FINAL DECISION OF
THE COMMUNICATIONS AUTHORITY

DISRUPTIONS OF THE TELECOMMUNICATIONS SERVICES OF CHINA UNICOM (HONG KONG) OPERATIONS LIMITED

Telecommunications Licensee Investigated:	China Unicom (Hong Kong) Operations Limited ("China Unicom")
Issue:	Disruptions of the mobile telecommunications services of China Unicom on 27 February and 31 March 2018
Relevant Instruments:	General Condition ("GC") 5.1 of China Unicom's Services-Based Operator ("SBO") Licence for provision of Class 3 Services (Licence No. 922)
Decision:	Breach of GC 5.1 of China Unicom's SBO Licence (Licence No. 922)
Sanction:	Financial penalty imposed
Case Reference:	LM T 50/18 in OFCA/R/R/134/2 C

BACKGROUND

On 27 February 2018, China Unicom reported to the Office of the Communications Authority ("OFCA") that there was an outage of its "1-Card-Multiple-Number" ("1CMN") System. About one month later, on 31 March 2018, China Unicom reported to OFCA that there was another outage of its 1CMN System. In both incidents, China Unicom's mobile voice services, short message services ("SMS") and mobile data services (i.e. Internet access) were disrupted. OFCA activated the Emergency Response System[1] in both

[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.

incidents and kept in close contact with China Unicom to monitor the situation throughout the incidents.

THE SERVICE DISRUPTIONS

The First Incident

2. According to China Unicom, the first incident occurred at about 10:50 am on 27 February 2018. Its network operating centre ("NOC") observed that a large number of customers using 1CMN service failed to complete the location update process and were unable to have access to its mobile services including mobile voice services, SMS and mobile data services. Upon detection of the problem, its vendor attempted to restore the 1CMN System, but without success. At about 1:00 pm, its NOC carried out procedures to manage affected customers' traffic with bypass of the 1CMN System[2]. Upon completion of the above procedures at about 2:20 pm, the affected mobile outgoing voice services and mobile data services began to resume. After the 1CMN System had been restored, all the affected mobile services resumed normal from about 4:30 pm on 27 February 2018. The outage lasted for about five hours and 40 minutes. About 138 150 customers of China Unicom using 1CMN service were affected, representing about 15.78% of its total number of active customers in Hong Kong. According to China Unicom, it had implemented relevant measures to prevent recurrence of similar incident (see paragraph 10 for details).

The Second Incident

3. At about 11:15 am on 31 March 2018, the second day of the Easter holidays, there was a sudden surge of traffic which again led to failure of China Unicom's 1CMN System. Similar to the first incident, China Unicom's mobile services including mobile voice services, SMS and mobile data services were disrupted. In response to the failure of the 1CMN System, its vendor attempted to activate a standby unit of the 1CMN System ("standby system") but failed. At about 12:10 pm, its NOC carried out similar procedures to bypass the 1CMN System, with a view to partially resuming the affected mobile services. Upon completion of the above procedures at about 1:15 pm, the affected mobile

[2] The procedures involve diverting traffic from China Unicom's mobile switching centre ("MSC") to its home location register ("HLR") directly.

outgoing voice services and mobile data services began to resume. At about 3:20 pm, the standby system restarted successfully. As the incoming traffic to the 1CMN System was high, China Unicom had to re-route the traffic to reduce the loading. At about 6:30 pm, the loading of the 1CMN System was back to normal. After reversing the bypass procedures, all the affected mobile services resumed normal from 6:40 pm on 31 March 2018. The outage lasted for about seven hours and 25 minutes. About 138 150 customers of China Unicom using 1CMN service were affected, representing about 15.78% of its total number of active customers in Hong Kong. China Unicom had also implemented remedial measures after the second incident (see paragraph 14 for details).

OFCA'S INVESTIGATION

4. 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 ("the Guidelines")[3], the two incidents were regarded as critical network outages. As a large number of China Unicom's customers were affected, OFCA considers it necessary to conduct an investigation into the incidents to –

(a) examine whether China Unicom has breached GC 5.1 of its SBO Licence (Licence No. 922), which stipulates 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

(b) review the actions taken by China Unicom in handling the incidents (including the efficiency of service restoration, the communications with OFCA and customers, etc.) to examine whether there are any areas requiring improvements by China Unicom.

