

PCCW Global Robocall Mitigation Program

1. Overview

PCCW Global consists of a group of companies operating as (amongst other products and services) a provider of Wholesale Voice Services (“WS Voice”) to carriers around the globe. It operates as a foreign service provider and it does not connect directly to end-users of voice services at either the originating or terminating end of a voice call.¹ PCCW Global’s voice network infrastructure is all IP (Internet Protocol)-based.

PCCW Global’s parent company, HKT Limited (quoted on the HKSE, stock code 6823), does provide voice services directly to end-users, both fixed and mobile, in Hong Kong.

PCCW Global Inc., PCCW Global Limited, and PCCW Global (UK) Limited, act as foreign providers, handling US-bound traffic to US carrier vendors. PCCW Global Inc., PCCW Global Limited, and PCCW Global (UK) Limited are registered in the FCC Robocall Mitigation Database (“RMD”).²

2. Use Policy

PCCW Global publishes its acceptable use policy (“AUP”) on its website at:
<https://www.pccwglobal.com/acceptable-use-policy/>.

The AUP states that PCCW Global’s network may only be used for lawful purposes and that PCCW Global will investigate suspected abuse or illegal activity, which may lead to suspension of service to sources of abuse or illegal activity. The persistent routing of robocall traffic to US destination numbers would be a violation of the AUP.

This Policy is in addition to any restrictions or other limitations on use that a user may be subject to by virtue of any service agreement or other terms and conditions executed between a user and PCCW Global (“Service Agreement”), described in the next section.

3. Contractual Provisions with Upstream Providers

PCCW Global’s Service Agreements with other carriers define machine-generated traffic (other than from PCCW Global’s own Test Call System (“TCS”)) as Fraudulent Traffic and require that, in the provision and use of the services, the parties must comply with all relevant laws and regulations. The agreements also require the parties to cooperate on all issues related to fraud and misuse of the network. Breach of these provisions can lead to termination of the services.

¹ PCCW Global does in limited circumstances for International Toll Free Services (“ITFS”) carry voice traffic directly from the originating US ITFS carrier directly to the far end international call center customer and thus acts as a terminating foreign voice service provider in this limited case.

² PCCW Global has identified in the RMD relevant principals, affiliates, subsidiaries, and parent companies in sufficient detail to facilitate the FCC’s ability to determine whether it has been prohibited from filing in the RMD. It has not included in this list, for example, intermediate holding companies that have no operations or foreign affiliates that do not provide service in the US. PCCW affirms that none of these intermediate holding companies or foreign affiliates have been prohibited from filing in the RMD.

Extracts of the relevant contractual provisions are set out below for reference:

“4.5 FRAUDULENT TRAFFIC.

- 4.5.1 *Fraudulent traffic includes but is not limited to traffic that the Supplier reasonably determines as: (i) calls terminated to repeating interactive voice responses (IVRs) or recordings platforms; (ii) not routed for termination in the country of destination and/or to the owner of the number range; (iii) involving numbers that are unallocated or unassigned at time of traffic; or (iv) machine generated, sequential, or simultaneous in nature.*
- 4.5.2 *The Supplier may suspend terminating traffic to certain dial codes/numbers in the event that it suspects or has likely evidence of the fraudulent use of such traffic.*

6.3 TERMINATION. *Either Party may terminate this Agreement and/or order:*

- (a) *if the other Party fails to fulfil any of its material obligations under this Agreement;”*

4. Know your Customer Protocols

HKT Group’s Risk Management and Compliance Team has policies in place to ensure that new prospects whether upstream or downstream providers or customers for voice (including ITFS) and/or messaging traffic are compliance checked against various authoritative databases. In particular, checks are carried out against the export regulations and economic sanctions programs administered by the Bureau of Industry and Security of the United States Commerce department and at the Office of Foreign Assets Control of the Treasury Department to ensure that the potential providers have no record of inappropriate behaviour.

Before signing up any prospective customer or carrier for voice services, PCCW Global completes an internal KYC questionnaire which includes:

A. Contracting party identity

- B. Incorporation details – location and registration number**
- C. Contact details of CEO and CFO**
- D. Nature of the business**

Together with supporting documents. This is then reviewed by the Export Compliance Officer. Any identified potential issues are subject to further cross-checks by Group Legal Counsel and Group Risk Management & Compliance and result in either the issue being resolved or the contract not proceeding to execution. If the new prospect is approved, finance performs a credit assessment. Federal tax details of the new prospect (if applicable) are collected by finance when implementing the new agreement.

5. Active participation in fraud-centric industry organizations

PCCW Global has been an active member of the major industry forums countering fraud from their early beginnings. PCCW Global is a member of the **Global Leadership Forum (GLF)**, participates in the **GLF Anti-fraud Working Group** and is a signatory to the **GLF Fraud-Prevention Code of Conduct** (copy attached).

PCCW Global is also an active member of the **i3Forum Anti-Fraud Working Group** and the **GSC Forum**.

6. Monitoring

- A) PCCW Global has a dedicated **Quality Assurance team** and operates a carrier grade monitoring system and analytical tools.
- B) PCCW Global has built a dedicated **Fraud Prevention Team**, completely focused on the revenue protection & loss prevention of both the customer and our own business.

In order to safeguard customer interests, PCCW Global operates an **Anti-Fraud System** with associated internal processes in place. The entirety of voice traffic handled by PCCW Global is protected by this state-of-the-art fraud prevention solution.

