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

In the Matter of	)	
	)	
	)	
China Mobile Hong Kong Company Limited	)	EB-TCD-25-00039513

ORDER

Adopted: December 8, 2025 **Released: December 8, 2025**

By the Chief, Enforcement Bureau:

I. INTRODUCTION

1. By this Order, the Enforcement Bureau (Bureau) of the Federal Communications Commission (Commission or FCC) directs China Mobile Hong Kong Company Limited (CMHK or the Company) to (1) cure the deficiencies in its Robocall Mitigation Database (RMD) certification and notify the Bureau that the deficiencies have been cured, or to file a response explaining why the Bureau should not remove the Company's certification from the RMD; and (2) explain why CMHK's inclusion in the RMD is not contrary to the public interest. **Removal of CMHK's certification from the RMD would require all intermediate providers and voice service providers to cease accepting all calls directly from CMHK that use North American Numbering Plan (NANP) resources that pertain to the United States.**[1] CMHK must provide its response to this Order to the Bureau no later than 14 days after the release of this Order.[2]

II. BACKGROUND

2. *RMD Certification Requirements*. The FCC established the RMD in 2020 to promote transparency and effective robocall mitigation.[3] In order to have U.S.-based providers accept their voice traffic that uses U.S. NANP resources in the caller ID field, foreign voice service providers must comply with the same RMD certification requirements as U.S. voice service providers.[4] On March 16, 2023, the Commission adopted amendments to section 64.6305 of its rules in the *Sixth Caller ID Authentication Order* that enhanced the information requirements for RMD certifications and expanded the obligation to submit a robocall mitigation plan for new and existing filers.[5] On May 18, 2023, the Commission adopted additional amendments to section 64.6305 in the *Seventh Call Blocking Order* that required all providers to include a commitment to respond fully to traceback requests within 24 hours in their RMD

[1] *See* 47 CFR § 64.6305(g)(2).

[2] *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*).

[3] *Call Authentication Trust Anchor*, WC Docket No. 17-97, Second Report and Order, 36 FCC Rcd 1859, 1902, para. 82 (2020) (*Second Caller ID Authentication Order*).

[4] *Id.* at 1906, para. 93. "The term 'foreign voice service provider' refers to any entity providing voice service outside the United States that has the ability to originate voice service that terminates in a point outside that foreign country or terminate voice service that originates from points outside that foreign country." 47 CFR § 64.6300(c).

[5] *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2592-2601, paras. 36-52.

certifications.[6] Both of these rule amendments took effect on February 26, 2024, and required all existing filers to update their RMD certifications to provide the newly-required information and newly-required or updated robocall mitigation plans by that same date.[7]

3. Under the amended rule, voice service providers, gateway providers, and non-gateway intermediate providers must submit several pieces of information in their RMD certifications.[8] *First*, a provider must certify that all calls that it originates on its network are subject to a robocall mitigation program, that any prior certification has not been removed by Commission action and it has not been prohibited from filing in the RMD, and whether it has fully, partially, or not implemented STIR/SHAKEN on the Internet Protocol portions of its network.[9] *Second*, the provider must upload a robocall mitigation plan that describes the specific reasonable steps the provider has taken to avoid originating, carrying, or processing illegal robocall traffic as part of its robocall mitigation program based on the role(s) it serves in the call chain,[10] including: (a) a description of the effective measures it is taking to prevent new and renewing customers from originating illegal robocalls (if it is a voice service provider); (b) a description of any call analytic system(s) that it utilizes, including those operated by a third-party vendor; and (c) a description of the procedures it is using to know its upstream providers.[11] *Third*, the provider must provide its business name, address, and other identifying information, including contact information for a person responsible for addressing robocall mitigation-related issues, and its principals, affiliates, subsidiaries, and parent companies.[12] *Fourth*, the provider must include certain other information, including: (a) the role it is playing in the call chain; (b) detailed information supporting any claimed STIR/SHAKEN implementation extension or exemption; (c) a statement whether it or any affiliated entity has been subject to a Commission or other law enforcement agency action or investigation in the prior two years due to suspected involvement with illegal robocalling or spoofing, or due to a deficiency in its RMD certification; and (d) the provider's commitment to respond fully to traceback requests within 24 hours.[13]

---

[6] *Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97, Seventh Report and Order 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, 5422, para. 52 (2023) (*Seventh Call Blocking Order*).