---

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

5. For the first incident, China Unicom submitted, as per OFCA's request, a preliminary report [4] on 2 March 2018 and a full report [5] on 19 March 2018. For the second incident, China Unicom submitted a preliminary report[6] on 6 April 2018 and a full report[7] on 23 April 2018. In the course of OFCA's investigation, China Unicom also provided supplementary information in response to OFCA's enquiries about the two incidents.

6. OFCA received a total of 24 consumer complaints/enquiries arising from the two incidents. Most of the complaints/enquiries were about dissatisfaction of the repeated service disruptions within the timespan of about one month, the long disruption periods, and difficulties in reaching China Unicom's customer service hotline during the periods of service disruption.

7. OFCA completed its investigation and submitted its findings to the Communications Authority ("CA") on 20 August 2018. Having considered the findings of OFCA, the CA issued its Provisional Decision to China Unicom on 24 August 2018 and invited China Unicom to make representations within 14 days. China Unicom submitted its representations on the CA's Provisional Decision on 7 September 2018.

MAJOR ISSUES AND OFCA'S ASSESSMENT

The Cause of the Incident and the Adequacy of China Unicom's Preventive Measures

China Unicom's Representations on the First Incident

8. According to China Unicom, the first incident was caused by a

---

[4] The preliminary report regarding the first incident of China Unicom may be downloaded from OFCA's website at https://www.ofca.gov.hk/filemanager/ofca/en/content_723/cuol_report_20180302.pdf

[5] The full report regarding the first incident of China Unicom may be downloaded from OFCA's website at https://www.ofca.gov.hk/filemanager/ofca/en/content_723/cuol_report_20180319.pdf

[6] The preliminary report regarding the second incident of China Unicom may be downloaded from OFCA's website at https://www.ofca.gov.hk/filemanager/ofca/en/content_723/cuol_report_20180406.pdf

[7] The full report regarding the second incident of China Unicom may be downloaded from OFCA's website at https://www.ofca.gov.hk/filemanager/ofca/en/content_723/cuol_report_20180423.pdf

hardware fault in one of the servers of the 1CMN System[8] and a software bug. As confirmed by the hardware manufacturer (IBM), the hardware fault was due to a hardware defect in one of the Central Processing Units ("CPUs") used in the abovementioned server. Even though China Unicom's 1CMN System had been designed with resiliency and protection mechanisms (including, among others, an arrangement ("Arrangement") in which if any one of the servers of the 1CMN System malfunctioned, it could be detected and isolated with all the traffic capable of being handled by other servers), the software bug had resulted the 1CMN System unable to identify the malfunctioned server with the hardware fault and unable to activate the Arrangement. As a result, the signalling messages were stacked in queue and grew continuously, which subsequently led to failure of the entire 1CMN System.

9. China Unicom submitted that the root cause of the first incident was beyond its control since it was due to hardware defect and software bug which led to software operation error and failure of the protection mechanisms of the 1CMN System. According to China Unicom, the hardware platform (including the CPUs) was supplied by reputable hardware manufacturers and the 1CMN System software was tailor made by its vendor, Syniverse Technologies. The resiliency and protection mechanisms of the 1CMN System had been considered during the design of the network architecture and capacity expansions, and were implemented effectively thereafter before the first incident. Prior to putting the 1CMN System with the abovementioned servers into operation, acceptance tests had been conducted by its vendor on the resiliency features including auto-switching, load balancing, electricity and network outage tests[9] to ensure that the designed protection mechanisms were working properly.

10. In order to prevent recurrence of similar incident, China Unicom submitted that it had –

(a) as an interim measure, replaced the defective CPUs of the malfunctioned server, and liaised with its vendor and hardware manufacturer to replace all the CPUs concerned of the other servers under the same batch;

---

[8] According to China Unicom, the 1CMN System is responsible for managing the Signalling System No. 7 messages between its MSC and its HLR.

[9] The test cases included abnormal power down and network cable unplug for the failover test examination. According to China Unicom, all the test results were positive. Those tests were conducted by its vendor to simulate the condition of hardware fault and network fault.

(b) applied software patch to the set of servers in the malfunctioned unit of the 1CMN System so that these servers would work as a standby system for contingency purpose while detailed and rigorous tests were conducted before applying the software patch to the production unit of the 1CMN System ("main system"); and

(c) worked with its vendor to develop a "fast restoration procedure" for the 1CMN System, with a view to shortening the restoration time to less than an hour under normal circumstances.

