FINAL DECISION OF
THE COMMUNICATIONS AUTHORITY

DISRUPTIONS OF THE TELECOMMUNICATIONS SERVICES OF CHINA MOBILE HONG KONG COMPANY LIMITED

Telecommunications Licensee Investigated:	China Mobile Hong Kong Company Limited ("CMHK")
Issue:	Disruptions of the mobile telecommunications services of CMHK on 4 January and 26 February 2017
Relevant Instruments:	General Condition ("GC") 5.1 of CMHK's Unified Carrier Licence ("UCL") No. 002
Decision:	Breach of GC 5.1 of UCL No. 002
Sanction:	Financial penalty imposed
Case Reference:	LM T 1/17 in OFCA/R/R/134/2 C

BACKGROUND

On 4 January and 26 February 2017, there were two incidents of disruption of the mobile services of CMHK. Both incidents were caused by power supply problems in CMHK's network. As the disruptions extensively affected CMHK's mobile voice and data services at various locations in Hong Kong, the Office of the Communications Authority ("OFCA") activated the Emergency Response System[1] on both occasions and kept in close contact with CMHK to monitor the situation throughout the disruption periods.

[1] Emergency Response System is the communication arrangement for maintaining contacts among OFCA and all the major public telecommunications network service operators when there is a risk of possible network congestion or network outage which may affect the general public.

THE SERVICE DISRUPTION

First incident on 4 January 2017

2. CMHK reported that its network operations centre was alerted by system alarms at around 11:30 am on 4 January 2017 that one of the two uninterrupted power supply ("UPS") systems located at its IT Data Centre had failed. The resulting power interruption led to the shutdown of the application servers which were connected to the failed UPS system. The affected application servers included the RADIUS server[2] and the wireless application protocol ("WAP") gateway[3], which were deployed over the same hardware system. The shutdown of the RADIUS server resulted in the disruption of CMHK's mobile data and voice services, whereas the shutdown of the WAP gateway caused the outage of the WAP data service and multimedia messaging service ("MMS").

3. According to CMHK, once the disruption was detected, its on-site engineers immediately decided to implement the procedures to bypass the RADIUS server cum WAP gateway to enable the resumption of the mobile data and voices services, and the affected services were back to normal operation starting from 1:45 pm. In total, the disruption of CMHK's mobile data and voice services had lasted for two hours and 15 minutes. However, the recovery of CMHK's WAP data service and MMS had taken a longer time, as after the resumption of electricity supply, CMHK discovered that the RADIUS server cum WAP gateway had hardware faults. After replacing the faulty hardware, the RADIUS server cum WAP gateway resumed normal operation and the WAP data service and MMS were fully recovered by 7:30 am on 5 January 2017. In total, the disruption of the WAP data service and MMS had lasted for 20 hours.

4. According to CMHK, the incident affected about 189 172 of its active customers. CMHK reported that, during the entire disruption period, its main telecommunications networks and equipment including mobile base

---

[2] According to CMHK, the RADIUS server is used for user accounting purpose of mobile data application service. It stores user accounting information and other relevant data and is logically interfaced with the Packet Gateway inside the mobile core network.

[3] The WAP gateway is mainly used for the provision of the WAP data service for CMHK's subscribers using 2G network to access the Internet, and the Multimedia Messaging Service ("MMS") which allows mobile service subscribers to send messages that include multimedia content. The use of these two services is insignificant nowadays because of decreasing popularity.

stations in various locations of the territory and the core network equipment located in the four mobile switching centres ("MSCs") were unaffected by the power interruption problem. Of the four MSCs, two are of an older design, whilst the other two are of newer design with full site level and equipment level redundancy. The IT Data Centre hosting the failed UPS system is co-located with one of the two MSCs with the older design.

Second Incident on 26 February 2017

5. On 26 February 2017, the industrial building housing CMHK's MSC (which happens to be the same building involved in the first incident) had scheduled power maintenance work from 9:00 am to 6:00 pm during which time arrangement was made for the MSC to be powered by the diesel generator. At 1:48 pm, the diesel generator shut down due to high temperature. The backup batteries which were supposed to take over the function of the diesel generator (in case it was down) failed to provide output power due to the tripping of four out of the five moulded case circuit breakers ("MCCBs")[4] and the malfunctioning of the remaining battery (with unbroken MCCB). This resulted in disruption of power supply to the MSC and other telecommunications network equipment accommodated in the same building. The diesel generator resumed operation at 2:14 pm after cooling down. During the power outage between 1:48 pm and 2:14 pm, only limited mobile network service could be provided by the redundant network equipment at other MSCs of CMHK, with downgrade in network quality due to the ensuing network congestion.

