Tribunal meeting number 284

Case reference: 189274
Level 2 provider: Moblix Media Limited
Type of service: Subscription alerts service
Level 1 provider: Tap2Bill Limited

This case was brought against the Level 2 provider under paragraph 4.5 of the 14th Edition of the Code of Practice of the Code of Practice.

Background

1. This case concerned a subscription alerts Service called "f(b) Friday" ('the Service') which provided consumers with voucher codes and discount offers for retail stores. The Service was provided by Moblix Media Limited ('the Level 2 provider') and the Level 1 provider was Tap2Bill Limited the ('the Level 1 provider').

2. The Service charges were stated to be a maximum of £2 per month. This consisted of a maximum of two reverse billed £1 messages per month from the shortcode 84222. The Service information supplied by the Level 2 provider, indicated that the Service used the Mobile-Originated (MO) keyword opt-in method. To subscribe to the Service, users would have to text the keyword 'Freeb' to shortcode 84222.

3. The Service had been in operation for a significant period of time. The Level 1 provider indicated that the Service had been in operation for '*nearly eight years*'. The Level 2 provider stated in its correspondence with the Executive, that the Service was suspended on 25 September 2020 after a technical issue had resulted in the billing of thousands of MSISDNs.

The investigation

4. The Level 2 provider and Service have previously been subject of a Track 2 procedure. On 6 March 2014, the Tribunal upheld breaches of the Code of Practice (12th Edition), namely Rule 2.3.3 (Consent to charge), Rule 2.2.5 (Pricing prominence and proximity) and Rule 2.2.1 (Information likely to influence the decision to purchase). As a result of the sanctions that were imposed as part of the previous adjudication, the Level 2 provider had previously sought and implemented compliance advice in relation to the Service.

5. On 28 September 2020, a significant issue regarding the Service was brought to the attention of the Executive by the Level 1 provider. The Level 1 provider informed the Executive that a technical issue on the Level 2 provider's platform had resulted in 25,770 consumers being overcharged on 25 September 2020. The incident resulted in

the Executive receiving 220 complaints from consumers affected by this incident. The complaints from these consumers alleged that they had not signed up to the Service or agreed to be charged by it and that they were unaware of how they had come to receive the chargeable messages.

6. In addition to the 220 complaints, the Executive also received 91 complaints about the Service from May 2018 to August 2020 (prior to the technical incident). These complainants also alleged that they had not signed up to the Service or agreed to be charged for the Service.

7. The Executive also received information from a whistleblower ('**the Whistleblower**') regarding the Service. The Whistleblower stated that the Level 2 provider had obtained a significant number of consumers' MSISDNs (mobile telephone numbers) from an external public events venue and that the Level 2 provider had charged these consumers without their consent.

8. Documentation was provided by the Whistleblower which included an analysis report and two witness statements by a Developer and Technical Operator of the Level 2 provider's system and a Data Analyst. The Executive was also provided with a list of MSISDNs which are alleged to have been taken from the public events venue.

9. The Level 2 provider engaged with the investigation and submitted evidence in response to the Executive's directions for information. However, the Executive was of the view that the Level 2 provider failed to co-operate fully and raised breaches in respect of this.

Apparent breaches of the Code

10. The Executive sent a Warning Notice to the Level 2 provider on 1 July 2021 in which the following breaches of the Code were raised:

    - Breach 1 Rule 2.3.3 - Consent to charge
    - Breach 2 Rule 2.3.3 - Consent to charge
    - Breach 3 Paragraph - 4.2.3 Failure to disclose information requested
    - Breach 4 Paragraph - 4.2.2 Provision on false information

11. The Tribunal was originally scheduled to take place on 15 September 2021 however the Tribunal was adjourned on the application of the Executive with the agreement of the Level 2 provider. The Tribunal was re-scheduled to take place on 28 October 2021 but was adjourned on that occasion on application of the Level 2 provider.

12. On 24 November 2021, the Tribunal reached a decision regarding the alleged breaches. The Level 2 provider was in attendance to make oral representations to the Tribunal.

Submissions and conclusions

Alleged breach 1

Rule 2.3.3 Consent to charge
Consumers must not be charged for PRS without their consent. Level 2 providers must be able to provide evidence which establishes that consent.

13. The Executive submitted that a breach of the Rule 2.3.3 of the Code had occurred as the Level 2 provider had not obtained consent to charge consumers and as the Level 2 provider had charged consumers more than the cost of the Service.

14. In support of its case, the Executive relied on the consumer complaints and the discrepancies in the message logs which had been provided by the Level 1 and Level 2 providers. The Executive also relied on the evidence from the Whistleblower which alleged that consumer MSISDNs had been obtained from a public events venue database without consumer consent and that those consumers had then been charged for the Service. The Whistleblower also supplied evidence that consumers had been overcharged regularly by a process known as a 'whoops' once they signed up to the Service.

15. The Executive explained that it was initially contacted by the Whistleblower, who alleged that the Level 2 provider had obtained a significant number of consumers' MSISDNs from external sources and that these consumers had been charged without their consent.

Complainant evidence (May 2018- August 2020)

16. As a result of this contact, the Executive reviewed the 91 complaints that it had received concerning the Service between May 2018 to August 2020 (prior to the incident on 25 September 2020). The Executive was unable to review any complaints prior to May 2018 as complaints prior to this time could not be accessed as a result of the GDPR restrictions on the Executive's systems.

17. The Executive noted that various complainants had stated that the charges they had incurred were unsolicited. The complainants also stated that they had not signed up to the Service or agreed to be charged and therefore did not know how the Level 2 provider had obtained their MSISDNs. Some examples of the complaints received by the Executive are set out below:

"I have been being charged for a premium rate subscription I haven't signed up too"

"I never Knowingly signed up for this service. I first started receiving messages from this service in March 2016. I texted stop on 30 April 2017 and 15 September 2017 and received a confirmation the service would be stopped on each occasion. I never knew that there was a charge for this service so saw it as a nuisance only and blocked it on my phone

on 26th April 2019. When checking my phone bill this morning I noticed that I have still been charged for this service at an average of 8 messages a month each costing £1."

"I have just realised that I have been incurring extra charges on my mobile phone bill for several months due to unsolicited premium spam messages sent to my mobile, (which appear as number 84222). After VAT this amounts to approx. £10/month for several months."

"I received texts from this number which I did not subscribe to, I blocked the number but still being charged, £5 in one month."

"I have never subscribed to 84222 and yet I have been charged twice now for a subscription service I do not want or use"

"I received a text from this number in February but have no idea how they received my number as did not sign up to their service? I received another text in March and then saw on my 02 bill I had been charged £0.83 each time for receiving these texts. I then text the word STOP as per the text to stop receiving messages from this number when I realised I was being charged and was charged £0.083 for doing this. I received a message back saying FREE MSG. Thank you for your STOP message. You will no longer receive messages from this short code. However just now I have received another text from them which has cost me again."

