

## **Tribunal meeting number 283**

Case reference: 152741  
Level 2 provider: Taptronic FZC  
Type of service: Subscription alert service  
Level 1 providers: mGage Europe Limited  
Infomedia Limited  
Trendtech Ltd (Payguru)  
Network operator: Vodafone, O2, Three and EE

This case was brought against Taptronic FZC, 'the Level 2 provider' under Paragraph 4.5 of the 14<sup>th</sup> Edition of the Code of Practice.

### **Background and investigation**

1. This case concerned a subscription alerts service called Fitguru ('the Service'), which provided consumers with fitness training and nutritional videos, which included exercise plans, training videos and video recipes for healthy eating.
2. The Service operated via directed carrier billing (DCB) using two shortcodes: 64055 and 80206 with two value chains.
3. Shortcode 64055 operated by the Level 1 provider mGage Europe Limited, was available on the Vodafone, O2 and Three networks and shortcode 80206 operated by the top Level 1 provider Infomedia Limited, was available on EE. Each shortcode operated between various dates, with different value chains, and a different price point.

### **Service operation and value chains**

#### **Value chain 1**

4. A different Level 2 provider (Itech Logic Ltd) initially operated the Service on the 80206 shortcode. There was some dispute between the Executive and the Level 2 provider as to when the Service was novated from Itech Logic Ltd to the Level 2 provider. The Level 2 provider maintained that the Service was novated in April 2018, however the Executive maintained that the Level 2 provider had been involved in the provision of the Service on the 80206 shortcode from the outset in 2017.
5. Neither Itech Logic Ltd nor the Level 2 provider registered the Fitguru Service which operated on value chain 1 with the Executive.
6. The Level 1 provider Infomedia Limited stated that the Service commenced operation in July 2017.

The Level 2 provider confirmed that the marketing campaign started with Itech Logic Ltd in August 2017 until December 2017, at which point they stopped the campaign. The promotion resumed on 12 January 2018 and was paused again on 26 January 2018.

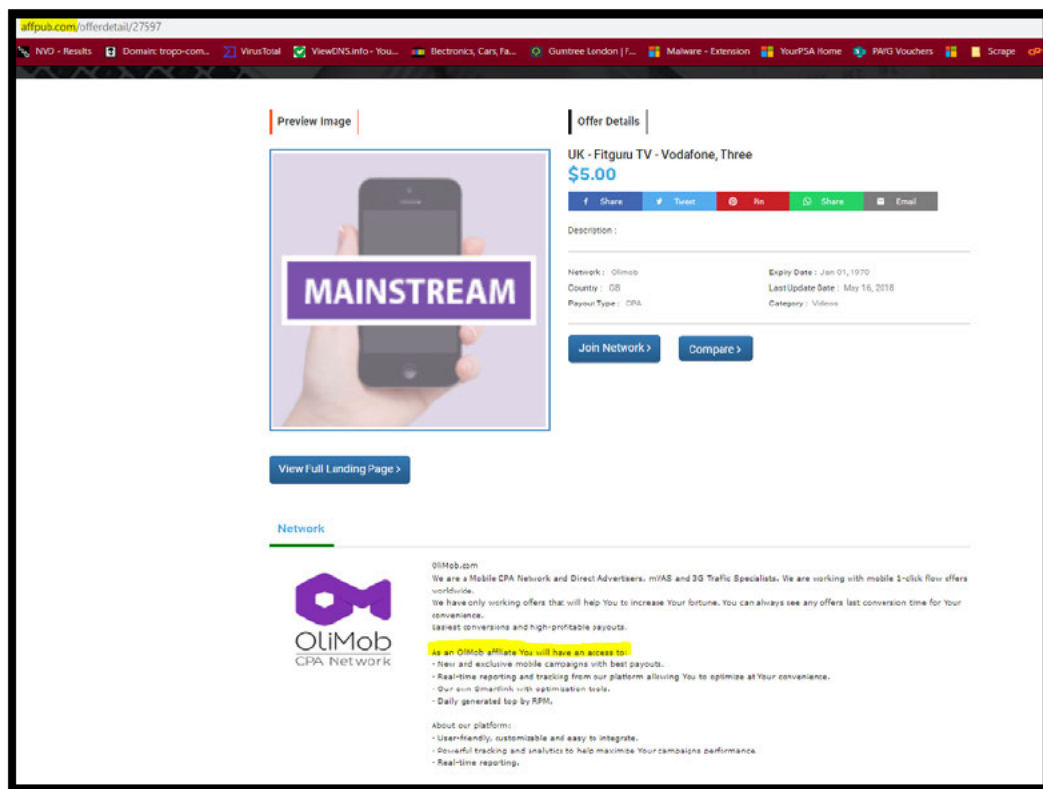
7. Infomedia Limited confirmed that 19,653 consumers were subscribed to the value chain 1 between July 2017 and January 2018. The Level 2 provider continued to bill consumers, and on 17 April 2020, the Level 2 provider confirmed that 311 consumers were still being billed for the Service. These consumers were billed for the service until it was terminated by another Level 1 provider within the same value chain, (Payguru/Trendtech) on 30 April 2020.

#### **Value chain 2**

8. The Level 2 provider also operated the Service on the 64055 shortcode. The Level 1 provider for the Service that operated on Value Chain 2 was mGage. The Level 2 provider registered the service on the value chain 2 after receiving registration notification from the Executive.
9. The promotional campaign for shortcode 64055 commenced in May 2018 and the Level 1 provider, mGage, terminated the Service on value chain 2 on 17 July 2020.