China Unicom's Representations on the Second Incident

11. According to China Unicom, the second incident was caused by a sudden surge of traffic on the second day of the Easter Holidays. This triggered another software bug that led to failure of China Unicom's 1CMN System. Although the designed maximum loading capacity of the 1CMN System should be more than sufficient to cope with the surge of traffic, the software bug triggered had caused abnormal signalling messages stacked in queue which substantially degraded the processing capacity of the 1CMN System.

12. China Unicom submitted that the root cause of the second incident was beyond its control since it was due to the software bug of the 1CMN System which rendered it unable to operate at its designed maximum loading capacity. According to China Unicom, a comprehensive load test had been conducted in the laboratory by its vendor before the system was put to service. However, as the scenario in the second incident could not be simulated in the test environment, the software bug was not discovered during the load test.

13. With regard to the standby system, China Unicom submitted that it was set up after the first incident, as a contingency plan, to serve as the backup of the main system in the event of failure in the latter. However, the standby system could not be started during the first attempt to activate it. According to China Unicom, the standby system entered into sleep mode after it had been left idle for eight hours. China Unicom claimed that it was not aware of such a sleep mode nor had it been informed by its vendor of that before the second incident.

14. In order to prevent recurrence of similar incident, China Unicom submitted that it had –

(a) upgraded the malfunctioned software to the latest version on 1 April 2018 with the software bugs identified in the two incidents fixed. A comprehensive acceptance test had also been conducted on the 1CMN System with the upgraded software;

(b) refined the acceptance test plan of the 1CMN System with new test items to specifically check the software problems identified during the two incidents; and

(c) made arrangement to closely monitor the 1CMN System.

OFCA's Assessment of the First Incident

15. OFCA notes that the software and hardware of the 1CMN System was procured from reputable hardware manufacturers and software vendors and that the incident was caused by a hardware problem which triggered a software bug that had not occurred before. OFCA also notes that China Unicom had taken measures to ensure stable operation of the 1CMN System through carrying out proper and regular maintenance activities and adopting a design to achieve resilience. During the material time of the first incident, the 1CMN System was operating with two production units and both of them acted as a backup to each other.

16. Notwithstanding the above arrangement, the software bug, which was triggered by the hardware fault of one of the servers, had rendered the 1CMN System unable to identify and isolate the malfunctioned server, and activate the Arrangement to cope with the problem according to the planned protection mechanisms. According to the information submitted by China Unicom, the software version which had fixed the abovementioned software bug was released on 17 August 2016, but it was not installed in the 1CMN System before the first incident which occurred on 27 February 2018. As such, OFCA does not subscribe to China Unicom's view that the disruption of its telecommunications services in the first incident was beyond its control. Although the hardware fault of the server triggered the first incident, the outage could be avoided had the updated software been installed prior to the first incident.

OFCA's Assessment of the Second Incident

17. According to the information provided by China Unicom, its vendor had conducted a comprehensive load test in the laboratory. OFCA notes that, similar to the first incident, the software version of 17 August 2016 or later version would fix the software bug which triggered the second incident on 31 March 2018. However, the relevant software version was only installed in the standby system but not in the main system before the second incident, even though China Unicom and its vendors had been well aware of the risk of failure of the main system due to software bug.

18. Similar to the first incident, the second incident could be avoided had China Unicom or its vendor expedited the installation of the software version of 17 August 2016 or later version on the 1CMN System before the second incident. Equally, the second incident could be avoided if there had been better communications between China Unicom and its vendor concerning the sleep mode of the standby system so that the standby system could be activated to take up traffic loading upon failure of the main system.

19. The two incidents clearly revealed that there were shortcomings in the design of the 1CMN System. Given the importance of the relevant software for proper operation of the 1CMN System, China Unicom and its vendor should closely monitor the developments of the software and proactively carry out updates with a view to minimising the risk to the normal operations of its mobile services.

20. In conclusion, having examined the facts and circumstances of the two incidents and the preventive measures taken by China Unicom, OFCA considers that the handling of software updates on the 1CMN System and the communications between China Unicom and its vendor were unsatisfactory. Neither China Unicom nor its vendor had recognised the importance of the software which could be a single point of failure for the entire 1CMN System.