"...i have been charged £3 in relation to texts from this number. I know i did not register with them. The first text was 8th feb and i thought it was just spam, i then received a further 2 texts on 15th february and have just realised that vodafone are applying a £1 charge per text"

"This company have been sending me messages, which I did not sign up for. The charge is £0.83 per time. I have been charged a total of £28.32 over the past several months"

Level 1 and Level 2 provider message logs

18. During the course of the investigation, the Executive requested that the Level 2 provider supply message logs for each of the 91 complainants, showing all the transactions between the complainants' MSISDNs and the Service. The Executive was provided with 73 message logs by the Level 2 provider. The Executive also asked the Level 2 provider for information on how the Service was intended to operate.

19. The Executive noted that the Service operated solely on shortcode 84222 and that it used an MO keyword opt-in method. Subscribers to the Service were to be charged a maximum of £2 per month according to the Level 2 provider.

20. Through analysing the message logs from the Level 2 provider, the Executive noted that the MO 'Freeb' appeared to have been sent by consumers to 84222 to request the Service. The Executive noted that the message logs suggested that the MO keyword was also subsequently by consumers which suggested ongoing use of the Service.

21. The Executive further observed that in 66 out of the 73 message logs which were supplied by the Level 2 provider, consumers had been charged for more than two chargeable £1 messages per month meaning that they had been overcharged. The Executive noted that the overcharging appeared to occur frequently and that in some cases consumers had been sent up to eight chargeable £1 messages.

22. The Executive illustrated the issue using two examples: In the case of MSISDN 07xxxxxxxx2, the Executive noted that the MO keyword was originally sent on 3 April 2019 to subscribe to the Service. This was followed by subsequent MO messages sent on 26 April 2019, 28 June 2019, 26 July 2019, 31 August 2019, 27 September 2019 and 25 October 2019. The message logs indicated that although the Service cost was £2 per month, the Level 2 provider's message logs showed that in August 2019, four chargeable messages were delivered to the consumer which amounted to an overcharge of £2. In the month of September 2019, five chargeable messages were delivered to the consumer, totalling an overcharge of £3. The Executive also noted that three chargeable messages were delivered in October 2019 and November 2019 – an overcharge of £1 in both months.

23. In relation to a second MSISDN, 07xxxxxxxx5, the Executive noted that the message logs indicated that the MO keyword was sent to subscribe to the Service on 12 February 2019. Subsequent MO messages were sent on sent on 22 February 2019, 29 March 2019, 26 April 2019, 28 June 2019, 26 July 2019, 31 August 2019, 27 September 2019 and 25 October 2019.

24. The Executive observed that the Level 2 provider's message log for 07xxxxxxxx5 showed that in August 2019, four chargeable messages were delivered to the consumer resulting in an overcharge of £2. In the month of September 2019, four chargeable messages were also delivered which amounted to another overcharge of £2. The Executive also noted that three chargeable messages were delivered in October 2019 – an overcharge of £1 and five chargeable messages were delivered in November 2019 – an overcharge of £3.

25. The Executive further relied on the message logs that it had obtained for the Level 1 provider in support of the breach.

26. The Executive noted that there were significant discrepancies between the message logs of the Level 1 provider and the Level 2 provider. For example, in relation to the MSISDN 07xxxxxxxx2 above, the Level 1 provider's message logs indicated that no MO messages had been sent by the consumer, save for the keyword 'STOPALL' on 13 January 2020. In addition to this, the Level 1 provider's logs indicated that the consumer had been overcharged by more than was indicated by the Level 2 provider's logs.

27. Similarly, the Executive noted that in relation to MSISDN 07xxxxxxxxx5, the Level 1 provider logs indicated that no MO messages had been sent by the consumer save for

the keyword 'STOPALL' on 16 December 2019. As with the other example, the Executive also observed that the consumer had been sent more chargeable messages and was therefore subsequently overcharged by more than what was indicated by the Level 2 provider's logs.

28. Due to the discrepancies in the message logs, the Executive sought to investigate the matter further by sending a sample of ten message logs from the Level 2 provider to the Level 1 provider in May 2021. The Executive explained that in response to these further enquiries, the Level 1 provider had confirmed that its records were correct and that it did not have records of the MO messages containing the keyword 'Freeb' for the MSISDN sample that was sent to it. The Level 1 provider also indicated that it was concerned in relation to the possible overcharging.

Evidence from the Whistleblower

29. In addition to all of the above, the Executive relied on the Whistleblower's evidence in support of this breach. The Whistleblower stated that the Level 2 provider had obtained MSISDNs through sources which did not relate to the Service. The evidence from the Whistleblower indicated that the Level 2 provider had commenced sending unsolicited text messages to those MSISDNs. The Whistleblower further claimed that in at least one incident, the Level 2 provider had obtained a significant number of MSISDNs from a public events venue in which the Director of the Level 2 provider's IT company had installed a public Wi-Fi system.

30. The Whistleblower supplied a list containing 36,394 MSISDNs (12,564 MSISDNs with the duplicates filtered out) which it claimed had been taken from the public events venue's database, imported to the Level 2 provider's system, and sent unsolicited chargeable messages. The Executive reviewed 91 complaints and noted that 20 of those MSISDNs appeared on the list obtained from the public events venue's database.

31. The Executive concluded by submitting that there was clear evidence that a breach had occurred as a result of the complainant accounts and as the Level 1 provider's messages logs which demonstrated that MO messages had not been sent to initiate the Service. The Executive further submitted that the evidence from the Whistleblower supported its case that a breach had occurred.

Level 2 provider's response

32. The Level 2 provider denied the breach.

33. The Level 2 provider stated that the trigger for the investigation had been when the Whistleblower first contacted the Executive back in March 2020. The Level 2 provider explained that since the last adjudication in 2014, the Service had operated compliantly and that the Executive had not indicated that it had any concerns in respect of the Service until it was contacted by the Whistleblower.

34. The Level 2 provider emphasised that the evidence of the Whistleblower should be considered as wholly unreliable and malicious. The Director of the Level 2 provider explained that there was a long running dispute between himself and the Whistleblower regarding the ownership of an IT company and that the Whistleblower had a vendetta in respect of the Level 2 provider.

35. The Director of the Level 2 provider explained that this had culminated in the Whistleblower removing the Director of the Level 2 provider from the IT company for ten days in late 2019. The Director of the Level 2 provider stated that in this ten-day period, the Whistleblower (in conjunction with other individuals) had extracted the Moblix Media Limited database and corrupted its data. The Level 2 provider indicated that it was for this reason that it was unable to supply all of the information requested by the Executive.

36. The Level 2 provider relied on copies of a Court order which confirmed that an injunction had been made on 17 December 2019 in respect of the Whistleblower. The terms of the injunction allowed the Director of the Level 2 provider to resume his position within the IT company. The Level 2 provider confirmed that further Court proceedings took place following that time, and that these were finally resolved in May 2021. The Level 2 provider confirmed that it could not disclose the outcome of those proceedings for legal reasons.