6. After the diesel generator resumed operation at 2:14 pm, CMHK found that some telecommunications network systems were still not functioning properly including the Mobile Number Portability ("MNP") platform causing failure of mobile-to-mobile outgoing voice calls, one Home Subscriber Server ("HSS")[5] node causing occasional 4G access failure, and two Base Station Controllers ("BSCs")[6] and a number of base stations were down causing weak mobile network coverage in certain areas. All prepaid

---

[4] The fuse of those four tripped MCCBs was at 570A, while the unbroken one in the 5th MCCB was at 600A.

[5] HSS is a database that stores the subscription-related information of all the users. It plays a central role in user authentication and authorization management.

[6] BSC is a critical mobile network component which controls one or more base stations. Its key functions include radio frequency control, base stations handover management and call setup etc.

services were also unavailable as the prepaid system failed to resume operation after power up. The prepaid services resumed operation starting from 3:43 pm. By 3:55 pm, CMHK managed to recover its MNP platform and mobile-to-mobile outgoing voice calls resumed services gradually. By 5:30 am the next day, i.e. on 27 February 2017, nearly all of the some 560 failed base stations were back to normal operation, except five of them which were only restored later at 4:35 pm on 28 February 2017. The impacts of the outage of these five base stations on CMHK's customers were insignificant because of the low usage, as one of them was located at country park and the remaining four were with coverage largely overlapped with other base stations nearby. In summary, the total disruption period of the second incident had lasted for 15 hours 42 minutes[7].

7. Based on CMHK's estimation, the second incident affected about 336 734 active CMHK customers.

OFCA'S INVESTIGATION AND ASSESSMENT

8. According to the criteria set out in the "Guidelines for Local Fixed, Mobile, and Services-Based Operators for Reporting Network and Service Outage" issued by OFCA ("Guidelines")[8], the two incidents constitute "critical events", affecting a significant number of CMHK's customers. OFCA considers it necessary to conduct an investigation to –

(a) examine whether CMHK has breached GC 5.1 of its UCL which specifies that –

> *"5.1 The licensee shall, subject to Schedule 1 to this licence and any special conditions of this licence relating to the provision of the service, at all times during the validity period of this licence operate, maintain and provide a good, efficient and continuous service in a manner satisfactory to the Authority…"*; and

[7] The duration of service disruption of the second incident was counted from 1:48 pm on 26 February 2017 to 5:30 am on 27 February 2017.

[8] For details of the Guidelines, please refer to – http://www.coms-auth.hk/filemanager/statement/en/upload/367/gn112016e.pdf

(b) review the actions taken by CMHK in handling the two service disruptions (including the efficiency of service restoration, the communications with OFCA, and customers and the media, etc.) to examine whether there are any areas warranting CMHK to make improvements.

9. For the first incident, CMHK submitted, as per OFCA's request, a preliminary report[9] on 9 January 2017 and a full report[10] on 24 January 2017. For the second incident, CMHK submitted a preliminary report[11] on 1 March 2017 and a full report[12] on 16 March 2017. In the course of the investigation, CMHK also provided supplementary information in response to OFCA's enquiries about the two incidents. Arising from the two incidents, OFCA received a total 121 consumer complaints. Most of the complaints were about dissatisfaction of the repeated service disruptions within a short period of time, the long disruption periods, and the difficulties in reaching CMHK's customer hotline during the period of service disruption.

10. OFCA completed its investigation and submitted its findings to the Communications Authority ("CA") on 20 May 2017. Having considered the findings of OFCA, the CA issued its Provisional Decision to CMHK on 22 May 2017 and invited CMHK to make representations within 14 days. CMHK submitted on 5 June 2017 that it had no comment on the CA's Provisional Decision.

---

[9] The preliminary report of CMHK on the first incident may be downloaded from OFCA's website at http://www.ofca.gov.hk/filemanager/ofca/en/content_723/cmhk_report_20170109.pdf

[10] The full report of CMHK on the first incident may be downloaded from OFCA's website at http://www.ofca.gov.hk/filemanager/ofca/en/content_723/cmhk_report_20170124.pdf

[11] The preliminary report of CMHK on the second incident may be downloaded from OFCA's website at http://www.ofca.gov.hk/filemanager/ofca/en/content_723/cmhk_report_20170301.pdf

[12] The full report of CMHK on the second incident may be downloaded from OFCA's website at http://www.ofca.gov.hk/filemanager/ofca/en/content_723/cmhk_report_20170316.pdf

Major Issues Examined

The Cause of the Incidents and the Adequacy of CMHK's Preventive Measures

CMHK's Representations on the First Incident

11. According to CMHK, the failed UPS system was deployed to supply power to a number of application servers, including the RADIUS server cum WAP gateway, and a Data Warehouse server used for big data analysis. All the above equipment was accommodated at CMHK's IT Data Centre. CMHK submitted that its vendor claimed that the incident was caused by the hardware fault of the Data Warehouse server which drew excessive output current from the UPS system, causing the tripping of two MCCBs connected respectively to the power input and output ports of the UPS system, and damaging the power module and the bypass module of the UPS system. CMHK reported that the UPS system was backed up by batteries and diesel generator which should provide alternative power supply in case the UPS system was down. However, as the bypass module of the UPS system was damaged in the incident, the mechanism for bypass to batteries did not function properly. As for the diesel generator, it was arranged to start up only when the mains power to the IT Data Centre was down. As there was no failure of the mains power at all, the diesel generator did not start up to take over to supply power.

