission (Commission or FCC) should not remove National Cloud from the Robocall Mitigation Database. National Cloud's robocall mitigation plan does not satisfy the Commission's rules requiring voice service providers describe the specific reasonable steps they have taken to avoid originating illegal robocall traffic and is therefore apparently deficient. **Removal from the database would require all intermediate providers and terminating voice service providers to cease accepting the Company's traffic.[1] If that were to occur, intermediate providers and voice service providers would be required to block *all* calls from the Company.** National Cloud must provide its response to the Enforcement Bureau no later than October 30, 2023.

II. BACKROUND

A. Robocall Mitigation Database Requirements

2. Protecting Americans from the dangers of unwanted and illegal robocalls is the Commission's top consumer protection priority.[2] As part of the Commission's multipronged approach to combatting illegal robocalls, the Commission has mandated adoption of the Secure Telephony Identity Revisited/Signature-based Handling of Asserted Information using toKENs (STIR/SHAKEN) caller ID authentication framework.[3] The Commission extended the implementation deadline for certain voice

[1] *Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, 36 FCC Rcd 1859, 1903, para. 83 and 1904, para. 86 (2020) (*Second Caller ID Authentication Order*); *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, 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, 6882-83, paras. 40, 44 (May 20, 2022) (*Gateway Provider Order*); 47 CFR § 64.6305(g).

[2] The Commission receives more complaints about unwanted and illegal calls than any other issue. *See* FCC, *Consumer Complaint Data Center*, https://www.fcc.gov/consumer-help-center-data (last visited Aug. 22, 2023).

[3] *Call Authentication Trust Anchor, Implementation of TRACED Act Section 6(a)—Knowledge of Customers by Entities with Access to Numbering Resources*, WC Docket Nos. 17-97 and 20-67, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3241 (Mar. 31, 2020) (*First Caller ID Authentication Report and Order and Further Notice*); *see also Gateway Provider Order*, 37 FCC Rcd at 6886-87, para. 51 (expanding STIR/SHAKEN requirements to gateway providers); *Call Authentication Trust Anchor*, WC Docket No. 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, FCC 23-18, at 8-9, para. 15 (Mar. 17, 2023)

(continued….)

service providers[4] on the basis of undue hardship or material reliance on a non-Internet Protocol (IP) network.[5] Voice service providers that received an extension were required to implement a robocall mitigation program to prevent unlawful robocalls from originating on their networks.[6] Furthermore, all voice service providers were required to file certifications with the Commission, stating whether their traffic is authenticated with STIR/SHAKEN or subject to a robocall mitigation program.[7] Voice service providers whose traffic is subject to a robocall mitigation program must detail in a robocall mitigation plan attached to their certifications the specific reasonable steps they have taken to avoid originating illegal robocall traffic.[8]

3. In 2022, the Commission adopted rules requiring gateway providers to implement STIR/SHAKEN for foreign-originated calls made to U.S. numbers.[9] The Commission also required all gateway providers to implement a robocall mitigation program, regardless of whether they had implemented STIR/SHAKEN on their networks.[10] Like voice service providers, all gateway providers must file certifications with the Commission stating whether their traffic is authenticated with STIR/SHAKEN and must detail in their certifications the specific reasonable steps they have taken to avoid carrying or processing illegal robocall traffic as part of their mitigation programs.[11]

4. In March 2023, the Commission adopted rules extending to all providers—whether they are voice service providers, gateway providers, or non-gateway intermediate providers—the requirement to implement a robocall mitigation program, regardless of whether their traffic is authenticated with

(*Sixth Caller ID Authentication Order*) (expanding STIR/SHAKEN authentication requirements to non-gateway intermediate providers that receive an unauthenticated SIP call directly from an originating provider). The STIR/SHAKEN requirements for non-gateway intermediate providers have not yet gone into effect. *See id.* at 15, para. 27.

[4] For the purposes of the Commission's call authentication rules, "voice service provider" means a service that is interconnected with the public switched telephone network and that furnishes voice communications to an end user using resources from the North American Numbering Plan. In other words, a voice service provider is an originating or terminating provider. *See* 47 CFR § 64.6300(n); *Sixth Caller ID Authentication Order*, FCC 23-18 at 3, para. 4 n.11.