37. In addition to this, the Level 2 provider also clarified that a number of the responses that had been sent to the Executive, had been sent by an individual within the Level 2 provider and not the Director. The Level 2 provider explained that it was this individual who had day to day responsibility for the running of the Service since the last adjudication in 2014 but that that they had now left the Level 2 provider's employment. The Level 2 provider indicated that it was likely that this individual was working in collaboration with the Whistleblower.

38. During oral representations to the Tribunal, the Level 2 provider stated that the discrepancies between the Level 1 providers message logs and the logs supplied by the Level 2 provider were attributable to the use by the Level 2 provider of another aggregator in order to send the MO keyword messages. The Level 2 provider indicated that for this reason, the Level 1 provider's logs would not show copies of the MO keyword messages that had been sent in by consumers.

Tribunal's decision

39. The Tribunal carefully considered the evidence put forward by both the Executive and the Level 2 provider applying the civil standard of proof

40. The Tribunal noted that this consent to breach was concerned with the time period from May 2018 until August 2020. The Tribunal noted that 91 consumer complaints had been received in this time period, and that the complainant evidence was

consistent in that consumers had repeatedly stated that they did not sign up to the Service and had received unsolicited charges.

41. The Tribunal also considered the message logs supplied by the Level 1 provider and the Level 2 provider. The Tribunal noted that the Level 2 providers logs taken on their own showed that consumers had also been overcharged by the Service on a number of occasions. The Tribunal further noted that the Level 1 provider logs also showed that overcharging had occurred but the Level 1 provider's logs indicated that consumers had been overcharged by more than the Level 2 provider's logs indicated.

42. The Tribunal considered the Level 2 provider's explanation that the use of a third-party aggregator meant that the message logs submitted by the Level 1 provider would not have shown the MO keyword messages that were in fact sent by consumers (which appeared on the Level 2 provider logs) and that this was the cause of the discrepancy.

43. The Tribunal noted that Level 2 provider had not previously indicated that there was any third-party aggregator in any of its responses to the Executive or provided any evidence of it, It was raised at the Tribunal for the the first time. t The Tribunal noted that the Level 2 provider had not provided any evidence which supported its assertion that a third-party aggregator had been used.

44. The Tribunal also observed that the Level 1 provider had confirmed that some MO keyword messages did appear in its logs, but not in respect of the consumers that had complained about the Service. In addition to this, the Tribunal also noted that the Level 1 provider had stated to the Executive that the only way in which the MO keyword messages would not have appeared, is if a different shortcode had been used that did not belong to the Level 1 provider. The Tribunal however noted that the Level 2 provider had not suggested that any different shortcode was being used.

45. As a result of all of the above, the Tribunal was unable to accept the explanations put forward by the Level 2 provider regarding the MO keyword opt in messages. The Tribunal was therefore of the view that it had no evidence before it to suggest that the MO keyword opt in messages had been sent by in by the complainants.

46. In addition to this, the Tribunal was of the view that even if some of the data had been destroyed or corrupted as described by the Level 2 provider, this did not explain why the Level 1 provider's message logs also demonstrated that consumers had been overcharged for the Service.

47. For all of the reasons above, the Tribunal was of the view that there was sufficient evidence to find the breach proved on the balance of probabilities. In reaching its decision, the Tribunal did not feel it necessary to rely on the evidence put forward by the Whistleblower. The Tribunal considered that it was therefore able to reach its decision solely on the basis of the cogent evidence of consumer complaints and the message logs from the Level 1 and Level 2 provider.

Decision: UPHELD

Alleged breach 2

Rule 2.3.3 Consent to charge
Consumers must not be charged for PRS without their consent. Level 2 providers must be able to provide evidence which establishes that consent.

Technical incident

48. The Executive submitted that a further breach of paragraph 2.3.3 of the Code had occurred. The Executive submitted that this breach had occurred as a result of the following:

    - the technical issue which occurred on 25 September 2020 which resulted in the Level 2 provider charging consumers. The majority of consumers were charged were charged more than the costs of the Service.
    - the Level 2 provider had not obtained consent to charge the affected consumers.

49. By way of background the Executive stated that it had been contacted on 28 September 2020 by the Level 1 provider, who reported that a technical error had occurred which resulted in the overcharging of consumers. On 13 October 2020, the Level 1 provider supplied further details of the issue to the Executive as follows:

    "The error which caused the incident on 25 September 2020, which is the subject of this investigation, occurred on the merchant's platform. Moblix Media reported that it had recently moved its service to a new platform. In addition, Moblix Media made an update to their service at this time to allow a higher 'throughput' of messages when sending via the Tap2Bill messaging gateway. A programming error in the update on the new Moblix Media platform resulted in messages (that were separated into arrays (an ordered series)) being sent in a cumulative way, instead of in individual one-time batch sends.
    Each array should send their allocated message batch as the program cycled through the batches. However, the error added all the previously sent arrays messages to the current processing one, resulting in an ever-increasing amount of duplicated sends. The Batch 1 send was correct, but Batch 1 was not then deleted after the send. Batch 1 was then added to the Batch 2 send and both were sent, but again, not deleted. Batches 1 and 2 were then added to the Batch 3 send, etc."

50. The Executive relied on the evidence from a number of complainants. In total 220 consumers made a complaint regarding the Service on or after the incident which occurred on or after 25 September 2021. Some of the examples of the consumer complaints which were relied on by the Executive are set out below:

"I received around 16 unsolicited messages In the space of a few minutes from the above. It read: "f (b) fri lockdown offer goto www.freebee.eu/claim enter code COFFEE be sure to claim by 4PM 27/09 Unsubscribe? Txt FREEB STOP 84222 or call 02032913904". I have not signed up for this service."

"I have been charged premium rate texts from this number. I have never signed up to the service and never even heard of them. I have been bombarded by text messages from them 15 with 5 seconds. The same message over and over again."

"Premium text for around £1 x 8 lots over a minute.
Not instigated by myself and no idea how these people got my number"

"I received 81 text messages from 84222 in under 2 minutes this evening. I have no idea what the number relates to, but am now worried I am going to be charged."

"I have received dozens of SMS messages from 842 22. I have never heard of or signed up to this service.
I then received a message from Vodaphone that I had been charged £100 in SMS messages."

"I have not subscribed to the service but received £30 of charges following a barrage of incoming texts messages from them. They have unlawfully contacted me without my consent and I now have the charges on my phone bill."

"This company sent 147 text messages within a minute or two. I have never heard of this company and have never signed up with them. I have now received multiple charges on my phone bill totalling £25 (my cap limit) without my agreement."

"I received 20 premium texts between 17.37 hrs and 17.40hrs on 25th September 2020 each text charging £0.83 to my monthly bill from O2. I had not given authorisation for the texts or subscribed to any premium service. The only change to my phone, (for the last 2 years) was the down loading of the NHS covid app on 25th Sept."