12. As a result of the power failure, the RADIUS server cum WAP gateway which was connected to the above UPS system stopped operation. As the RADIUS server was responsible for handling user accounting for mobile data services, its shut down resulted in failure of CMHK to respond to the queries from the mobile core network and therefore new requests for setting up mobile data service from customers could not be processed. Due to the subsequent large amount of setup retry attempts initiated by the mobile core network, high traffic load occurred in certain network nodes leading to network congestion and disruption of the mobile data and voice services for some of CMHK's customers. In addition, the incident also disrupted the WAP data service and MMS, because of the shutdown of the RADIUS server cum WAP gateway.

13. CMHK submitted that both the UPS system[13] and the RADIUS server cum WAP gateway[14] were supplied by reputable equipment vendors. It reported that it had made its best endeavours to maintain the stability and reliability of the UPS system and the RADIUS server cum WAP gateway. There were regular preventive maintenance and health checking procedures in place for the two systems. According to CMHK, the latest upgrade of the RADIUS server cum WAP gateway took place in 2010. The last inspection and preventive maintenance procedures for the UPS and the electrical facilities were carried out in November and December 2016 respectively, and no anomaly was found.

14. CMHK admitted that the power resilience of the application servers (including the RADIUS server cum WAP gateway and the Data Warehouse server as mentioned above) installed at its IT Data Centre was not as good as that of its MSCs where its mobile telecommunications equipment was installed. Before the incident, the IT Data Centre was located in premises with comparatively older power system design such that the RADIUS server cum WAP gateway and other equipment in the IT Data Centre were only connected to one UPS system without power supply backup from another separate and independent UPS system.

15. In order to prevent similar incidents from recurring in future, CMHK submitted that –

(a) as an interim measure, it had after the incident improved the power supply backup arrangement by connecting the RADIUS server cum WAP gateway to two separate UPS systems;

(b) it had configured its mobile core network to permanently bypass the RADIUS server. In case there was any power failure at the IT Data Centre again, the shut down of the RADIUS server would no longer affect the mobile data and voice services; and

---

[13] The UPS was supplied by American Power Conversion Corporation which is a multinational European corporation with expertise in energy management and automation. It was acquired by Schneider Electric in 2007.

[14] The RADIUS server cum WAP gateway was supplied by Ericsson which is a reputable vendor of telecommunications equipment. It provides telecommunications equipment and services to various telecommunications operators in the world.

(c) it was in the process of upgrading its network for the provision of 4.5G mobile services. The new setup of the core mobile network equipment, together with the new Cloud Value Added Service ("VAS") platform which supports multiple functions replacing the RADIUS server cum WAP gateway, would be installed at the two more advanced MSCs with full site level and equipment level redundancy by June 2017. The two MSCs of older design and the IT Data Centre would eventually be phased out after the network migration.

CMHK's Representations on the Second Incident

16. CMHK submitted that despite its preparations for the scheduled power maintenance work on 26 February 2017, the day of the incident, unexpected consecutive failures in its power supply systems on that very same day gave rise to the service disruption. First, the diesel generator was overheated and it shut down due to high temperature. Secondly, all of the five backup batteries failed to take over the function of the diesel generator to supply power after it shut down.

17. CMHK reported that the root cause for the overheating of the diesel generator was improper operation of the cooling fan due to the loose tension of the V-Fan Belt, such that ventilation was poor and the diesel generator was shut down automatically by the high temperature protection mechanism after the cooling water temperature reached 95°C. As regards the failure of the backup batteries, CMHK reported that the root cause was that one of the batteries (i.e. the one with the unbroken MCCB) was faulty, and as a result, the system load was transferred to the other four batteries during the discharge, resulting in overload and the tripping of the MCCBs connected with them.

18. According to CMHK, both the diesel generator[15] and the backup batteries[16] of the DC power system were supplied by reputable equipment vendors. CMHK submitted that the diesel generator had been put into

[15] The diesel generator was supplied by FG Wilson which is a multinational corporation with over fifty years of experience in the supply of diesel and gas generator sets and maintained by ATAL which is a reputable electrical, and mechanical engineering company with over thirty five years of experience.