[7] *See Wireline Competition Bureau Announces Robocall Mitigation Database Filing Deadlines and Instructions and Additional Compliance Dates*, WC Docket No. 17-97, Public Notice, 39 FCC Rcd 383, 383-87 (WCB 2024) (*RMD Public Notice*); Fed. Commc'ns Comm'n, *Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor*, 89 Fed. Reg. 4833, 4833 (Jan. 25, 2024) (establishing February 26, 2024 as the effective date for the amendments to section 64.6305).

[8] The *Sixth Caller ID Authentication Order* amended section 64.6305 to require non-gateway intermediate providers to file certifications in the RMD for the first time. *See* 47 CFR § 64.6305(f); *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2593, para. 38; *RMD Public Notice*, 39 FCC Rcd at 384.

[9] 47 CFR § 64.6305(d)(1), (e)(1), (f)(1); *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2595, para. 42; *id*. at 2597, para. 46; *RMD Public Notice*, 39 FCC Rcd at 385.

[10] *See Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2593, para. 39; *RMD Public Notice*, 39 FCC Rcd at 385, 388.

[11] 47 CFR § 64.6305(d)(2)(ii), (e)(2)(ii), (f)(2)(ii); *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2593-95, paras. 40-41; *RMD Public Notice*, 39 FCC Rcd at 386-87.

[12] 47 CFR § 64.6305(d)(4), (e)(4), (f)(4); *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2595-96, 2597, 2599, paras. 42-43, 46, 48; *RMD Public Notice*, 39 FCC Rcd at 385-86.

[13] 47 CFR §§ 64.6305(d)(2)(i), (iii), (iv), 64.6305(e)(2)(i), (iii), (iv), 64.6305(f)(2)(i), (iii), (iv); *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2596-99, paras. 43-47; *RMD Public Notice*, 39 FCC Rcd at 385-86.

4. The Bureau may remove a certification from the RMD that is deficient.[14] To do so, the Commission first contacts the provider, notifying it that its certification is deficient, explaining the nature of the deficiency, and giving the provider an opportunity to cure the deficiency.[15] If the provider fails to cure the deficiency, the Bureau will release an order finding that a provider's certification is deficient based on the available evidence and direct the provider to, within 14 days, cure the deficiency in its certification and notify the Bureau that the deficiency has been cured, or explain why the Bureau should not remove the provider's certification from the RMD.[16] If the provider fails to cure the deficiency or provide a sufficient explanation why its certification is not deficient within that 14-day period, the Bureau will release an order removing the provider's certification from the RMD.[17]

5. Following the February 26, 2024, effective date of the amendments to section 64.6305, the Wireline Competition Bureau (WCB) conducted a review of certifications in the RMD and identified that CMHK had failed to update its RMD certification (including its robocall mitigation plan) with the newly required information by that date to comply with section 64.6305, as amended. WCB notified CMHK on March 29, 2024, that its certification was noncompliant with section 64.6305 because the Company had failed to submit an updated RMD certification and updated robocall mitigation plan by the February 26, 2024 deadline.[18] WCB's notification informed CMHK that it "must submit an updated certification and updated robocall mitigation plan in the Robocall Mitigation Database by Monday, April 29, 2024."[19] After this second deadline, CMHK still had not updated its RMD certification and robocall mitigation plan with the required information; as a result, WCB referred CMHK to the Bureau to initiate removal proceedings.

6. CMHK is a foreign voice service provider located in Hong Kong and is a wholly owned subsidiary of China Mobile Limited (CML).[20] Seventy percent of CML is owned by China Mobile Hong Kong (BVI), which, through its parent entity, is wholly owned by China Mobile Communications Corporation (China Mobile).[21] China Mobile is a Chinese state-owned company subject to the

[14] 47 CFR § 0.111(a)(28)(i); *see Second Caller ID Authentication Order*, 36 FCC Rcd at 1902-03, para. 83 (voice service provider certifications); *id*. at 1906, para. 93 (foreign voice service providers); *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, 6882, para. 40 (2022) (*Gateway Provider Order*) (gateway provider certifications); *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2602-03, paras. 56-57 (non-gateway intermediate provider certifications).

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

[16] *Id*.

[17] *Id.*

[18] E-mail from Robocall Mitigation Database Team (Mar. 29, 2024) (on file in EB-TCD-25-00039513) (WCB E-mail).