"I recieved 149 text messages from 84222 between 21:17 and 21:18, in just one minute, on Friday 25th September! I blocked the number straight away when I saw my phone was going crazy. However, I then woke up to a text from O2 saying I was being charged £124.12 for these 149 texts at 83p each!!!! Unacceptable.
I've never ever subscribed to this 84222 company for anything, ever. I tried to contact Freebe as on the text that's who they said they were but there's never an answer."

"I had never heard of the service before receiving dozens of premium texts from them within a few minutes. I blocked and deleted the number, and a few days later received a text listed as coming from "Freebee": "We are aware of a technical issue that means you've received premium messages you didn't request. We will be in touch shortly to arrange a full refund.""

"I did not authorise this company to text me or seek any information on any level from them. The number is 84222 and the company name is Moblix Media Limited and I have been charged £1 for text messages sent consecutely on 25th Sept commencing at 20.01 and going on for over 4 hours adding £73 to my bill. ID mobile, my provider say they cannot do anything. Please advise the next step in an effort to recover my outlay. I have left a number of messages for the company and sent emails but no reply"

"I recieved 149 text messages from 84222 between 21:17 and 21:18, in just one minute, on Friday 25th September! I blocked the number straight away when I saw my phone was going crazy. However, I then woke up to a text from O2 saying I was being charged £124.12 for these 149 texts at 83p each!!!! Unacceptable.
I've never ever subscribed to this 84222 company for anything, ever. I tried to contact Freebe as on the text that's who they said they were but there's never an answer."

"I had never heard of the service before receiving dozens of premium texts from them within a few minutes. I blocked and deleted the number, and a few days later received a text listed as coming from "Freebee": "We are aware of a technical issue that means you've received premium messages you didn't request. We will be in touch shortly to arrange a full refund.""

"I did not authorise this company to text me or seek any information on any level from them. The number is 84222 and the company name is Moblix Media Limited and I have been charged £1 for text messages sent consecutely on 25th Sept commencing at 20.01 and going on for over 4 hours adding £73 to my bill. ID mobile, my provider say they cannot do anything. Please advise the next step in an effort to recover my outlay. I have left a number of messages for the company and sent emails but no reply"

"I was unaware of these charges being applied to my mobile phone bill until my spend cap and data cap was reached. I checked my account after being alerted to the cap and saw texts from a premium service 84222 (and one other, which is also unauthorised) creating an excess charge to my monthly calling plan.
I do not recognise these texts, they did not display on my phone, I did not authorise them and did not subscribe to them (or any premium service). I think this is fraudulent and should be stopped, therefore I am reporting it."

51. The Executive observed that the Level 2 provider had accepted in its responses to the Executive that a technical issue had occurred. In response to the Executive's direction of 16 October 2020 for example, the Level 2 provider stated that the technical issue was as a result of "*an incorrect coding change in our new platform to improve message throughput via our aggregator*".

52. In addition to this, the Level 2 provider also provided information describing how the technical issue had occurred:

    "The revised script correctly created the messages and then began cycling through each scheduled message, one per subscribed MSISDN, to create the outbound format.

    These batched messages were placed into separate arrays and then sent to the respective gateway [Tap2Bill].

    Each individual arrays should have been cleared down after each cycle but this did not happen due to the platform coding error. The consequence was that the array grew with duplicates in each subsequent cycle after the first cycle of 40 messages. This error therefore caused incremental cycles; cycle 1 was ok, then cycle 2 had cycle 1 and cycle 2 data in it, cycle 3 had 1,2 and 3 and so on."

    Furthermore, the Level 2 provider stated that *"the failure of the number arrays to be deleted after a send request was submitted to Tap2Bill caused a corruption of the send string to include additional numbers other than our active base"*.

53. The Executive further submitted that a breach had occurred as the Level 2 provider had not obtained consent from consumers to be charged for the Service.

Evidence of consent to charge

54. The Executive stated that it had requested evidence from the Level 2 provider of how it came to be in possession of all the MSISDNs that were billed on 6 October 2020 following on the incident of 25 September 2020. The Level 2 provider responded to this request on 16 October 2020 confirming that all MSISDNs billed had been identified as "*Active Subscribers, non -Active (previously subscribed) and Marketing*".

55. The Level 2 provider also stated on 16 October 2016 that it was unable to provide any data as the technical error that had occurred had also led to a corruption of its database and the cross contamination of data. The Level 2 provider indicated that it was attempting to recover the data from an archive which was held by a previous supplier.

56. However, on 16 December 2020, the Executive asked for an update from the Level 2 provider on the data recovery. The Executive further requested that the Level 2 provider send in any supporting evidence in relation to the data recovery such as any correspondence that it had sent to the former supplier who held the archive data. The Executive further requested that the Level 2 provider supply separate MSISDN lists of active subscribers, non-active subscribers and marketing groups that the Level 2 provider previously referred to. The Executive submitted that none of this information was forthcoming and that the Level 2 provider had responded as follows:

    "Our old data is not recoverable, as per the link it was available for up to a maximum of 180 Days
    https://docs.microsoft.com/en-us/compliance/assurance/assurance-data-retentiondeletion-and-destruction-overview"

57. The Level 2 provider confirmed that it had never used advertising to promote the Service however during the lockdown it had used direct print promotions which were placed in online delivery orders to promote the Service.

58. The Executive relied on the message logs that it obtained from the Level 1 provider which showed all of the transactions between the 220 complainants and the Service. The Executive noted from the message logs that only four out of the 220 complainant MSISDNs had received any messages from the Service prior to the technical incident and that no MO messages were sent by any of the 220 complainants to request the Service.

59. The Executive submitted that as result of all of the above, a breach of the Code had occurred as consumers had not only been overcharged without their consent as a result of the technical error, but also as there was no evidence that the affected consumers had consented to be charged by the Service.

60. When further questioned by the Tribunal, the Executive accepted that all consumers had received refunds but stated that there was nonetheless consumer harm as not all of the harm was solely financial.

Level 2 provider's response

61. The Level 2 provider denied the breach. In oral representations to the Tribunal, the Level 2 provider explained that it did not deny that the technical issue had occurred but explained that this had not been done deliberately. The Level 2 provider also stated that no harm had occurred as all consumers that were affected by the incident had been refunded.

62. The Level 2 provider stated that it had not gained any benefit as a result of the incident, and that it would have served no purpose to charge consumers in this way intentionally as the issue would have been readily discovered.

Tribunal's decision

63. The Tribunal carefully considered all of the evidence before it. The Tribunal noted that there was no dispute that the technical incident had occurred and that the Level 2 provider had accepted this.

64. The Tribunal was minded to accept the assertions of the Level 2 provider that the technical incident of itself was not deliberate. In addition to this, the Tribunal also noted that it was accepted by all parties that the affected consumers had been refunded.

65. However, while the Tribunal was of the view that the technical incident may not have been deliberate, the Tribunal was concerned that there was no evidence before it to suggest that any of the affected consumers had ever consented to be charged by the Service. The Tribunal noted in particular for example that only four complainant MSISDNs had any interaction with the Service prior to the incident and that the Level 1 provider message logs indicated that there had been no MO keyword opt-in messages from any of the complainants.