[16] The five backup batteries of the DC power plant were supplied and supported by Vertiv Co., formerly called Emerson Network Power, which is a global provider of critical equipment for vital applications in data centers, including critical power equipment, UPS, etc.

service since August 2011 and had been activated for a few times before, when there were suspension of mains power outage or maintenance works. CMHK also reported that the diesel generator was checked twice by maintenance vendors on 7 and 23 February 2017 (i.e. shortly before the second incident) for the purpose of getting prepared for the scheduled power maintenance and no anomaly was found. With regard to the backup batteries of the DC power system, CMHK submitted that three out of five batteries had been put to service since 2015 and the remaining two since 2005 and 2013. The last preventive maintenance of DC power system was conducted on 29 December 2016, and that for the electrical system at the MSC on 7 February 2017. No anomaly was identified during the regular check.

19. In order to prevent similar incidents from recurring in future, CMHK submitted that –

(a) as an immediate measure, it had shut down some unused equipment to reduce the loading at the MSC. Besides, two new backup batteries were added on 16 March 2017. CMHK also upgraded the capacity of all MCCBs (from 570A to 1250A) with effect from 18 March 2017 to increase the tolerance margin of the batteries;

(b) its maintenance vendor had tightened the V-Fan Belt and replaced the cooling water temperature sensor on 8 March 2017. CMHK also confirmed the healthy operation of the diesel generator, with cooling water temperature maintained at around 70°C during the load test;

(c) it would arrange checking and tightening of the V-Fan Belt tension of the diesel generator at least once a year, in addition to conducting the visual check of belt tension during the monthly preventive maintenance. It would also arrange a full load test for the diesel generator before every planned mains power outage of the industrial building in the future; and

(d) it was in the process of migrating and upgrading its network to a design with 100% site resiliency of network equipment (including BSC). The migration would be completed by Q3 of 2017. The MNP platform would also be replaced by new nodes with full site

level and equipment level resiliency by July 2017. Besides, the prepaid system would be migrated to a new system with equipment to be deployed in two different MSCs to provide full site level and equipment level resiliency by November 2017. After the completion of the migration, all network equipment would have dual power feeds with separate power systems, and the two MSCs of older design and the IT Data Centre would be phased out.

OFCA's Assessment on the First Incident

20. OFCA notes that the UPS system and the RADIUS server cum WAP gateway were procured from reputable equipment suppliers and CMHK also took reasonable measures to maintain their technical healthiness and stability after they were put into service. However, the incident revealed problems in the original design of the power backup system in CMHK's IT Data Centre and the redundancy design of the application servers. OFCA's assessment is set out below.

21. First, OFCA considers that the UPS system should have been equipped with adequate and effective protection against over-voltage and over-current surges so as to ensure uninterrupted power supply to the concerned application servers. Although CMHK had arranged to back up the concerned UPS system by batteries and diesel generator, both alternative power sources failed to take over to supply power as the bypass module of the UPS system was damaged and not functioning.

22. Secondly, OFCA considers it undesirable that the RADIUS server cum WAP gateway, an important network component of CMHK's mobile network in that its failure would lead to widespread network congestion as in the present case, was only connected to a single power source via the failed UPS system, without access to any alternative power sources. Furthermore, CMHK had only maintained a single RADIUS server cum WAP gateway without equipment redundancy. Both such features reflected that CMHK had not adopted a robust design for the operation of these systems (which should be regarded as part of its telecommunications network) to cater for unexpected system failures and equipment faults etc. CMHK reported that it had immediately improved the backup arrangement after the incident by connecting the RADIUS server cum WAP gateway to two separate UPS

systems. If this had been done before the incident, the service disruption could have been avoided.

23. OFCA notes that CMHK is now in the process of phasing out the two older MSCs and the IT Data Centre, and is migrating the RADIUS server cum WAP gateway to its new Cloud VAS platform which would be installed at the two more advanced MSCs with full site level and equipment level redundancy by June 2017. OFCA expects that the implementation of such arrangement will rectify the power design problems and improve the reliability of CMHK's network.

OFCA's Assessment on the Second Incident

24. OFCA observes that there were three problematic areas. First, CMHK reported that it was alerted by the temperature alarm only when the cooling water temperature reached 90°C, and the diesel generator was shut down automatically shortly later by the high temperature protection mechanism. Although CMHK explained that the triggering threshold of the temperature alarm and the automatic shut down mechanism of the diesel generator were set by the manufacturer since the equipment was installed, the evidence showed that CMHK had just relied on the temperature alarm and had not closely kept track of the water cooling process by monitoring the actual water temperature level. Otherwise, CMHK would have been alerted by the rapid temperature increase at an earlier stage before the alarm was triggered so that it would have more time to respond before the automatic shut down of the diesel generator and to take any possible corrective action.