[19] *Id.*

[20] China Mobile Hong Kong Company Limited (RMD0007000), Fed. Commc'ns Comm'n, Robocall Mitigation Database (filed Sep. 24, 2021) https://fccprod.servicenowservices.com/rmd?id=rmd_form&table=x_g_fmc_rmd_robocall_mitigation_database&sys_id=52b45c691b327410822320efe54bcb39&view=sp (CMHK RMD Certification).

[21] *China Mobile International (USA) Inc., Application for Global Facilities-Based and Global Resale International Telecommunications Authority Pursuant to Section 214 of the Communications Act of 1934, as Amended*, ITC-214-20110901-00289, Memorandum Opinion and Order, 34 FCC Rcd 3361, 3363-64, para. 3 (2019) (*China Mobile Section 214 Order*). See China Mobile Limited, Form 20-F for the fiscal year ended December 21, 2021, at 59 (filed Apr. 28, 2022),

(continued….)

supervision of the State-Owned Assets Supervision and Administration Commission of the State Council of the People's Republic of China, a Chinese government body.[22] In 2011, China Mobile International (USA) Inc. (China Mobile USA), another wholly owned subsidiary of CML, applied for international section 214 authorizations.[23] In 2019, the Commission denied China Mobile USA's application because it raised serious national security and law enforcement risks.[24] The Commission found it "highly likely" that China Mobile USA would "succumb to exploitation, influence, and control by the Chinese government" as "supported by [the Commission's] understanding that Chinese law requires citizens and organizations, including state-owned enterprises, to cooperate, assist, and support Chinese intelligence efforts wherever they are in the world."[25] As such, there was a significant possibility that the Chinese government's influence and control over China Mobile USA could result in computer intrusions and attacks and economic espionage.[26]

7. The FCC's decision to deny China Mobile USA's application was based in part on a filing submitted by the Executive Branch, which the Commission often consults on national security matters, recommending denial.[27] In this filing, the Executive Branch agencies noted that no mitigation measures could adequately resolve the substantial and unacceptable national security and law enforcement risks arising from China Mobile USA's anticipated operations involving interconnection with the U.S. telecommunications infrastructure and the importance and sensitivity of that infrastructure to U.S. national security and law enforcement interests.[28] On March 25, 2022, the Public Safety and Homeland Security Bureau (PSHSB) added China Mobile USA's telecommunications services associated with its application for section 214 authorizations to the FCC's Covered List.[29] The Commission is required under the Secure and Trusted Communications Networks Act (Secure Networks Act) to maintain the Covered List as a list of communications equipment and services that have been determined by certain enumerated sources, including certain national security agencies or interagency national security bodies, to "pose an unacceptable risk to the national security of the United States or the security and safety of United States persons."[30] This addition to the Covered List, as with other additions, included China Mobile USA's "subsidiaries and affiliates."[31] CMHK, as an affiliate of China Mobile USA through its shared parent company CML, is identified on the Covered List, because its telecommunications services

https://www.sec.gov/Archives/edgar/data/1117795/000119312522125601/d260521d20f.htm#tx260521_10 (last accessed Nov. 14, 2025).

[22] *China Mobile Section 214 Order*, 34 FCC Rcd at 3364, para. 3.

[23] *See id.*, para. 4.

[24] *Id.* at 3362, para. 1.

[25] *Id.* at 3369-71, paras. 17-19.

[26] *Id.* at 3372-76, paras. 21-30.

[27] *See* Executive Branch Recommendation to the Federal Communications Commission to Deny China Mobile International (USA) Inc.'s Application for an International Section 214 Authorization, File No. ITC-214-20110901-00289 (filed July 2, 2018) (Executive Branch Recommendation).

[28] *See* Executive Branch Recommendation at 7.

[29] *Public Safety and Homeland Security Bureau Announces Additions to the List of Equipment and Services Covered by Section 2 of the Secure Networks Act*, WC Docket No. 18-89, Public Notice, 37 FCC Rcd 4078, 4079-80 (PSHSB 2022) (*Covered List Public Notice*).

[30] *Id.* at 4079. *See* 47 U.S.C. § 1601; 47 CFR § 1.50003.