66. Having previously discounted the evidence of there being a third-party aggregator (which would have held the details of the MO keyword opt-in messages) as only one shortcode had been used, the Tribunal were of the view that there was no evidence that any of the 220 complainants had consented to be charged for the Service at any stage.

67. Although the Tribunal accepted that all consumers had received refunds, it was also of the view that this did not mean that no harm had occurred, as the harm may have included harm that was other than financial in nature, such as alarm and distress at being charged at all. The Tribunal considered that this was evident from some of the complainant accounts.

68. As a result of all of the above, the Tribunal was satisfied on the balance of probabilities that a further consent to charge breach had occurred. The Tribunal considered that this breach related solely to the complainants affected by 25 September 2020 incident. The Tribunal was of the view that there was clear undisputed evidence that consumers had been overcharged as a result of the technical error and that these affected consumers had not consented to be charged for the Service. As with the previous breach, the Tribunal reached its decision solely on the evidence of the complainants and the evidence produced by the Level 1 and Level 2 providers which it considered to be cogent and compelling. The Tribunal did not consider it necessary to rely on the evidence of the Whistleblower in light of this.

Decision: UPHELD

Alleged Breach 3

Paragraph 4.2.3 of the Code

Where a direction is made pursuant to Paragraph 4.2.1, a party must not fail to disclose to the PSA, when requested, any information that is reasonably likely to have a regulatory benefit in an investigation.

Directions for information

69. The Executive submitted that the Level 2 provider had breached paragraph 4.2.3 of the Code as the Level 2 provider had failed to provide information which was likely to have a regulatory benefit.

70. The Executive stated that following the technical incident on 25 September 2020, it had sent a direction to the Level 2 provider requesting an explanation of how the incident had occurred, details of the billing process, advertising material and how the Level 2 provider had come to have the MSISDNs which had been charged.

71. In its response to this direction, on 6 October 2020 the Level 2 provider explained how the error had occurred. However, in response to the request for information on how it came to hold the MSISDNs it had charged, the Level 2 provided stated that the technical error had led to a corruption of data and that it was attempting to recover that data from the archive which was held by a former supplier. The Level 2 provider indicated that it would present this information to the Executive once it was received.

72. On 16 December 2020, the Executive requested evidence of all correspondence including evidence of the steps that had been taken to improve the system, an update on the data recovery attempts with supporting evidence as well as the subscriber and marketing lists.

73. In its response to this request, the Level 2 provider stated that there was no evidence of any proposals to improve the system as all meetings had taken place over the telephone or verbally. The Executive noted that the Level 2 provider also stated in this response that "*our old data is not recoverable, as per the link it was available for up to a maximum of 180 days"* despite previously having stated that it was in contact with a previous supplier to obtain data from the archive.

74. The Executive also noted that its initial request on 6 October 2020 and the Level 2 provider's response to the request had occurred within the 180 day time limit and was therefore of the view that this explanation did not account for the missing data.

75. As a result of the Level 2 provider's response, the Executive made a further request on 18 February 2021 for the following information:

- detailed explanation as to how the Microsoft data handling/retention policy prevented the Level 2 provider from recovering archived data
- details of the type of data that has been lost and confirm the date/s the data was lost
- details of the internal/external system(s) the Level 2 provider used to capture and store its data, including details of any software packages used, third parties involved in data storage
- all correspondence (internal and external) regarding the corruption of data and the attempts to recover the lost data
- details of the previous supplier that stored the archived data, including copies of contracts and contact information
- all correspondence instructing the previous supplier to obtain the information from the archive and any responses.

76. The Executive confirmed that none of this information was provided by the Level 2 provider. The Executive noted that the Level 2 provider simply re-iterated that the Microsoft data retention policy of 180 days meant that the date was no longer recoverable. The Executive also observed that the Level 2 provider did not however offer any explanation as to why this was relevant when the Executive's initial request for the data was made within the 180-day time limit.

77. The Executive further relied on paragraph 10 of the PSA's guidance on the retention of data which stated that providers should retain data for a minimum period of two years from the point at which it is collected to say that a breach had occurred.

78. The Executive also asserted that a breach of this paragraph had occurred as a result of the failure of the Level 2 provider to supply any evidence of the invoices and payments made to any third parties used for the direct marketing of the Service and copies of all versions of the Service website promotions for the last two years.

79. The Executive explained that it had requested this information as a result of the Level 2 provider's explanation that the Service had been marketed previously only through "word of mouth" but that in the pandemic it had used "print promotions" which had been inserted into deliveries of online orders.

80. In response to this request on 7 January 2021, the Level 2 provider supplied an older version of the website and stated the following:

    "We have tried to recover the previous web site files from our web developer; they have confirmed that they do not hold a back up of the previous site. As we amended the live site back in September 2020 to show the current information page, we have been informed that this has now over written any historic files."

    "However, we have kept the site relatively static since 2014 when we took guidance from PPP, the records should show PPP sign off, this was agreed and checked with….
    …... Please see the attached screen shots."

81. In relation to the invoices requested, the Level 2 provided stated it had requested copy invoices however given the Christmas break, Covid-19 and furlough it was *"taking time"*.

82. On 9 February 2021, the Executive further requested evidence of correspondence instructing its web developer to recover the website files and again requested evidence of the invoices and payments made to third parties in relation to direct marketing. The Executive stated that the Level 2 provider failed to respond to this request.

83. The Executive submitted that all of the information which was requested was capable of having a regulatory benefit within the meaning of the Code. The Executive explained that it wanted this information to ascertain how the Level 2 provider had come to hold the MSISDNs that were affected by the incident of 25 September 2020 so that it could understand whether there was any consent to charge issue. In relation to the information requested regarding the marketing of the Service, the Executive explained that this information was required to understand the way in which the Service was promoted and the likely volume of consumers that would have engaged with the Service through those promotions.

84. The Executive asserted that for all of the reasons above a breach of paragraph 4.2.3 had occurred.

Level 2 provider's response

85. The Level 2 provider denied the breach. The Level 2 provider stated that the Level 2 provider had attempted to co—operate fully with the Executive's investigation and provided all the information that it could.

86. The Level 2 provider stated that the no data was recoverable as a result of Microsoft's 180-day policy and that the Whistleblower had been responsible for deleting all of the data for the Service on 15 December 2019. The Level 2 provider stated that the time period from December 2019 to September 2020 was 280 days and therefore caught by Microsoft's retention policy which only kept data for 180 days before it was deleted. The Level 2 provider stated that the deletion by the Whistleblower had involved deletion of all of the data on the servers including any backed up data. The Level 2 provider indicated that as result of this the Level 2 provider did not hold any data.

Tribunal's decision

87. The Tribunal carefully considered all of the evidence before it, including the explanation provided by the Level 2 provider.

88. The Tribunal noted that there was no dispute between the parties that the information requested by the Executive had not been supplied.