25. Secondly, OFCA observes that CMHK had not taken reasonable measures to ensure smooth handover between the diesel generator and the backup battery banks of the DC power plant. CMHK admitted that the transition of power supply from diesel generator to backup batteries had never been tested. OFCA considers this undesirable as without tests CMHK would not have any degree of certainty as to whether the backup batteries would serve their intended function in taking over the diesel generator in case of emergency, and whether any unexpected problems would arise during or after the transition.

26. Thirdly, CMHK claimed that, in addition to the implementation of other improvement measures, it had upgraded the capacity of those four

original MCCBs after the incident. CMHK claimed that this action would increase each battery bank's tolerance margin for large unbalanced current loading among the batteries, without reducing the protection of telecommunications equipment because the power feeds of the telecommunications equipment was protected by individual circuit breakers with proper ratings in the DC power plant. In that case, OFCA notes that the second incident would not have occurred if CMHK had been mindful of the problem in advance and had deployed the MCCBs with suitable capacity before the incident.

27. In conclusion, having examined the facts and circumstances of the two incidents, OFCA considers that, although CMHK had acted reasonably in the procurement and maintenance of the equipment for power supply, the effectiveness of the backup arrangement for the power supply systems was unsatisfactory. In both incidents, the backup arrangements did not function as intended to provide substitutional power supply in the event of power supply interruption. The two incidents have revealed that CMHK had not put in place effective measures to safeguard against the occurrence of service disruption in the event of power supply interruptions caused by UPS system failure in the first incident and diesel engine cum battery failures in the second incident.

Time and Actions Taken by CMHK to Restore Services

CMHK's Representations on First Incident

28. In the first incident, CMHK submitted that, once the network alarms were received at around 11:30 am on 4 January 2017, its on-site engineers immediately carried out troubleshooting and conducted various call tests to trace the cause of the problem. Once it was confirmed that an UPS system at the IT Data Centre was down at 11:35 am, CMHK immediately decided to implement the procedures to bypass the RADIUS server. At 12:15 pm, CMHK's engineers started to reconfigure the mobile core network to bypass all queries to the RADIUS server. After the completion of the system reconfiguration at 12:40 pm, the mobile data and voice services of CMHK resumed operation progressively and were mostly back to normal at 1:45 pm.

29. CMHK had also requested the vendor of the UPS system to offer assistance once it had discovered that an UPS system at the IT Data Centre was down. CMHK reported that the vendor's engineer arrived on-site at 12:15 pm on 4 January 2017 and started the troubleshooting procedures. At 12:35 pm, the dysfunctional UPS system was bypassed and the supply of electricity was resumed by mains power. After the resumption of electricity, CMHK discovered that the RADIUS server cum WAP gateway had hardware faults. After replacing the faulty hardware components, the WAP service and MMS resumed by 7:30 am on 5 January 2017.

CMHK's Representations on Second Incident

30. CMHK reported that, once the diesel generator was shut down and the backup batteries of the DC power system was found not functioning, it immediately triggered the internal emergency escalation procedures at 1:48 pm on 26 February 2017. The on-site vendor support engineer started troubleshooting and power supply to the MSC resumed at 2:14 pm.

31. As soon as CMHK discovered that some of the network equipment were still not functioning normally after the resumption of power, it requested the equipment vendor(s) to dispatch engineers to provide on-site support immediately. CMHK worked closely with the vendor to restore the operation of the failed BSCs and base stations, as a result of which nearly all base stations were restored by 5:30 am on 27 February 2017, with the remaining five base stations fixed and resumed operation by 4:35 pm on 28 February 2017. To deal with the problem of the HSS node, CMHK isolated the unstable HSS at 4:09 pm and divert the traffic to a redundant HSS at another MSC. After taking such an action, the 4G network started to resume normal operation. With the assistance of the vendor, CMHK also managed to reboot the MNP platform successfully by 3:55 pm on 26 February 2017 to resume the mobile outgoing voice services. With regard to the prepaid system, CMHK decided to bypass the charging mechanism to enable the prompt resumption of prepaid voice and data services (without charging) starting from 3:43 pm on 26 February 2017. Prepaid services (with charging) were fully recovered subsequently by 10:20 pm on the same day.

OFCA's Assessment on First Incident

32. OFCA is of the view that CMHK's performance in restoring the services was not entirely satisfactory. In particular, CMHK had taken a long time to fix the RADIUS server cum WAP gateway, such that the WAP service and MMS could only be restored 20 hours after the service disruption. Although CMHK said that the usage of the two services was insignificant, OFCA considers that CMHK must at all times during the validity period of its licence operate, maintain and provide a good, efficient and continuous service to customers, regardless of whether the service is heavily used or not. The long duration of the outage of the WAP service and MMS is clearly unacceptable.