[31] *Covered List Public Notice*, 37 FCC Rcd at 4080.

are listed on the Covered List as posing "unacceptable risks to the national security of the United States."[32]

III. DISCUSSION

A. CMHK Failed to Update its Deficient Certification with Required Information by the Commission's Deadline

8. All voice service providers, gateway providers, and non-gateway intermediate providers had to submit compliant RMD certifications in accordance with the Commission's amendments to section 64.6305 of its rules by February 26, 2024.[33] Foreign voice service providers that had filed certifications in the RMD were subject to these same revised certification requirements.[34] WCB identified CMHK as a provider with a deficient certification because it failed to update its certification with the required information by the February 26, 2024, deadline. WCB notified the Company that its RMD certification was noncompliant with section 64.6305 because it had failed to submit an updated certification and robocall mitigation plan by February 26, 2024, and that it had until April 29, 2024, to update its certification.[35] CMHK did not update its RMD certification after WCB notified it that its certification was noncompliant. Thus, CMHK's certification is deficient because it lacks required information and an updated robocall mitigation plan.[36]

B. CMHK's Certification in the Robocall Mitigation Database is Contrary to the Public Interest.

9. CMHK poses national security risks. In 2019, the Commission found that China Mobile USA, as a subsidiary of CML, was "highly likely to succumb to exploitation, influence, and control by the Chinese government."[37] China is a foreign adversary of the United States.[38] CMHK, like China Mobile USA, is a wholly owned subsidiary of CML, which, through its parent companies, is ultimately majority owned by China Mobile, a Chinese state-owned enterprise.[39] We therefore conclude that CMHK poses similar national security concerns as China Mobile USA.[40]

10. The RMD is a crucial tool in providing transparency to industry and the public because it displays information about the company's organization (including "principals, affiliates, subsidiaries, and parent companies"), role in the call chain, implementation of STIR/SHAKEN, and robocall mitigation measures.[41] A foreign voice service provider's RMD certification is a Commission authorization and is

[32] *Id.* at 4079.

[33] 47 CFR § 64.6305(d)-(f); *see Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2599, para. 49; *RMD Public Notice*, 39 FCC Rcd at 383-84.

[34] *See Second Caller ID Authentication Order*, 36 FCC Rcd at 1906, para. 93 (stating that "foreign voice service providers that use U.S. telephone numbers to send voice traffic to U.S. subscribers must file the same certification as U.S. voice service providers in order to be listed in the database").

[35] WCB E-mail, *supra* note 18.

[36] *See Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2592-99, paras. 36-49.

[37] *China Mobile Section 214 Order*, 34 FCC Rcd at 3371, para. 19.

[38] 15 CFR § 791.4(a)(1).

[39] *China Mobile Section 214 Order*, 34 FCC Rcd at 3364, para. 3.

[40] Similarly, CMHK is an "affiliate" of China Mobile USA, so CMHK's telecommunications services subject to section 214 are listed on the FCC's Covered List as posing "unacceptable risks to the national security of the United States." *See Covered List Public Notice*, 37 FCC Rcd at 4080 ("The inclusion of these services on the Covered List extends both to subsidiaries and affiliates of the named entities.").

[41] *See* 47 CFR § 64.6305(d)-(f).

required in order for intermediate providers and voice service providers to be able accept calls directly from the foreign voice service providers that use U.S. NANP resources in the caller ID field.[42] As we have previously noted, "[w]here the Commission grants a right or privilege, it unquestionably has the right to revoke or deny that right or privilege in appropriate circumstances."[43] Therefore, "holders of these and all Commission authorizations have a clear and demonstrable duty to operate in the public interest,"[44] and we have the authority to revoke authorizations that are not in the public interest.[45] There is no question that protecting against national security threats from foreign adversaries is in the public interest.[46] The public interest is not served by allowing entities "highly likely to succumb to exploitation, influence, and control by the Chinese government," to maintain access to valuable Commission authorizations, such as an RMD certification.[47]

C. CMHK Shall Cure Its Certification and File a Response with the Bureau.

11. The Bureau may remove a deficient certification from the RMD after providing sufficient notice and opportunity to cure.[48] We direct CMHK to cure its deficient RMD certification and notify the Bureau that the deficiency has been cured or explain why the Bureau should not remove the Company's certification from the RMD.[49] This Order affords CMHK a final opportunity to cure its deficiency by updating its certification with required information and submitting an updated robocall mitigation plan.[50] We also direct CMHK to explain to the Bureau why its certification in the RMD is not a national security concern and thus not contrary to the public interest.[51] Even if CMHK cures its deficient RMD

[42] *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2608, para. 70; 47 CFR § 64.6305(g)(2).

[43] *Sixth Caller ID Authentication* Order. 38 FCC Rcd at 2608-09, para. 70.

[44] *Id*.