Time and Actions Taken by China Unicom to Restore Services

China Unicom's Representations on the First Incident

21. China Unicom submitted that after detecting problems with the 1CMN service at about 10:50 am on 27 February 2018, China Unicom's network

engineers and its vendor immediately carried out investigation and attempted to restore the system but without success. At about 12:45 pm, the malfunctioned system was suspended by China Unicom's vendor for further testing. At about 1:00 pm, the NOC of China Unicom carried out the procedures to bypass the 1CMN System. At about 2:20 pm, all mobile outgoing voice services and mobile data services started to resume and customers were able to access to these services after completion of the location update process. After restoring the 1CMN System and performing call tests, China Unicom started to reverse the bypass procedures at about 4:15pm. After the 1CMN System started to take up normal traffic loading again, all the affected services including mobile voice services, SMS and mobile data services were resumed normal from 4:30 pm on 27 February 2018.

China Unicom's Representations on the Second Incident

22. China Unicom submitted that at about 11:15 am on 31 March 2018, when its NOC observed an abnormal alarm on the 1CMN System, its network engineers and its vendor immediately carried out investigation. China Unicom attempted to activate the standby system at 11:40 am but without success. At about 12:10 pm, China Unicom carried out the procedures to bypass the 1CMN System. At about 1:15 pm, all mobile outgoing voice services and data services started to resume and customers were able to access to these services after completion of the location update process. At about 2:15 pm, China Unicom's vendor attempted to restore the main system and the standby system. The standby system was successfully restarted at about 3:20 pm. However, due to high incoming traffic caused by repeated requests for location update by customers, China Unicom had to change the routing of the traffic to relieve the loading of the system. With the traffic back to normal level and having reversed the bypass procedures, all the affected services including mobile voice services, SMS and mobile data services began to resume normal from 6:40 pm on 31 March 2018.

OFCA's Assessment of the First Incident

23. OFCA considers that China Unicom's performance in restoring the services in the first incident was not satisfactory. In particular, China Unicom and its vendor had taken more than two hours to trouble shoot and to restart the relevant equipment before it decided to carry out the procedures to bypass the 1CMN System. Although China Unicom claimed that part of the services

including mobile outgoing voice services and mobile data services started to resume from 2:20 pm, other services including mobile incoming voice services and SMS remained inaccessible to the customers until 4:30 pm after the bypass procedures had been reversed and the 1CMN System started to take up traffic. The long duration of the outage (for more than five hours) of the mobile (incoming) voice services and SMS was unacceptable.

OFCA's Assessment of the Second Incident

24. OFCA considers that China Unicom's performance in handling the restoration of services in the second incident was also unsatisfactory. As pointed out by China Unicom, the affected services could have been restored earlier and the second incident could be avoided if the standby system could be activated as expected. Although China Unicom claimed that it was not informed of the sleep mode of the standby system by its vendor before the incident, this does not absolve China Unicom of its responsibility. China Unicom should have conducted thorough verification tests on the standby system and maintained close communications with its vendor to ensure that the standby system could be brought into operation as and when required. Further, despite its submission that service restoration was further delayed as a result of high incoming traffic and accordingly extra work was required to re-route the traffic to relieve the loading of the system, OFCA considers an outage duration of more than seven hours (with more than three hours to trouble shoot high loading issue and re-route traffic) to be unsatisfactory.

25. In conclusion, OFCA considers that the time and actions taken by China Unicom to restore the affected services in both incidents were not up to a satisfactory standard.

China Unicom's Communications with OFCA over the Service Disruption

China Unicom's Representations on the First Incident

26. According to China Unicom, the service disruption occurred at about 10:50 am on 27 February 2018, which was a weekday. It affected a total of about 138 150 customers and lasted for five hours and 40 minutes. Pursuant to the Guidelines, China Unicom should report the incident to OFCA by 11:20 am. According to OFCA's record, the first contact between China Unicom and OFCA was at 11:16 am but China Unicom had not provided

any further information on the progress or nature of the incident. It was not until around 4:22 pm, after OFCA had made several attempts to contact China Unicom, had it reported the details of the incident to OFCA.

27. Pursuant to the Guidelines, China Unicom should report to OFCA within one hour from the restoration of all the affected services, i.e. by 5:30 pm on 27 February 2018. According to OFCA's record, China Unicom had done so at about 4:39 pm on that day. The restoration of all the affected services was subsequently confirmed by China Unicom vide an email at 6:28 pm.

China Unicom's Representations on the Second Incident

28. According to China Unicom, the service disruption occurred at about 11:15 am on 31 March 2018, which was a public holiday. It affected a total of about 138 150 customers and lasted for seven hours and 25 minutes. Pursuant to the Guidelines, China Unicom should report the incident to OFCA by 12:30 pm. According to OFCA's record, the first contact between China Unicom and OFCA was at 1:12 pm but China Unicom had not provided any further information on the progress or nature of the incident. It was not until around 4:07 pm, after OFCA had made several attempts to contact China Unicom, had it reported the details of the incident to OFCA.