89. The Tribunal noted that there had been a clear failure on the part of the Level 2 provider to supply the data requested regarding the MSISDNs and also the information in respect of the marketing of the Service. The Tribunal was also of the view that all of the information requested was likely to have had a regulatory benefit as the data requested by the Executive regarding the MSISDNs was clearly relevant to the issue of consent to charge as was the information regarding how the Service was marketed (particularly the direct marketing aspect).

90. The Tribunal considered the explanation put forward by the Level 2 provider as to why the information could not be provided.

91. In relation to the requests for the MSISDN data, the Tribunal noted that when the information was originally requested by the Executive on 6 October 2020, the Level 2 provider indicated that the information might be recoverable and that it was liaising with a previous supplier to try to obtain archived information. The Tribunal noted that it was only later in December, after the Executive requested an update, that the Level 2 provider referred to the 180-day time limit.

92. The Tribunal was of the view that the Level 2 provider had not been forthcoming in respect of the information requested by the Executive. In particular, the Tribunal noted that the Level 2 provider had failed to provide any correspondence with the previous supplier demonstrating that it was attempting to recover the data. The Tribunal noted that the Level 2 provider had indicated that some communications were only verbal, but the Tribunal was of the view that it was unlikely that none of these requests were sent in writing at any stage. The Tribunal noted that the Level 2 provider had also failed to provide an explanation as to how the 180-time limit operated in practice. The Tribunal was of the view, that even if it was the case that the data could not be recovered, the Level 2 provider had failed to provide other information that it should have had available.

93. The Tribunal went on to consider the Executive's request for information regarding the direct marketing of the Service. The Tribunal noted that while the Level 2 provider gave an explanation as to why previous versions of the website may not be available, the only explanation provided regarding why the correspondence or invoices were not available was that the both the companies the Level 2 provider had used for the website and the company that it had used for advertising were in administration and that communication was therefore verbal only.

94. The Tribunal was of the view that the Level 2 provider had not provided any cogent evidence to support these assertions. For example, the Tribunal was of the view that if it was the case that both companies had gone into administration, the Level 2 provider could have provided details to the Executive of the companies involved. The Tribunal was also of the view that if the companies were in administration, it was more likely that there would be correspondence between the Level 2 provider and the administrators.

95. The Tribunal concluded that I it was unable to accept the explanations out forward by the Level 2 provider in circumstances where the Level 2 provider had provided no supporting evidence. The Tribunal was of the view that even if some of the evidence that had been requested by the Executive was no longer available, the Level 2 provider should have been able to provide some of the other evidence such as correspondence, invoices and more details but that it had failed to do so. The Tribunal was therefore satisfied on the balance of probabilities that a breach of paragraph 4.2.3 of the Code had occurred as the Level 2 provider had failed to disclose information requested by the Executive that was likely to have had a benefit to the investigation.

Decision: UPHELD

Alleged breach 4

Paragraph 4.2.2

A party must not knowingly or recklessly conceal or falsify information, or provide false information to the PSA (either by inclusion or omission)

Message logs

96. The Executive submitted that the Level 2 provider had breached paragraph 4.2.2 of the Code as result of the message logs which it had provided which were false.

97. The Executive stated that the Service used the MO (Mobile-Originated) keyword opt-in method. Consumers who wished to sign up to the Service would therefore need to send the MO keyword 'Freeb' to the shortcode 84222. The Executive noted that the message logs supplied by the Level 2 provider in response to requests for information from the Executive displayed the message 'Freeb' being sent by consumers subsequently to their initial sign up to the Service.

98. As part of its investigation, the Executive also asked the Level 1 provider for the message logs in order to analyse all of the interaction between the consumers of the Service. The Executive notes that when it compared the logs supplied by the Level 2 provider with those supplied by the Level 1 provider, there were significant discrepancies. In particular, the Executive observed that the Level 1 provider's logs did not indicate that MO messages had been sent by consumers to opt into the Service initially or that consumers had sent subsequent MO messages whereas the logs from the Level 2 provider indicated that the MO messages were sent.

99. In addition to this, the Executive noted that the message logs from the Level 1 provider indicated that consumers had been overcharged for the Service in greater amounts than indicated by the Level 2 provider. The Executive provided examples of this issue using the logs for MSISDNs 07xxxxxxxx2 and 07xxxxxxxx5, both of which showed that there were more instances of overcharging on the Level 1 provider's logs when compared with the Level 2 provider's message logs.

Whistleblower's evidence

100. The Executive further submitted that the Whistleblower had provided evidence which suggested that the Level 2 provider had obtained MSISDNs through sources which did not relate to the Service. The Whistleblower supplied a list of 12,564 unique MSISDNs which the Whistleblower stated had been imported to the Level 2 provider's system. The Executive noted that out of the 91 complaints received prior to the technical incident, 20 MSISDNs appeared on the list provided by the Whistleblower. The Executive submitted that this evidence supported the assertion that the MO messages were not sent in by consumers to opt into the Service.

Level 2 provider's response

101. The Level 2 provider denied the breach. The Director of the Level 2 provider stated that the responses which were provided to the Executive had been provided by another individual within the Level 2 provider, and that this individual had been working in collaboration with the Whistleblower.

102. The Level 2 provider also stated that due to the deletion of data by the Whistleblower, it had been unable to review the message logs and any accompanying email correspondence.

103. During oral representations to the Tribunal, the Level 2 provider also added that the MO messages were missing from Level 1 provider's logs as a third aggregator had been used. The Level 2 provider explained that it was for this reason that the message logs appeared to be different. The Level 2 provider concluded by submitting that it had done its best to provide full and accurate information to the Executive and that any issues were as a result of the actions of the Whistleblower as opposed to any deliberate attempt on the Level 2 provider's part to mislead the Executive.

Tribunal's decision

104. The Tribunal gave careful thought to all of the evidence before it. The Tribunal was of the view that there were clearly discrepancies between the message logs that were supplied by the Level 1 and the Level 2 provider. The Tribunal, having analysed the logs, was of the view that the Executive's assertions that there were no MO messages on the Level 1 provider's message logs and that consumers appeared to be overcharged by more in the Level 1 provider's message logs than in the Level 2 logs was clearly correct.

105. The Tribunal considered the explanation put forward by the Level 2 provider. The Tribunal was of the view that even if the responses had been provided by another individual within the Level 2 provider who may have been working in collaboration with the Whistleblower, the responsibility still lay with the Level 2 provider to ensure that the Executive was provided with accurate information. The Tribunal noted that the Level 2 provider had not informed the Executive at any stage that the information provided may not be accurate.

106. In addition to this the Tribunal noted that in oral representations, the Level 2 provider had in fact indicated that the message logs were accurate given the use of the third-party aggregator. The Tribunal considered this to be at odds with the written response provided by the Level 2 provider which had indicated that the message logs could not be checked or verified due to the actions of a former employee and the Whistleblower.