[5] *Second Caller ID Authentication Order*, *supra* note 1, at 1892-93, para. 66; Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence (TRACED Act), Pub. L. No. 116-105, 133 Stat. 3274, § 4(b)(5)(A)(i) (TRACED Act). On December 9, 2021, the Commission shortened the deadline to implement STIR/SHAKEN for non-facilities-based small voice services providers and small voice service providers of any kind suspected of originating illegal robocalls. *Call Authentication Trust Anchor*, WC Docket No. 17-97, Fourth Report and Order, 36 FCC Rcd 17840, 17844, para. 9 (2021) (*Fourth Caller Authentication Order*); *see also* TRACED Act § 4(b)(5).

[6] TRACED Act § 4(b)(5)(C)(i); 47 CFR § 64.6305(a); *Second Caller ID Authentication Order*, *supra* note 1, at 1897-98, para. 75.

[7] 47 CFR § 64.6305(d); *Second Caller ID Authentication Order*, *supra* note 1, at 1902, para. 82.

[8] 47 CFR § 64.6305(d)(2)(ii); *Second Caller ID Authentication Order*, *supra* note 1, at 1902, para. 82 (quotations omitted).

[9] *Gateway Provider Order*, *supra* note 1, at 6886-87, para. 51. A "gateway provider" is "a U.S.-based intermediate provider that receives a call directly from a foreign originating provider or foreign intermediate provider at its U.S.-based facilities before transmitting the call downstream to another U.S.-based provider." 47 CFR § 64.6300(d).

[10] *Gateway Provider Order*, *supra* note 1, at 6880, paras. 34-35; 47 CFR § 64.6305(b).

[11] 47 CFR § 64.6305(e)(1), (e)(2)(ii); *Gateway Provider Order*, *supra* note 1, at 6880-82, paras. 35-38. Gateway providers' mitigation programs must also include a description of their compliance with the know-your-upstream-provider requirements in section 64.1200(n)(4) of the rules. *See* 47 CFR § 64.6305(e)(2)(ii).

STIR/SHAKEN.[12] The Commission also expanded to all providers the requirement to file certifications in the Robocall Mitigation Database reporting: (1) the extent to which they have implemented STIR/SHAKEN authentication on their networks, and (2) the details of their robocall mitigation programs, including the specific reasonable steps they have taken to avoid originating, carrying, or processing illegal robocall traffic.[13] The expanded certification requirements are not yet in effect.[14]

5. Currently, voice service providers that have not fully implemented STIR/SHAKEN authentication on their networks pursuant to an extension granted by the Commission, and gateway providers must submit certifications to the Robocall Mitigation Database that include adequate robocall mitigation plans.[15] Provider certifications and robocall mitigation plans are publicly available in the Robocall Mitigation Database.[16]

6. Commission rules prohibit any intermediate provider or terminating voice service provider from accepting voice traffic directly from any voice service provider or gateway provider that does not appear in the Robocall Mitigation Database.[17] The Enforcement Bureau may take enforcement action, including removal of a certification from the Robocall Mitigation Database, against voice service providers or gateway providers that have deficient certifications.[18] A deficient certification includes one that fails to describe specific robocall mitigation steps as required by section 64.6305(d)-(e) of the Commission's rules.[19] Prior to removing a certification from the Robocall Mitigation Database, the Enforcement Bureau must provide notice to the originating voice service provider and allow an opportunity to cure.[20]

---

[12] *See* 47 CFR § 64.6305(a)-(c); *Sixth Caller ID Authentication Order*, *supra* note 4, at 16-20, paras. 29-34. This requirement went into effect on August 21, 2023. *See* Call Authentication Trust Anchor, 88 Fed. Reg. 40096 (June 21, 2023).

[13] *See* 47 CFR § 64.6305(d)-(f); *Sixth Caller ID Authentication Order*, *supra* note 4, at 20-21, paras. 36-37. The Commission also adopted rules requiring all providers to submit additional information regarding their robocall mitigation plans. *Id.* at 24-27, paras. 43-48.