OFCA's Assessment on Second Incident

33. OFCA considers that CMHK's performance in handling the restoration of services was also unsatisfactory. As two BSCs and some base stations were down, despite the fact that CMHK had acted promptly to isolate the dysfunctional HSS, reboot the MNP platform and bypass the charging mechanism of the prepaid service, CMHK's mobile data and voice services could not be fully restored to normal operation within a short period of time. Although CMHK claimed that it had managed to restore the two failed BSCs and 75% of its base stations by 5:15 pm on 26 February 2017 (nearly 3.5 hours after the occurrence of the incident) and the mobile data and voice services largely resumed normal operation by 7:45 pm, the quality and coverage of the mobile data and voice services of CMHK remained unsatisfactory until 5:30 am on the next day (i.e. 27 February 2017) when nearly all base stations of CMHK were recovered, with a total disruption period of nearly 16 hours for its mobile data and voice services. Such a long duration of service outage is unacceptable.

34. In conclusion, OFCA considers that the time and action taken by CMHK to restore the affected services in both incidents were not up to a satisfactory standard.

CMHK's Communications with OFCA over the Service Disruption

CMHK's Representations on First Incident

35. The service disruption occurred at around 11:30 am on 4 January 2017, a weekday. Pursuant to the Guidelines, CMHK should have notified OFCA of the incident by 12:00 pm, i.e. 15 minutes after the triggering criteria were met. According to OFCA's record, the first instance when CMHK reported the details of the incident to OFCA was at around 12:30 pm, after OFCA had made several attempts to contact CMHK to enquire about the situation.

36. CMHK's mobile data and voice services resumed normal operation at 1:45 pm on 4 January 2017. Pursuant to the Guidelines, CMHK should have notified OFCA before 2:45 pm, i.e. within one hour after resumption of the mobile data and voice services. According to OFCA's record, CMHK informed OFCA at 2:15 pm of the resumption of the services.

CMHK's Representations on Second Incident

37. The service disruption occurred at 1:48 pm on 26 February 2016, a Sunday. Pursuant to the Guidelines, CMHK should have notified OFCA of the incident before 3:03 pm, i.e. within one hour after the triggering criteria were met. According to OFCA's record, CMHK informed OFCA of the outage at 2:42 pm. As regards service resumption, pursuant to the Guidelines, CMHK should have notified OFCA within four hours after resumption of services. CMHK claimed that its mobile data and voice services had largely resumed normal operation starting from 7:45 pm on 26 February 2017. It informed OFCA at 8:44 pm of the resumption of its services.

OFCA's Assessment on Both Incidents

38. According to the Guidelines, both incidents had led to a loss of call capabilities by customers for longer than 15 minutes which were considered as critical network outages. The first incident occurred on a weekday and CMHK should have reported to OFCA within 15 minutes after the triggering criterion was met. The second incident occurred on a Sunday and CMHK should have reported to OFCA within one hour after the triggering

criterion was met. CMHK failed to meet the requirements stipulated in the Guidelines for reporting the occurrence of outage for the first incident, which was 45 minutes later than the reporting timeframe specified in the Guidelines, but it had complied with the relevant reporting requirement for the second incident. As for the restoration of services, CMHK complied with the relevant reporting requirement for both incidents, i.e. within one hour and four hours after the restoration of services for the first incident and second incident respectively.

39. CMHK had not been proactive in keeping OFCA informed of the updated status of the first incident during the disruption period. Though CMHK had taken a more proactive role in reporting the status of the second incident to OFCA, OFCA considers that there is still room for improvement regarding the way CMHK handled it's communications with OFCA. CMHK should remind its staff of the need and importance of timely communications with OFCA on the updated status of the service disruption, in order for OFCA to make an accurate and timely assessment of the severity of the incident and its impact on the public, and for OFCA to assist in providing timely advice and guidance to users on alternative arrangements during service disruption.

40. Overall speaking, OFCA considers that CMHK had failed to comply with the Guidelines to report to OFCA the occurrence of the first incident within the timeframe as stipulated. In addition, in both incidents, the manner in which CMHK handled its communications with OFCA, in particular to keep OFCA informed of the updated status of the incident during the disruption period, was unsatisfactory.

<u>CMHK's Communications with Customers and the Media</u>

CMHK's Representations

41. CMHK claimed that it had taken the following actions to notify customers of both incidents –

(a) In the first incident,

(i) after the incident occurred, CMHK immediately notified its retail sales, corporate sales and hotline staff and provided them with the updated information to answer customer

enquiries. In addition, it also adjusted the manpower in its Customer Services Hotline Centre (including arranging staff to work overtime) to deal with the influx of customers' enquiries;

(ii) at 12:59 pm on 4 January 2017, CMHK posted the first message on Facebook to notify customers of the incident. At 3:38 pm, CMHK posted the second message on Facebook to notify customers that mobile data and voice services had resumed normal. At 11:42 pm, CMHK posted the third message on Facebook to notify customers that access to CMHK's corporate website and other applications had restored; and

(iii) at about 2 pm on 4 January 2017, CMHK issued the first media statement to inform the media of the progress of the emergency repairs and to apologize to the affected customers. At about 5 pm, CMHK issued the second media statement to update the media that mobile data and voice services had resumed normal.