29. Pursuant to the Guidelines, China Unicom should report to OFCA within four hours from the restoration of all the affected services, i.e. by 10:40 pm on 31 March 2018. According to OFCA's record, in response to OFCA's enquiry, China Unicom informed OFCA at about 6:50 pm of the restoration of all the affected services from 6:40 pm.

OFCA's Assessment

30. 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 China Unicom should have reported to OFCA within 15 minutes after the triggering criterion was met. The second incident occurred on a public holiday and China Unicom should have reported to OFCA within one hour after the triggering criterion was met. China Unicom failed to meet the requirements stipulated in the Guidelines for reporting the occurrence of outage to OFCA on

both occasions (a delay of five hours and two minutes in the first incident and a delay of three hours and 37 minutes in the second incident). As for reporting the restoration of all the affected services to OFCA, China Unicom complied with the relevant reporting requirements for both incidents.

31. China Unicom had not been very proactive in keeping OFCA informed of the updated status of the incident during the disruption periods in both incidents, thus affecting OFCA's ability to make an accurate assessment of the severity of the incident and its impacts on the affected customers, and to offer timely advice and assistance to the public.

32. Overall speaking, OFCA considers that China Unicom had failed to comply with the Guidelines for reporting to OFCA on the occurrence of the incidents within the respective timeframes as stipulated. In addition, in both incidents, the manner in which China Unicom informed OFCA of the updated status of the incident during the disruption period was unsatisfactory.

China Unicom's Communications with Customers

China Unicom's Representations in Both Incidents

33. China Unicom submitted that in both incidents, it had made announcements on its official website and on its customer service page on Facebook to inform customers of the service disruptions. It had also notified the staff of its customer service hotline centre, provided them with the relevant information about the incidents, and increased the manpower of the centre to answer customer enquiries. Details of the relevant communications are as follows –

(a) In the first incident,

(i) announcements were posted on China Unicom's official website at 12:11 pm and 7:00 pm on 27 February 2018;

(ii) announcements were posted on China Unicom's customer service page on Facebook at 1:41 pm and 7:21 pm on 27 February 2018;

(iii) internal notifications were dispatched to the staff of China Unicom's customer service hotline centre at 12:00 pm on 27 February 2018; and

(b) In the second incident,

(i) announcements were posted on China Unicom's official website at 4:00 pm and 8:20 pm on 31 March 2018;

(ii) announcements were posted on China Unicom's customer service page on Facebook at 3:06 pm and 7:35 pm on 31 March 2018;

(iii) internal notification was dispatched to the staff of China Unicom's customer service hotline centre at 11:15 am on 31 March 2018.

34. According to China Unicom, it had received a total of 4 007 and 1 604 complaints/enquiries regarding the first incident and the second incident respectively. OFCA had received a total of 16 and eight complaints/enquiries from the public about the first and second incidents respectively. The complaints/enquiries can be classified into the following areas –

(a) repeated disruptions of China Unicom's mobile services within about a month;

(b) the long disruption periods in both incidents;

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

(d) China Unicom's customer service hotline was always engaged.

OFCA's Assessment

35. After examining the actions taken by China Unicom and the complaints/enquires from the public, OFCA is of the view that China Unicom had failed to provide customers with timely information about the two incidents.

36. For the first incident, OFCA notes that China Unicom made the first notification to its customers (by posting a message on its official website) at 12:11 pm on 27 February 2018, which was one hour and 21 minutes after the occurrence of the service disruption. For the second incident, China Unicom made the first notification to its customers (by posting a message on its customer service page on Facebook) at 3:06 pm, which was three hours and 51 minutes after the occurrence of the service disruption. In OFCA's view, pursuant to the Guidelines, China Unicom should have informed its customers in an expeditious and effective manner and made public announcement over mass media channels when communications channels were severely interrupted by the outage. Although China Unicom notified its frontline staff and provided them with the relevant information about the two incidents to respond to customers' enquiries, OFCA received complaints/enquiries from members of the public to the effect that the China Unicom's customer service hotline during the outage period was always engaged and they could not get through to China Unicom's staff.

