

China Unicom (Hong Kong) Operations Limited (CUHK) 'S ROBOCALL MITIGATION PROGRAM

CUHK has undertaken the following reasonable measures to avoid originating illegal robocall traffic and to mitigate robocalls throughout its network:

Know Your Customer and Know Your Upstream Provider Measures. CUHK applies affirmative and effective Know Your Customer (“KYC”) and Know Your Upstream Provider (“KYUP”) measures to prevent the origination and transit of illegal robocalls.

- When customers sign up for service, CUHK requires them to provide complete and accurate corporate information, including registered company name, business registration details, registered business address, billing information, and designated operational and commercial contact persons. All submitted information is subject to verification prior to service activation. CUHK’s agreements with customers and upstream providers require strict compliance with all applicable laws, regulations, and industry standards related to fraud prevention and robocall mitigation. Partners are contractually obligated to cooperate fully with CUHK in any investigation involving suspected fraud, misuse, or illegal robocall activity.
- CUHK expressly prohibits customers and partners from initiating or facilitating illegal robocalls. Where suspicious or illegal robocall traffic is detected, CUHK will notify the relevant customer or carrier and require immediate corrective action. Persistent or unresolved violations may result in traffic blocking, service suspension, or termination.
- CUHK refuses to accept traffic from any voice service provider, gateway provider, or applicable intermediate provider that is not listed in the Robocall Mitigation Database, in accordance with applicable regulatory requirements.

24/7 Network Monitoring. CUHK operates a global network operations function that monitors network traffic on a continuous 24/7 basis to ensure service quality, stability, and regulatory compliance. CUHK employs internal monitoring and analytics systems to analyze inbound and outbound call traffic, including high-volume traffic patterns, abnormal calling behavior, and other indicators of potentially illegal robocalls. Traffic analysis is performed using multi-layered, rule-based detection mechanisms and historical call data review. Detection rules and analytical thresholds are reviewed and updated periodically to enhance the effectiveness of monitoring controls. CUHK conducts these analytics using internal systems and operational resources.

Investigating Suspicious Traffic. CUHK maintains internal operational and commercial coordination procedures to address suspected illegal robocall activity when monitoring thresholds are exceeded or when external notifications are received. Upon identification of suspicious traffic, CUHK works expeditiously and in good faith with the relevant customer or carrier to assess the legitimacy of the traffic. This may include review of call detail records, traffic patterns, and customer explanations.

Suspending and Mitigating Illegal Traffic. When suspicious or illegal robocall traffic is identified, CUHK may take one or more of the following actions:

- a. Request the identified customer or carrier to verify the legitimacy of the traffic through established operational channels;
- b. Require the customer or carrier to immediately cease sending illegal or suspicious calls;
- c. Escalate the issue internally to commercial and management teams if the traffic cannot be promptly verified or mitigated;
- d. Block specific numbers, routes, or traffic patterns associated with the illegal activity; or
- e. Suspend or terminate service if the customer or carrier fails to mitigate the illegal robocalls within a reasonable timeframe.

Specific Measures for +1 (North American Numbering Plan) Traffic. CUHK applies additional controls to traffic associated with +1 numbering resources. CUHK permits +1-originated traffic only for customers that are properly registered in the Robocall Mitigation Database and that send legitimate retail voice traffic. CUHK blocks all +1-originated traffic from customers that are not listed in the Robocall Mitigation Database. Customer registration status is verified on an ongoing basis and during onboarding of new customers or partners.

A statement of the voice service provider's commitment to respond within 24 hours 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 originate calls. CUHK is committed to responding fully and in a timely manner, and in any event within 24 hours, to all traceback requests from regulatory authorities, law enforcement agencies, and industry traceback consortia, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls. Upon receipt of a traceback request, CUHK will take appropriate steps, which may include blocking the identified caller line identification, reviewing call detail records,

identifying the sending customer or carrier, providing the required response to the requesting entity, and taking mitigation actions as necessary.