(b) In the second incident,

(i) after the incident had occurred, CMHK briefed all its frontline staff at 2:15 pm to facilitate them to handle customer enquiries. It also immediately adjusted the manpower in its Customer Services Hotline Centre (including arranging staff to work overtime) to deal with the influx of customers' enquiries. In addition, CMHK also prepared and uploaded announcements in the Interactive Voice Response system to inform its customers about the status of service resumption at 8:10 pm and 10:09 pm;

(ii) at 3:39 pm on 26 February 2017, CMHK posted the first message on its corporate website to notify customers of the incident. At 7:00 pm, CMHK posted the second message on its corporate website to notify customers that mobile data and voice services had resumed gradually. At

9:35 pm, CMHK posted the third message on its corporate website to notify customers that the mobile data and voice services had restored;

(iii) at 3:04 pm on 26 February 2017, CMHK posted the first message on Facebook to notify customers of the incident. At 7:30 pm, CMHK posted the second message on Facebook to notify customers that mobile data and voice services had resumed gradually. At 9:55 pm, CMHK posted the third message on Facebook to notify customers that the mobile data and voice services had restored; and

(iv) At 3:20 pm on 26 February 2017, CMHK issued the first media statement to inform the media of the progress of the emergency repairs and to apologize to the affected customers. At 9:30 pm, CMHK issued the second media statement to inform the media that mobile data and voice services had largely resumed.

42. According to CMHK, up to 16 March 2017, it received a total of 3 196 enquiries and 573 complaints regarding the first incident and 5 913 enquiries and 6 517 complaints regarding the second incident. OFCA received a total of 121 complaints (19 for the first incident and 102 for the second incident) from the public and a few enquiries from the media about the two incidents. The complaints can be classified in the following areas –

(a) the repeated disruptions of CMHK's mobile and data services within a few days;

(b) the long disruption periods in the second incident;

(c) CMHK's failure to notify customers of the service disruption in a timely manner; and

(d) CMHK's hotline was always engaged.

OFCA's Assessment

43. After examining the actions taken by CMHK and the complaints from the public and the media, OFCA is of the view that CMHK had failed to provide customers with timely information about the two incidents.

44. In the first incident, OFCA notes that the first notification made by CMHK to its customers (by posting a message on CMHK's official Facebook) was at 12:59 pm on 4 January 2017, being one hour and 29 minutes after the occurrence of the service disruption). The affected customers therefore did not know what had happened with CMHK's mobile data and voice services and when the services would resume normal operation before that time. Although CMHK notified its retail sales, corporate sales and hotline staff and provided them with the relevant information to enable them to answer customer enquiries, OFCA received complaints from the public to the effect that they had tried to call CMHK's hotline during the outage period but it was always engaged and they could not get through to any CMHK staff. In addition, OFCA also notes that the media statements were issued by CMHK only after emergency repair had been conducted and the network data and voice traffic was mostly back to normal level. OFCA considers that CMHK could have notified its customers and the media of the service disruption earlier (e.g. around the time when it could provide details of the incident to OFCA at 12:30 pm on 4 January 2017) and this would help alleviate customer concern and grievances.

45. In the second incident, the service disruption occurred at 1:48 pm on 26 February 2017. CMHK made its first notification to its customers (by posting a message on CMHK's official Facebook) at 3:04 pm, one hour and 16 minutes after the occurrence of the service disruption. Although CMHK also announced the service disruption by posting an announcement on its corporate website and issuing a media statement, the announcements were not issued in a timely manner. CMHK's first media statement was announced at 3:20 pm and it posted its first announcement on its corporate website at 3:39 pm, one hour and 32 minutes and one hour and 51 minutes after the occurrence of the service disruption respectively. Similar to the first incident, although CMHK briefed its frontline staff and provided them with the relevant information to respond to customers' enquiries, OFCA received complaints from the public to the effect that they had tried to call CMHK's hotline during the outage period but it was always engaged and they could not get through to any CMHK staff.

OFCA notes that the announcements through various means were made more than one hour after the occurrence of the incident. In OFCA's view, CMHK should inform its customers and the media shortly after the time it was required to notify OFCA of the occurrence of the service disruption pursuant to the Guidelines.

46. Overall speaking, OFCA considers that the arrangements made by CMHK in notifying its customers and the media of the service disruption were unsatisfactory in both incidents. CMHK should improve its internal procedures to ensure more timely dissemination of information to its customers and the media in the event of service disruption in future.