37. Overall speaking, OFCA considers that the arrangements made by China Unicom in notifying its customers of the service disruptions were unsatisfactory in both incidents. China Unicom should improve its internal procedures to ensure timely and effective dissemination of information to its customers in the event of service disruption in the future.

THE CA'S CONSIDERATION AND DECISION

38. Having examined all the facts and circumstances of both incidents, including the representations of China Unicom and the assessment of OFCA, the CA considers that China Unicom has –

(a) failed to ensure the proper operation of its 1CMN System and to maintain it with the latest software version, hence resulting in the two incidents of service disruptions;

(b) in both incidents, failed to restore the mobile voice services, SMS and mobile data services within a reasonable timeframe;

(c) in the second incident, failed to obtain necessary information from its vendor and to conduct necessary verification tests on the standby system to ensure that it could be activated as and when required;

(d) in both incidents, failed to comply with the Guidelines to report to OFCA the occurrence of the incidents within the respective timeframes as stipulated therein; and

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

39. In conclusion, the CA considers that in both incidents China Unicom failed to comply with GC 5.1 of its SBO Licence (Licence No. 922), which requires it to operate, maintain and provide a good, efficient and continuous service in a manner satisfactory to the CA. In view of the severity of both incidents, the CA considers that China Unicom should be imposed a financial penalty pursuant to section 36C(1)(a) of the Telecommunications Ordinance (Cap. 106) ("TO"). Furthermore, due to the similar nature of the two incidents which occurred within a relatively short period of time and were caused by problems of similar nature, the CA considers it appropriate to consider the two incidents together as a single occasion of breach.

FINANCIAL PENALTY

40. 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.

41. This is the second occasion[10] where China Unicom is to be imposed a financial penalty for non-compliance with GC 5.1 of its licence, and the maximum penalty stipulated by the TO is $500,000. In considering the appropriate level of financial penalty, the CA has paid regard to the Guidelines on the Imposition of Financial Penalty under Section 36C of the TO (the "Financial Penalty Guidelines")[11]. Under the Financial Penalty Guidelines, the CA will consider a number of factors including the gravity of the breach (which includes the nature and seriousness of the infringement); whether any repetition

[10] There were disruptions of the telecommunications services of China Unicom on 3 April and 5 April 2015. The CA decided that China Unicom had not complied with GC 5.1 of its licence and a financial penalty was imposed on China Unicom. A copy of the CA's decision is available at https://www.coms-auth.hk/filemanager/statement/en/upload/343/Unicom_FinalDecision_e.pdf.

[11] The document is available at http://tel_archives.ofca.gov.hk/en/legislation/guideline_6d_1/guideline_6d_1_150402.pdf.

of conduct is involved; and whether there are any aggravating or mitigating factors.

42. 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 two service disruptions were serious because –

(a) about 138 150 customers of China Unicom using its 1CMN service were affected in each of the two incidents;

(b) the mobile voice services and SMS were disrupted for five hours and 40 minutes in the first incident and seven hours and 25 minutes in the second incident; and

(c) the scope of service disruption was extensive, covering mobile voice services, SMS and mobile data services.

43. Drawing reference from precedent cases of breach of licence conditions where financial penalties were imposed, the CA considers that the appropriate starting point for determining the level of financial penalty should be $250,000. In considering the mitigating factors, the CA notes that China Unicom has provided full cooperation to OFCA in the course of the investigation. China Unicom has also taken prompt and responsible actions to implement preventive measures against the recurrence of similar incidents. The CA has not identified any aggravating factor which should be taken into account.

44. Having carefully considered the circumstances of both incidents and taken all factors into account including China Unicom's representations of 7 September 2018, the CA concludes that a financial penalty of **$160,000** is proportionate and reasonable in relation to the breach.

IMPROVEMENT MEASURES

45. In addition, the CA recommends China Unicom to implement the following measures to prevent the recurrence of similar incidents in the future, and to enhance its capability in handling service disruptions –

(a) conduct a holistic review of the design of its 1CMN System, including the relevant hardware and software platforms as well as the resiliency and protection mechanisms, to ensure that the 1CMN System is resilient, reliable, stable and up-to-date;

(b) review the process of service restoration and liaise with its vendors in order to work out an efficient and effective contingency plan, which may include a clear and effective communications mechanism among relevant parties and an expeditious service restoration arrangement to shorten the service disruption time as far as possible; and

(c) review and improve its internal procedures to ensure more timely and effective dissemination of information to its customers and OFCA in the event of service disruption.

The Communications Authority
October 2018