[45] *Id*. (describing our authority to revoke authorizations for repeated violation of our robocall mitigation rules, but on the grounds that such conduct is "wholly inconsistent with the public interest").

[46] *See* 47 U.S.C. 151; *China Telecom (Americas)*, Order on Revocation and Termination, 36 FCC Rcd 15966 (2011) (revoking the section 214(a) operating authority of China Telecom (Americas) on public interest grounds based on national security and law enforcement risks), *aff'd*, *China Telecom (Americas) Corp. v. FCC*, 57 F.4th 256 (D.C. Cir. 2023); *Pacific Networks Corp. and ComNet (USA) LLC*, Order on Revocation and Termination, 37 FCC Rcd 4220 (2022) (revoking the section 214(a) operating authority of Pacific Networks and ComNet on public interest grounds based on national security and law enforcement risks), *aff'd*, *Pacific Networks Corp. and ComNet (USA) LLC v. FCC*, 77 F.4th 1160 (D.C. Cir. 2023). *Cf. Haig v. Agee*, 453 U.S. 280, 307 (1981) ("It is obvious and unarguable that no governmental interest is more compelling than the security of the Nation.") (quotation marks and citation omitted).

[47] *See China Mobile Section 214 Order*, 34 FCC Rcd at 3369-71, paras. 17-19

[48] 47 CFR § 0.111(a)(28)(i); *see Second Caller ID Authentication Order*, 36 FCC Rcd at 1902-03, para. 83; *Gateway Provider Order*, 37 FCC Rcd at 6882, para. 40; *Sixth Caller ID Authentication Order*, 38 FCC Rcd at 2602-2603, paras. 56-57; *see also Viettel Business Solutions Co. et al.*, Order, 39 FCC Rcd 1319, 1319, para. 1 (2024) (removing certifications of 12 entities from the Robocall Mitigation Database after being provided with notice and opportunity to cure, and an opportunity to show cause as to why the provider should not be removed); *BPO Innovate*, Order, 39 FCC Rcd 130, 130, para. 1 (2024) (directing BPO Innovate to show cause within 14 days as to why the provider should not be removed from the Robocall Mitigation Database after being provided with notice and opportunity to cure).

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

[50] *Id.*

[51] The Commission is not obligated to provide CMHK additional notice of the facts or conduct which may warrant this action or provide CMHK an opportunity to demonstrate or achieve compliance with all lawful requirements because this is a matter of public interest and national security. 5 U.S.C. § 558(c).

certification, removal may still be warranted if the Company cannot offer convincing evidence that its presence in the RMD is not a threat to national security and is in the public interest.

12. CMHK shall file its response with the Bureau within fourteen (14) calendar days of the date of the release of this Order.[52] Failure to respond and correct the deficiency or provide a sufficient explanation for why the Bureau should not remove the Company's certification from the RMD will result in removal of the Company's certification.[53] Removal of CMHK's certification from the RMD will require all voice service providers and intermediate providers to cease accepting calls directly from CMHK that use NANP resources that pertain to the U.S. in the caller ID field to send voice traffic to residential or business subscribers in the U.S.[54] If CMHK is removed from the RMD, it shall not be permitted to refile unless and until both the Bureau and WCB consent.

IV. ORDERING CLAUSES

13. Accordingly, **IT IS ORDERED** that, pursuant to sections 4(i), 4(j), 227b, 251(e), and 403 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 154(i), 154(j), 227b, 251(e), and 403; and sections 0.111, 0.311, 1.1, and 64.6305 of the Commission's rules, 47 CFR §§ 0.111, 0.311, 1.1, and 64.6305, this Order is **ADOPTED.**

14. **IT IS FURTHER ORDERED** that CMHK **SHALL FILE** a written response to this Order **within fourteen (14) calendar days** from the date of release of this Order. The written response must either inform the Bureau that CMHK has corrected the deficiencies in its RMD certification or explain why its certification should not be removed from the RMD. The written response must also explain to the Bureau why CMHK's certification is not a national security concern and thus not contrary to the public interest.

15. The responses 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 responses must also be e-mailed to EnforcementBureauTCD@fcc.gov.

16. **IT IS FURTHER ORDERED** that copies of this Order shall be sent by certified mail and e-mail to the robocall mitigation contact (as certified in the RMD) for CMHK.

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

FEDERAL COMMUNICATIONS COMMISSION

Patrick Webre
Chief
Enforcement Bureau

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

[53] *See id.*

[54] 47 CFR § 64.6305(g)(2).