

China Telecom Global Robocalling Mitigation Plan

China Telecom Global Limited (“CTG”) updates its current Robocall Mitigation Plan (“RMP”) in accordance with the Federal Communications Commission’s (“Commission”) rules (47 C.F.R. §64.6305), the Commission’s recommended “Best Practices”, and the CTG Order.¹ The RMP is current as of its submission date and may be subject to change as necessary to further comply with applicable Commission regulations and requirements.

1. Overview and Summary

CTG is a Hong Kong based “Foreign Voice Service Provider” with no U.S. network.² As such, it relies on commercial agreements with U.S.-based or international carriers to terminate all voice calls in the U.S. CTG has no ability to originate or terminate voice calls in the U.S. on its own.

CTG has implemented a range of policies and practices consistent with the Commission’s requirements for a Foreign Voice Service Provider. As explained in more detail below, this RMP sets out the reasonable steps CTG undertakes to prevent the origination of illegal robocalls, including Know Your Customer and Know Your Upstream Provider procedures, relevant contractual provisions addressing robocall mitigation, and details of its analytics system.

2. Know Your Customers

CTG implements robust Know Your Customer (“KYC”) practices.

CTG’s customers must execute a Master Service Agreement (“MSA”), Service Order Form, and other contractual documents that require customers to (i) comply with applicable laws and regulatory policies, (ii) agree to work out measures to eliminate fraud and misuse related to the traffic sent to CTG, (iii) cooperate with CTG on all issues relating to fraudulent traffic, (iv) use only numbers assigned by authorized entities and transmit accurate, contractually approved caller IDs, and not alter, disguise, or misuse numbers, and (v) not engage in unauthorized call routing, spoofing traffic, or technical means to facilitate illegal voice services. CTG’s customers are also contractually required to provide valid business registration information to verify

¹ See 47 C.F.R. § 64.6301, 6305; *Call Authentication Trust Anchor*, WC Docket No. 17-97, Sixth Report and Order and Further Notice of Proposed Rulemaking, FCC 22-37, paras. 36, 40-41 (2023); *Caller ID Authentication Best Practices*, WC Docket No. 17-97, Public Notice, DA 20-1526 (2020); *In the Matter of China Telecom Global Limited*, EB-TCD-25-00039418, DA 25-1022 (2025) (“CTG Order”).

² CTG submits this certification based on the facts described herein and solely for purposes of the Commission’s robocall mitigation framework and respectfully reserves all rights concerning any further requirements from the Commission.

business legitimacy and to provide their contact information (including both commercial and technical contacts) to enable real-time and efficient communication with customers when necessary.

In addition to the contractual obligations mentioned above, CTG has adopted comprehensive credit control policies, which include pre-contractual due diligence process for new enterprises customers. This process involves conducting financial credit investigations and assessing the customers' creditworthiness.

CTG does not accept any voice traffic from customers that do not comply with the KYC practices outlined above.

3. Know Your Upstream Providers

CTG implements robust know your upstream provider practices when interconnecting with upstream providers to accept voice traffic from them. The relevant procedures for assessing upstream providers include but are not limited to:

- Requiring upstream providers to provide their company profile including business registration, business nature and type, to validate the legitimacy and healthiness of their business operations;
- Performing a screening against economic sanctions databases;
- Requiring the upstream providers to supply information on traffic destination and origination patterns as well as traffic types before accepting voice traffic; and
- Incorporating specific contractual clauses in relevant agreements that require upstream providers to comply with applicable laws and regulatory policies as well as relevant industry technical and commercial standards, and requiring them to take responsibility for preventing and stopping any illegal robocall or fraudulent calls.

4. Suspicious Call Analysis

CTG's International Voice Network Operations Center ("VNOC") provides 24/7 network traffic analysis to ensure service quality and monitor inbound and outbound voice traffic patterns to identify suspicious calls.

CTG has established and operates an in-house anti-suspicious call system to analyze suspicious call patterns coming to its network, and continuously enhances its analytical capability. CTG does not use third-party vendors to carry out the analysis.

The anti-suspicious call system uses multi-criteria models and configurable thresholds based on historical data of voice traffic patterns. The implemented analysis rules will also be reviewed and updated from time to time in order to enhance the effectiveness.

A dedicated cross-functional team, which includes experts in network operations, fraud analysis, and commercial staff, rapidly responds when threshold breaches, alarms or end-user reports of suspected robocalls occur. CTG promptly collaborates with customers, upstream providers, and downstream carriers to validate traffic legitimacy, examining caller number identification patterns, signaling data, and business use cases as necessary.

For the purpose of investigating and stopping any illegal robocallers, CTG will respond within 24 hours to any traceback requests from the Commission, law enforcement, and the industry traceback consortium, and cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls, consistent with applicable laws and regulations.³

5. Mitigation Measures

Upon identifying suspected illegal robocall traffic, whether through internal analytics, traceback requests, or law enforcement notification, CTG implements escalating robocall mitigation measures. In particular, CTG:

- Notifies implicated customers via operational channels to verify and cease non-compliant traffic immediately;
- Escalates unresolved cases to commercial and senior management for contractual enforcement;
- Analyzes ongoing suspected call traffic patterns by comparing current traffic against historical data in real-time, and issues immediate and repeated warnings to the customer/carrier in question;
- If the customer/carrier fails to mitigate the suspected illegal robocalls, restricts its service in accordance with the contract terms; and
- Applies enhanced post-mitigation review for a defined period to confirm recurrence prevention.

6. No Historical Record of Illegal Robocall Incidents

³ 47 C.F.R. §§ 64.6305(a)(2); 64.1200(n).

CTG has received no complaints or traceback requests concerning illegal robocall traffic terminating in the U.S., nor has CTG identified any illegal robocall traffic terminating in the U.S. in the past three years before the submission date of this RMP.

7. Actively Participating in Industry Forums

CTG is actively participating in GSMA's activities and other industry forums. On an ongoing basis, CTG adheres to the best industry practice guidelines as documented and released by the working groups of industry forums such as GLF (Global Leaders' Forum).

8. CTG Contact Information

Sharon Hua
Senior Carrier Relations Manager
sharonhua@chinatelecomglobal.com

9. RMP Updates

CTG anticipates that it will update this RMP as it continues to enhance and improve its robocall mitigation efforts in line with evolving industry best practices and regulatory requirements. Any material changes will be updated in the FCC Robocall Mitigation Database within ten (10) business days of such update.