107. The Tribunal observed that the Level 2 provider had failed to inform the Executive of the use of any third-party aggregator for the Service at any stage of the investigation. In addition to this, the Tribunal noted that the Level 2 provider had failed to provide any evidence which supported the assertions that there was a third-party aggregator involved in the provision of the Service. The Tribunal also gave consideration to the responses from the Level 1 provider which clearly stated that a third-party aggregator could not have used the same shortcode. For all of these reasons, the Tribunal was of the view that it could not accept the assertion by the Level 2 provider that a third-party aggregator had been used.

108. The Tribunal was also of the view that possible use of a third-party aggregator did not explain why there were discrepancies in the amount that consumers were being overcharged between the Level 1 and Level 2 providers' messages logs. The Tribunal considered whether there were any alternative explanations that could be put forward as to why there was a discrepancy in the message logs regarding the overcharging but was of the view that there was no alternative other than to conclude the message logs provided by the Level 2 provider were false.

109. The Tribunal was of the view that the evidence put forward by the Executive consisting of the message logs supplied by the Level 1 and Level 2 providers and the correspondence between the Executive and those two parties proved to be both cogent and compelling. The Tribunal was of the view that it had not received any evidence that was capable of undermining the Executive's case in respect of this breach, and therefore it was satisfied on the balance of probabilities that a breach had occurred.

110. In reaching its decision, the Tribunal did not consider it necessary to consider the evidence from the Whistleblower and reached its decision solely on the other evidence that was placed before it.

Decision: UPHELD

Sanctions

Assessment of breach severity

111. The Tribunal went on to assess the severity of the breaches of the Code that it had found proved. The Tribunal considered that overall, the breaches were very serious for the reasons set out below:

Rule 2.3.3 Consent to Charge

112. The Tribunal considered this breach to be **very serious.**

113. The Tribunal was of the view that the breach had a clear and highly detrimental impact or potential impact directly on consumers who may have unknowingly been signed up to and charged for the Service without their consent.

114. The Tribunal also agreed that the breach had resulted in consumers incurring a wholly unnecessary cost as they had not signed up to the Service. The Tribunal was also of the view that the breach had occurred of a significant or lengthy duration as the Executive had received complaints over a prolonged period regarding the Service.

Rule 2.3.3 Consent to Charge

115. The Tribunal considered this breach to be **very serious.**

116. As a preliminary matter, the Tribunal considered whether there was any overlap between this breach and the last consent to charge breach which should be taken into account in assessing the breach severity.

117. The Tribunal considered that the Executive had put this breach in a different basis as it related solely to the technical error which had occurred on 25 September 2021 and not the complaints that were received prior to this time. The Tribunal was of the view that the overcharging issue was different in this case as it occurred after the Level 2 provider rebuilt the Service following the dispute with the Whistleblower.

118. In addition to this, the Tribunal also considered that the nature of the overcharging was different to that outlined in the first breach. The Tribunal reasoned that in relation to this breach, the consent to charge issue had primarily arisen as a result of a technical issue which resulted in an exponential increase in the numbers of consumers that were charged accidentally.

119. The Tribunal were of the view that there was some overlap with the first breach in relation to the issue of how the complainants affected by the error came to sign up to the Service. The Tribunal was of the view that as with the first breach it was unclear how any affected complainants had signed up to begin with. However, the Tribunal was

of the view that there was a clear demarcation between the consumers that were affected by the technical incident and those that were affected in relation to breach 1 and on that basis the Tribunal was satisfied that it did not need to account for any overlap between breaches 1 and 2 in assessing the breach severity.

120. In considering the breach severity, the Tribunal considered that the breach had the potential to have a highly detrimental impact on consumers who were accidentally charged. The Tribunal accepted the evidence from the Level 2 provider that consumers had been refunded, but nonetheless the Tribunal was of the view that the initial charge by the Service had the potential to cause alarm and distress to the consumers that were affected.

121. The Tribunal was also of the view that the consumers affected had incurred a wholly unnecessary cost in the circumstances. While the Tribunal accepted that the issue was accidental, the Tribunal considered that the Level 2 provider should have taken more steps to ensure that its new system would not result in consumers being charged unnecessarily.

122. The Tribunal also considered that while the technical incident was likely to have been accidental, the lack of any evidence that complainants had consented to be charged by the Service at all was not merely accidental. The Tribunal considered that this element of the breach was likely to have been intentional. In light of this and for all of the reasons set out above, the Tribunal was of the view that the breach was very serious.

Paragraph 4.2.3 Failure to disclose

123. The Tribunal considered this breach to be **very serious**.

124. The Tribunal accepted the Executive's submission that the Level 2 provider had failed on multiple occasions to disclose information that had a regulatory benefit in response to the Executive's directions for information.

125. The Tribunal was of the view that the breach was not isolated as the Level 2 provider had failed to disclose information to varying kinds which ranged from evidence of consent to charge, information regarding marketing and advertising including invoices and correspondence. The Tribunal was of the view that the Level 2 provider was given ample opportunity to provide evidence to corroborate some of the assertions it had made about why it could not provide the requested information but also failed to provide this information.

126. The Tribunal agreed with the Executive that this breach was therefore committed intentionally and that it displayed a fundamental disregard for the requirements of the Code.

Paragraph 4.2.2 – False and misleading

127. The Tribunal was of the view that this breach was **very serious**.

128. The Tribunal agreed with the Executive that the nature of the breach meant that it had the potential to severely undermine the regulation of phone-paid services.

129. The Tribunal was of the view that the breach had been committed intentionally as the Tribunal was of the view that none of the explanations put forward by the Level 2 provider was capable of explaining the discrepancies within the message logs. The Tribunal was of the view that the breach therefore demonstrated a fundamental disregard for the provisions of the Code.

130. In making its assessment in respect of the severity of the breach, the Tribunal did not consider any of the evidence from the Whistleblower and based its conclusions solely on the evidence put forward by the Executive from complainants and from the Level 1 and Level 2 providers.

Representations on sanctions made by the Executive

Initial overall assessment

131. The Executive's initial assessment of the sanctions that should be imposed before any potential uplift or downgrade in light of aggravating or mitigating factors on the basis that the case was very serious overall was as follows:

- formal reprimand
- a prohibition on the Level 2 provider, from providing or having any involvement in any premium rate service for a period of eight years, starting from the date of publication of the Tribunal decision, or until payment of the fine and the administrative charges, whichever is the later
- a requirement that the Level 2 provider refunds all consumers who claim a refund, for the full amount spent by them for the Service, save where there is good cause to believe that such claims are not valid, and provide evidence to the PSA that such refunds have been made
- a total fine of £1,000,000 consisting of:
  Rule 2.3.3 - £250,000
  Rule 2.3.3 - £250,000
  Paragraph 4.2.3 - £250,000
  Paragraph 4.2.2 - £250,000
- 100% of the administrative charge.

132. The Tribunal agreed that the overall severity rating for the case was **very serious**.

133. The Tribunal noted that the Level 2 provider did not agree with the initial assessment of sanctions. In particular the Level 2 provider indicated that the fine was excessive and that a prohibition was not merited as there had been no concerns regarding the Service since 2014 and that the case was driven by the actions of the Whistleblower. The Level 2 provider also stated that refunds had already been provided.