The Fraud Prevention & Detection capabilities of the **Anti-Fraud System** are robust and dynamic and fully cover all Inbound and Outbound voice traffic to prevent unusual fraudulent traffic including illegal robocalls and spam traffic.

The **Anti-Fraud System** is a highly automated fast and versatile system to identify and fight telecommunication fraud. It immediately detects threats, generates alert notifications and sends blocking requests to the switch Integrator teams if any unusual or suspected fraudulent traffic/calling patterns are detected - including Machine-Generated or Illegal Robocalling, Illegal call attempts and many more, on specific destinations down to an individual originating or terminating numbers.

The Fraud Prevention team participates and often leads discussions in industry forums (i3Forum as an example) pertaining to monitoring tactics, new fraud patterns, identified calling/called numbers. This helps to stay ahead of the fraudsters and decrease the likelihood of PCCWGlobal transmitting any type of fraudulent traffic including Robocall.

7. Investigating Suspicious Traffic

PCCW Global takes the following steps once the Anti-Fraud System has identified suspicious traffic patterns and generates fraud alerts when the incident threshold is reached.

- Investigate as soon as possible any identified calls potentially illegal or fraudulent in nature following the below traffic patterns:
 - Machine-generated ,Sequential, or simultaneous in nature
 - Repeated Missed call
 - Calls terminated to repeating interactive voice responses (IVRs) or recordings platforms
 - Traffic with a high volume of durations or calls
 - Disproportional Answer Call Duration/Answer Seizure Ratio (ACD/ASRs) compared to historic traffic pattern
 - Involving numbers that are unallocated or unassigned at time of traffic
- Based on the nature of the attack, the system determines and suggests if number ranges or destinations should be blocked immediately in PCCW Global's network;
- The Anti-Fraud System Immediately sends auto-generated email alert notifications to Account Managers and Customers;
- PCCW Global adheres to the i3 Forum processes for both detection and avoidance of fraud ("*Fraud classification and recommendations on dispute handling within the wholesale telecom industry Release 4 – April 2023*") see [Fraud Classification v4.0 April2023.pdf \(i3forum.org\)](#)

8. Suspending/Mitigating Illegal Traffic

PCCW Global does not accept United States traffic from entities who are not in the RMD. Once suspected fraudulent wholesale traffic has been detected and verified further investigation and action is taken.

9. US Destination Voice Traffic

PCCW Global's voice network is fully Internet Protocol, although traffic is still received from some international carrier customers via TDM. The majority of PCCW Global's US-destined voice traffic is generated by a small number of retail (carrier) customers with whom it has close operational relationships in the monitoring, investigation and suppression of illegal traffic and misuse of the network.

10. Commitment to Cooperate

PCCW Global fully supports efforts to counter illegal activity through voice calls. PCCW Global will respond fully to traceback requests from the FCC, law enforcement, and the industry traceback consortium within 24 hours of receiving a request.

Code of Conduct for International Carriers to take leadership in the prevention of fraudulent traffic (Voice)

Principle 1 - Targets and Monitoring

Targets for prevention of fraudulent traffic to be included within management reporting

Carriers will include in their internal management reporting dashboards relevant metrics and targets to all top executives to understand, and oversee, all activity to reduce fraudulent traffic flows.

Principle 2 – Processes

Carriers to adhere to i3Forum recommended processes to detect and avoid fraud

Carriers will adopt the definitions and recommendations to avoid fraudulent traffic specified in “Fraud Classification and Recommendations on Dispute Handling within the Wholesale Telecoms Industry – Release 3.0” and shall use their reasonable efforts to support the investigation of suspected fraud.

Principle 3 – Destinations

Identified fraudulent number ranges and destinations to be blocked

Carriers will actively monitor their individual traffic patterns to identify fraudulent number ranges and destinations, and take appropriate measures individually to block traffic as soon as technically feasible.

Principle 4 – Payment Flows

All reasonable action to be taken to avoid payment flows to the instigators of fraudulent traffic

Where the instigators of fraudulent traffic have been identified beyond reasonable doubt, carriers will individually seek to stop payment flows as soon as technically and commercially feasible subject to any relevant legal obligations. The originating carrier will remain responsible for the fraudulent traffic and financially liable in case the payment flows cannot be stopped by the downstream carrier(s).

Principle 5 – Reporting

Commitment to share information regarding fraudulent traffic flows with carrier peers

Carriers will actively share information on fraudulent traffic and its origination, where permissible, subject to anti-trust legislation and commercial constraints, with all potentially impacted peers.

Principle 6 – Contracting

Adoption of standard contracting terms addressing fraudulent traffic management

Carriers will adopt, once available, standard contracting terms developed by the i3 Forum for the management of fraudulent traffic and subsequent dispute resolution.

Principle 7 – Commitment to reduce IRSF**Commitment to reduce international revenue share fraud (IRSF)**

Carriers who directly breakout special number ranges for revenue share purposes, including “special services” and audiotext i.e typically higher rate destined for content related services, will clearly outline in their rate sheet that they contain such breakouts and offer customers the ability to “opt out” of such ranges prior to engaging in voice traffic. Intermediary operators will not be accountable if they are not aware of these breakouts.

By signing this Code of Conduct, companies commit to ensure their organisations adhere to the seven principles. This Code of Conduct does not alter the Carriers’ responsibility to comply with relevant regulations, nor does it limit or alter the Carriers’ contractual rights and obligations

Organizational Chart

