

Robocall Mitigation Plan

China Mobile International Limited (CMI) has undertaken the following reasonable measures to avoid originating illegal robocall traffic and mitigate robocalls throughout its network:

Know Your Customer and Know Your Upstream Provider Measures

CMI uses the following affirmative, effective measures to prevent the origination or transit of illegal robocalls.

CMI employs stringent Know Your Customer and Know Your Upstream practices for its carrier customers. When customers sign up for service, they must supply their registered company name, their VAT number, their business address, and the name and contact details for several company contacts. They must also include their complete billing information. All of this information is verified by a CMI account manager before it is accepted.

CMI's agreements with its upstream providers require that the providers strictly comply with all relevant laws and regulations and cooperate fully with CMI in the case of fraud or misuse of the network.

CMI prohibits customers from initiating illegal robocalls. If CMI finds the customer initiating suspicious illegal robocalls, firstly we will warn them to stop. If such traffic is persisted, CMI tends to suspend their service.

CMI is already required to refuse traffic from any voice service provider or gateway provider that is not listed in the Robocall Mitigation Database.

Beginning on May 28, 2024, CMI will also be prohibited from accepting traffic from any non-gateway intermediate provider not listed in the Robocall Mitigation Database.

Any Analytics Systems

Monitoring

CMI's global network operation centre monitors network traffic to assure the service and quality. This is performed on a 24/7 basis.

CMI has a monitoring system to analyse network traffic, such as inbound and outbound high-volume traffic to identify suspicious call patterns. The system will regularly analyse the historical call summary in multi-layers based on pre-defined ruleset. The implemented detection rules will also be reviewed and updated from time to time in order to increase the effectiveness of the monitoring system. CMI does not use any third-party vendors to carry out these analytics.

Investigating Suspicious Traffic

CMI has a multidisciplinary group that is dedicated to collaborating in case of a threshold's control is broken and alarm is triggered or in case of a specific request.

Once suspicious traffic has been identified, CMI collaborates with customers/carriers expeditiously and in good faith to determine the legitimacy of the traffic.

Suspending/Mitigating Illegal Traffic

When the suspicious traffic has been identified on CMI's side, the following actions will be taken:

(a) Request the identified customer/carrier to verify the legitimacy of the traffic through the daily operational channel.

(b) Request the identified customer/carrier to stop sending illegal calls immediately through the daily operational channel.

(c) If the customer/carrier is still unable to determine the legitimacy of the traffic calls or unable to stop the suspicious traffic, CMI's global network operation centre will escalate the ticket internally to commercial team to push the commercial peers to resolve.

(d) If the customer/carrier fails to mitigate the illegal calls, CMI may suspend its service.

No History of Law Enforcement

CMI doesn't have a history of law enforcement actions for illegal robocalls or related state law violations. Nor has CMI been prohibited from filing in the Robocall Mitigation Database. CMI doesn't have detected abnormal traffic in the prior two years.

Traceback Request

CMI is willing to respond fully and 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.