[14] *See Sixth Caller ID Authentication Order*, *supra* note 4, at 27, para. 49. This includes requirements for voice service providers that have implemented STIR/SHAKEN to certify that their traffic is subject to an appropriate robocall mitigation plan, to be codified at 47 CFR § 64.6305(d), and for non-gateway intermediate providers to submit their initial Robocall Mitigation Database certifications, to be codified at 47 CFR § 64.6305(f).

[15] *See* 47 CFR § 64.6305(d) (voice service provider certifications); 47 CFR § 64.6305(e) (gateway provider certifications); *see also Sixth Caller ID Authentication Order*, *supra* note 4, at 27, para. 49 (effective date for new filers and those with expanded filing obligations).

[16] FCC, *Robocall Mitigation Database*, https://fccprod.servicenowservices.com/rmd?id=rmd_welcome (last visited Aug. 22, 2023).

[17] 47 CFR § 64.6305(g); *Second Caller ID Authentication Order*, *supra* note 1, at 1904, para. 86; *Gateway Provider Order*, *supra* note 1, at 6883-84, para. 44.

[18] *Second Caller ID Authentication Order*, *supra* note 1, at 1901-1902, 1906, paras. 81 and n.322, 83, 93; *Gateway Provider Order*, *supra* note 1, at 6882, para. 40.

[19] 47 CFR § 64.6305(d)(2)(ii); 47 CFR § 64.6305(e)(2)(ii); *see also Second Caller ID Authentication Order*, *supra* note 1, at 1900-02, paras. 77-82; *Gateway Provider Order*, *supra* note 1, at 6882, para. 40.

[20] *Second Call Authentication Trust Anchor Order*, *supra* note 1, at 1904-1905, para. 88; *Gateway Provider Order*, *supra* note 1, at 6882, para. 40; *see also Sixth Caller ID Authentication Order*, *supra* note 4, at 32, para. 60. We may take other enforcement actions such as requiring the voice service provider to submit more specific robocall mitigation measures or imposing a forfeiture. *Second Call Authentication Trust Anchor Order*, *supra* note 1, at 1903, para. 83; *Gateway Provider Order*, *supra* note 1, at 6882, para. 40; *see also Sixth Caller ID Authentication Order*, *supra* note 4, at 32-39, paras. 59-73 (establishing an expedited process for provider removal for facially deficient certifications and adopting rules that would impose consequences on repeat offenders of the Commission's robocall mitigation rules).

B. National Cloud's Deficient Certification

7. National Cloud filed a Robocall Mitigation Database certification on September 17, 2021.[21] National Cloud certified that it has not implemented the STIR/SHAKEN authentication framework on any portion of its network, and all of the calls that originate on its network are subject to a robocall mitigation program.[22] The robocall mitigation plan attached to its certification was a document titled "Windows Printer Test Page" that was unrelated to robocall mitigation.[23] The FCC's Wireline Competition Bureau (Wireline Bureau) contacted the Company on January 28, 2022, to inform it that its robocall mitigation program attachment contained with its certification may have been uploaded in error because it did not satisfy the Commission's rules requiring it to describe its robocall mitigation efforts.[24] The Wireline Bureau's notice asked National Cloud to upload a revised attachment that complied with the Commission's rules. The Wireline Bureau did not receive a response from National Cloud acknowledging or addressing this notice, and the Company did not correct the identified deficiencies in its certification.

III. DISCUSSION

8. Our review of the evidence finds that National Cloud apparently has filed a deficient Robocall Mitigation Database certification. The Company certified that it is subject to a robocall mitigation program,[25] but it failed to describe specific reasonable steps that the Company is taking to prevent the origination of illegal robocall traffic.[26] The Company's public mitigation plan does not offer any specific mitigation steps. Rather, it is a document titled "Windows Printer Test Page" that is unrelated to robocall mitigation. Because the mitigation plan does not provide the specific reasonable steps the voice service provider has taken to avoid originating illegal robocall traffic as part of its robocall mitigation program, it is insufficient under section 64.6305(d)(2)(ii) of the Commission's rules.[27] Moreover, National Cloud did not respond or take any corrective action after the Wireline Bureau informed the Company of errors or the apparent deficiencies in its certification.[28]

9. Accordingly, we direct National Cloud to explain why the Enforcement Bureau should not remove the Company's certification from the Robocall Mitigation Database.[29] This Order affords National Cloud notice and an opportunity to cure any deficiencies in its robocall mitigation program description or explain why its certification is not deficient.