THE CA'S CONSIDERATION AND DECISION

47. After examining the facts of the two incidents, the assessment of OFCA and the representations of CMHK on the CA's Provisional Decision, the CA considers that CMHK has –

(a) in the first incident, failed to ensure that the operation of its UPS system as well as the RADIUS server cum WAP gateway was supported by an effective backup power supply system, and also failed to ensure that the application servers in the IT Data Centre were provided with redundancy in site level and equipment level, which led to a critical network outage, adversely affecting the mobile data and voice services provided to a significant number of users;

(b) in the second incident, failed to commission and operate a well designed and effective backup power supply system to ensure a continuous power supply to the network equipment of its telecommunications network in response to the scheduled maintenance of the mains power;

(c) in the first incident, failed to restore the WAP service and MMS and, in the second incident, failed to restore the quality and coverage of the mobile data and voice services within a reasonable timeframe;

(d) in the first incident, failed to comply with the Guidelines to report to OFCA the occurrence of the first incident within the timeframe as stipulated; and

(e) in both incidents, failed to notify its customers and the media of the service disruptions in a satisfactory manner.

48. In conclusion, after taking into account all the above, the CA considers that CMHK has failed to comply with GC 5.1 of its UCL No. 002, which requires it to operate, maintain and provide a good, efficient and continuous service in a manner satisfactory to the CA during the two incidents. In view of the severity of the incidents, the CA considers that CMHK should be imposed a financial penalty pursuant to section 36C(1)(a) of the Telecommunications Ordinance (Cap. 106) ("TO").

FINANCIAL PENALTY

49. Pursuant to section 36C(1)(a) of the TO, the CA may, subject to section 36C(3B), impose a financial penalty in any case where the licensee fails to comply with any licence condition. Under section 36C(3) of the TO, a financial penalty so imposed shall not exceed $200,000 for the first occasion, and $500,000 for the second occasion, on which a penalty is so imposed.

50. On the basis that this is the first occasion where CMHK is to be imposed a financial penalty for non-compliance with GC 5.1 of its licence, the maximum penalty stipulated by the TO is $200,000. In considering the appropriate level of financial penalty, the CA has had regard to the "Guidelines on the Imposition of Financial Penalty under Section 36C of the TO" (the "Financial Penalty Guidelines")[17]. Under the Financial Penalty Guidelines, the CA is to consider a number of factors including the gravity of the breach (which includes the nature and seriousness of the infringement), whether any repetition of conduct is involved and whether there are any aggravating or mitigating factors.

51. In considering the gravity of this breach, and therefore the starting point for the level of penalty, the CA notes that the impacts of the outage were serious because –

[17] The document may be downloaded from http://tel_archives.ofca.gov.hk/en/legislation/guideline_6d_1/guideline_6d_1_150402.pdf

(a) it was estimated that 189 172 and 336 734 of CMHK's active customers were affected in the first and the second incident respectively;

(b) the disruption of mobile data and voice services had lasted for two hours and 15 minutes in the first incident, and 15 hours and 42 minutes in the second incident. Also, the two incidents which were both related to power supply problems occurred within a short period of time (i.e. less than two months); and

(c) the scope of service disruption was extensive, covering basically all mobile services provided by CMHK including mobile data service, voice service, prepaid services and some VAS like WAP data service and MMS.

52. The CA also notes that there is no information to suggest any foul play or ill intent in the incident, which would have added to the severity of the breach. Making reference to the precedent cases, the CA considers that the appropriate starting point for determining the level of financial penalty should be $180,000.

53. In considering the mitigating factors, the CA notes that CMHK has provided full cooperation to OFCA in the course of the investigation. CMHK has also taken prompt action to implement remedial measures to prevent the recurrence of similar incidents in the future.

54. The CA has not identified any aggravating factors which offset the mitigating factors that have been taken into account.

55. Having carefully considered the circumstances of the case and taken all factors into account, the CA concludes that a financial penalty of $150,000 is proportionate and reasonable in relation to the breach.

IMPROVEMENT MEASURES

56. The CA notes that CMHK has taken expeditious action to improve the backup power supply system after the first incident and has performed necessary rectifications to ensure the effectiveness of the ventilation system of the diesel generator and the reliability of the backup batteries after the second incident. In addition, the CA also notes that CMHK is in the process of

migrating all its network equipment to the two more advanced MSCs with full site level and equipment level redundancy. After the migration, all the mobile network equipment of CMHK would be deployed in the two more advanced MSCs which will be equipped with dual power feeds to separate power systems to ensure power security.

57. Notwithstanding the above, the CA considers that CMHK should also implement the following measures to improve the manner in which it handles the communications with OFCA, the customers and the media in the future –

(a) remind its staff of the need and importance of timely communications with OFCA on the updated status of any service outage as soon as practicable; and

(b) review its internal procedures to ensure more timely dissemination of information to its customers and the media in the event of service disruption. The target should be to notify customers and the media at the time shortly after the first report of the incident to OFCA.

The Communications Authority
June 2017