134. The Tribunal did not accept that there were no issues with the Service since 2014 as it was clear from the Executive's evidence in relation to breach 1 that there were complaints from May 2018. The Tribunal did accept the assertion by the Level 2 provider that refunds were made to consumers affected by the technical incident but was of the view that a general refunds sanction was still appropriate as breach 1 had involved consent to charge issues that were unrelated to the technical incident.

135. The Tribunal did not consider it necessary at this stage to consider the proportionality of the fine as this assessment would be made later in the process.

136. The Tribunal was of the view that the suggested prohibition for eight years was however excessive. The Tribunal decided that a prohibition for a period of five years was more proportionate to the nature of the breaches overall. The Tribunal's initial assessment of sanctions was therefore as follows:

- formal reprimand
- a prohibition on the Level 2 provider, from providing or having any involvement in any premium rate service for a period of 5 years, starting from the date of publication of the Tribunal decision, or until payment of the fine and the administrative charges, whichever is the later
- a requirement that the Level 2 provider refunds all consumers who claim a refund, for the full amount spent by them for the Service, save where there is good cause to believe that such claims are not valid, and provide evidence to the PSA that such refunds have been made
- a total fine of £1,000,000 consisting of:
  Rule 2.3.3 - £250,000
  Rule 2.3.3 - £250,000
  Paragraph 4.2.3 - £250,000
  Paragraph 4.2.2 - £250,000
- 100% of the administrative charge.

Proportionality Assessment

137. The Tribunal's assessment of the aggravating and mitigating factors in relation to the case was as follows:

Aggravation

138. The Executive submitted that there were a number of aggravating factors which went to the investigation as a whole. The Executive asserted that the Level 2 provider had

failed to follow guidance on consent to charge, which had it been followed it could have prevented the breaches from occurring.

139. The Executive submitted that it was an aggravating factor to the case that the breaches had occurred following a previous adjudication against the Level 2 provider which related to issues of consent to charge in 2014. In addition to this the Executive also stated that the Level 2 provider had failed to co-operate fully with the investigation overall and that this failure to co-operate went beyond the facts of breach 1.

140. The Level 2 provider did not accept that these factors were aggravating and stated that it had not been made aware of the investigation until after the technical incident of 25 September 2020. The Level 2 provider also re-iterated that it had done its best to co-operate with the investigation throughout.

141. The Tribunal did not accept that the failure to follow guidance was an additional aggravating factor of the case. However, the Tribunal agreed that it was an aggravating factor to the case that there had been a previous adjudication which had considered consent to charge issues against the Level 2 provider. The Tribunal considered that while much of the failure of the Level 2 provider to co-operate with the Executive was already captured by breaches 3 and 4, the Level 2 provider had failed to be open and transparent with the Executive throughout. The Tribunal considered that this failure went beyond the breaches raised and was therefore additionally aggravating.

Mitigation

142. The Executive submitted that there were no mitigating factors to the case.

143. The Level 2 provider submitted that it was a mitigating factor to the case that it had collaborated with the Level 1 provider to ensure that consumers were fully refunded following the technical incident and that no harm occurred.

144. The Tribunal agreed that it was factually correct that the Level 2 provider had co-operated with the Level 1 provider to ensure that consumers were refunded after the technical incident had occurred. However, the Tribunal was of the view that this was not a mitigating factor and was merely what it would have expected the Level 2 provider to have done in the circumstances. The Tribunal was therefore of the view that there were no mitigating factors to the case.

Financial benefit/need for deterrence

145. The Executive stated that the Level 2 provider had generated £995,617.02 from 2018 until the Service was terminated. The Executive submitted that this was the relevant figure given the nature of the breaches raised as breach 1 started from May 2018.

146. The Executive submitted that the revenue flowed directly from the first consent to charge breach as while there was some evidence that some consumers had opted into the Service, the evidence which the Executive relied in relation to breach 1 demonstrated that consumers had not all consented to be charged.

147. The Executive argued that, in light of the seriousness of the breaches, the consumer harm and the need to deter conduct of this nature, there was a need to remove as much of the financial benefit accrued from the breaches through the imposition of a substantial fine.

148. The Level 2 provider stated that no concerns had been raised since 2014 until the technical incident in September 2020. The Level 2 provider also submitted that all consumers affected by the technical incident were refunded. The Level 2 provider stated that a fine of a substantial level would impact on the viability of the Level 2 provider going forward which in turn would impact on staff.

149. The Tribunal was satisfied that the revenue flowed from the first consent to charge breaches for the reasons advanced by the Executive and as there was clear evidence that consumers had not sent the MO messages to opt into the Service.

150. The Tribunal agreed that in light of this, there was a need to remove the financial benefit accrued from the service given the nature of the breaches. The Tribunal also considered this necessary to send out a clear message to the wider industry that services which charged consumers without their consent were not acceptable and that it was unacceptable to fail to co-operate with the regulator's investigation fully and transparently.

Sanctions adjustment

151. The Executive submitted that the prohibition and refunds sanctions were proportionate as while they were likely to have a detrimental impact on the Level 2 provider, they were the minimum measures that were necessary to ensure that the sanctioning objective of credible deterrence was met.

152. The Executive however stated that the initial fine recommendation of £1,000,000 exceeded the revenue that the Level 2 provider derived from the breaches, and that the recommended fine, in combination with the recommended non-financial sanctions, was likely to have a significant impact upon the Level 2 provider. In light of this, the Executive submitted that the recommended fine amount should be adjusted downwards in the interests of proportionality, to a total fine of £850,000.

153. The Tribunal was of the view that despite the impact on the Level 2 provider's viability and its staff, it was necessary to impose a high financial penalty on the Level 2 provider in order to ensure that the sanction imposed had a deterrent effect given the severity of the breaches.

154. The Tribunal agreed that it was appropriate to adjust the initial recommended fine downwards, for the reasons advanced by the Executive. The Tribunal was of the view that the figure of £900,000 was appropriate and proportionate, as it removed the revenue which had been generated by the service and was also sufficiently high to achieve the sanctioning objective of credible deterrence in combination with the other recommended sanctions.

Sanctions imposed

155. Taking into account all of the above the Tribunal considered the following sanctions to be appropriate and proportionate:

- formal reprimand
- a prohibition on the Level 2 provider, from providing or having any involvement in any premium rate service for a period of 5 years, starting from the date of publication of the Tribunal decision, or until payment of the fine and the administrative charges, whichever is the later
- a requirement that the Level 2 provider refunds all consumers who claim a refund, for the full amount spent by them for the Service, within 28 days of their claim, save where there is good cause to believe that such claims are not valid, and provide evidence to the PSA that such refunds have been made
- a total fine of £900,000 consisting of:
  Rule 2.3.3 - £250,000
  Rule 2.3.3 - £250,000
  Paragraph 4.2.3 - £150,000
  Paragraph 4.2.2 - £250,000.

Administrative charge recommendation: 100%