10. National Cloud shall file its response with the Enforcement Bureau within fourteen (14) calendar days of the date of this Order.[30] Failure to respond and correct the deficiency, or provide a

---

[21] National Cloud Communications, LLC, Robocall Mitigation Database, FCC (Sept. 17, 2021), https://fccprod.servicenowservices.com/rmd?id=rmd_form&table=x_g_fmc_rmd_robocall_mitigation_database&sys_id=cf4059571be630507ccf20ecac4bcbb9&view=sp (Robocall Mitigation Database Filing).

[22] *Id.*

[23] *Id.*

[24] Email from Wireline Competition Bureau to National Cloud (Jan. 28, 2022) (Warning Notice). *See also* Exhibit A.

[25] *See* Robocall Mitigation Database Filing (attesting that the Company has no STIR/SHAKEN implementation and is performing robocall mitigation).

[26] *See* 47 CFR § 64.6305(d)(2)(ii); *Second Caller ID Authentication Order*, *supra* note 1, at 1902, para. 82.

[27] 47 CFR § 64.6305(d)(2)(ii); *Second Caller ID Authentication Order*, *supra* note 1, at 1903, para. 83.

[28] *See* Warning Notice.

[29] *See Second Caller ID Authentication Order*, at 1903, para. 83 ("Enforcement Actions may include, among others, removing a defective certification from the database after providing notice to the voice service provider and an opportunity to cure the filing . . . .").

[30] *See Sixth Caller ID Authentication Order*, *supra* note 4, at 32, para. 60.

sufficient explanation for why National Cloud should retain its certification in the Robocall Mitigation Database will result in removal of the certification and accompanying filing.[31] **Removal of National Cloud's certification from the Robocall Mitigation Database will require any intermediate providers and terminating voice service providers to cease accepting calls from the Company.**[32] If National Cloud is removed from the Robocall Mitigation Database, the Company shall not be permitted to refile until the Wireline Bureau and the Enforcement Bureau determine that National Cloud has addressed and resolved any deficiencies in its Robocall Mitigation Database certification.

IV. ORDERING CLAUSES

11. 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), 64.1200, and 64.6305 of the Commission's rules, 47 CFR §§ 0.111, 0.311, 1.1, 1.102(b)(1), 64.1200, 64.6305; and the *Second Caller ID Authentication Order*,[33] National Cloud **SHALL FILE** a written response to this Order **within fourteen (14) calendar days** from the release date of this Order.

12. The written response must either inform the Enforcement Bureau that National Cloud has corrected the deficiencies in its Robocall Mitigation Database certification or explain why its certification should not be removed from the Robocall Mitigation Database.

13. The 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 e-mailed to Kristi Thompson, Division Chief, Telecommunications Consumers Division, at kristi.thompson@fcc.gov, and Alexander Hobbs, Attorney Advisor, Telecommunications Consumers Division, at alexander.hobbs@fcc.gov.

14. **IT IS FURTHER ORDERED** that copies of this Order shall be sent by email and registered mail, return receipt requested, to: 1505 Wallace Drive #154, Carrollton, TX 75006.

FEDERAL COMMUNICATIONS COMMISSION

Loyaan A. Egal
Chief
Enforcement Bureau

[31] *See id.*

[32] 47 CFR § 64.6305(g); *Second Caller ID Authentication Order*, *supra* note 1, at 1904, para. 86.

[33] *Second Caller ID Authentication Order*, *supra* note 1, at 1902, 1903, paras. 81 and n.322, 83.

EXHIBIT A