#### **Service promotion**

10. The Level 2 provider stated that the Service was promoted online through banner ads, which drove users to a landing page which in turn gave full details of the Service and the charges. Users then had to confirm their subscription.
11. The Level 2 provider stated that the Service was not promoted via affiliate marketing and all marketing was done by Google Display ads and DSP platforms Smadex and startAPP. All ads were displayed on apps and mobile websites. However, the evidence gathered by the Executive indicated that the Service was promoted using affiliate marketing. For example, an advertisement for the Service was found on [www.affpub.com](http://www.affpub.com) which marketed itself as an “Exclusive Affiliate Marketing Hub” as displayed below:



## Previous relevant cases

12. The Level 2 provider has not previously been the subject of a Track 1 or Track 2 investigation by the Executive. However, on 8 December 2020 a Tribunal prohibited Mr Ravi Kumar Metta (the director of the Level 2 provider) for a period of five years from providing, or having any involvement in, any premium rate services in the UK. The prohibition followed a previous adjudication which had taken place in respect of Itch Logic Ltd in relation to a different premium rate service in April 2020.

## The investigation

13. The Executive received 410 complaints from members of the public between May 2018 and February 2020. The first complaint about the Service was received on 2 May 2018.
14. Complainants variously alleged that they had not signed up to nor agreed to be charged by the Level 2 provider and that they were unable to successfully complain to the Level 2 provider.
15. A sample of complainant accounts have been provided below:

*"I have received the text message on 11 June 2018, stating that I had subscribed to "fitguru" by Taptronic, which would charge me £3 per week. I have been charged once so far. I never subscribed to such service. I was unable to speak with anyone from that company. My phone operator (GiffGaff) asked me to raise an inquiry with the Phone-Paid Services Authority."*

*"Received this unsolicited message for a service I did not subscribe to. Have unsubscribed but have also been billed for £3. Tried calling them on 03302231099 but it only gives an option to leave a VM which of course they never respond to."*

*"I received this text message on 12/6/18 and was charged £3 for a service I have never subscribed to. . I have no idea who or what Fitguru is and have no interest in it. Called O2 and they said they could not help. Left a message on the phone number provided - 03302231099 - but have had no response. This is a total scam and illegal. Searching online shows I'm not the only person this has happened to."*

*"I did not subscribe to this account. I have contacted my service provider who will not refund my money although they have put a stop on any premium rate services and told me to contact yourselves. . I have not received or responded to any unknown emails and yet have been charged £12 for a fitness subscription. . I am receiving no subscription information or benefits. I have emailed twice the Taptronic group and received no reply."*

16. On 12 November 2019, the Executive sent a consumer survey to all its complainants. The Executive received 93 detailed responses to its survey.
17. During the investigation, the Executive's monitoring mobile phone number ('MSISDN'). was signed up to the Service without consent on value chain 2. The monitoring demonstrated the extent to which Direct Carrier Billing Malware (DCBM) was used to covertly sign up consumers to the service without their knowledge or consent. The Executive found that DCBM was widespread and affected the Service as a result of DCBM being pre-installed on mobile handsets prior to shipping and apps being available to download and install by Android device users.
18. The Executive asserted that the Level 2 provider did not pick up on the DCBM issues and did not ensure that its subscribers had consented to the charges.
19. Based on analysis of the Request for Information MSISDN activity logs, the Executive suspected that the provider had also intentionally falsified evidence.

### **Apparent breaches of the Code**

20. The Executive sent a Warning Notice to the Level 2 provider on 8 June 2021 and 14 June 2021 in which the following breaches of the PSA's Code were raised:

- Rule 2.3.1 – Fairness
- Rule 2.3.3 – Consent to charge
- Rule 2.6.1 – Complaint handling
- Paragraph 3.4.14 Registration
- Paragraph 4.2.2 Concealing or falsifying information
- Paragraph 4.2.2 Concealing or falsifying information
- Paragraph 4.2.2 Concealing or falsifying information

21. Responses to the Warning Notice were received from solicitors acting for one of the directors of the Level 2 provider and from Mr Ravi Kumar Metta on behalf of the Level 2 provider.

22. On 17 August 2021 the Tribunal reached a decision in respect of the breaches.

### **Preliminary issue – Service and proceeding in absence**

23. As the Level 2 provider did not attend the Tribunal, the Tribunal considered as a preliminary issue the issues of the Service and proceeded in his absence.

24. Regarding the issue of service, the Tribunal noted that the Executive had attempted to serve the Warning Notice via email and post on 8 June 2021. The Tribunal further noted that the Executive also called the Level 2 provider on 10 June 2021, and that as a result of this call it served a further copy of the Warning Notice on the Level 2 provider using a different email address that it had obtained on 14 June 2021.

25. The Tribunal observed that on 23 June 2021, a response to the Warning Notice had been received from solicitors acting for a director for the Level 2 provider. In addition to this, a further response to the Warning Notice was received on 25 June 2021 from Mr Metta on behalf of the Level 2 provider which addressed the breaches.

26. The Tribunal also observed that the Executive had notified the Level 2 provider of the Tribunal date and time by email on 5 August 2021. The email explained that the Tribunal would be held remotely via Microsoft Teams and enclosed instructions on how to join the paper-based hearing via Microsoft Teams. The Tribunal further observed that the Level 2 provider downloaded the email of 5 August 2021 which indicated that it was aware of the Tribunal date and time.

27. As a result of all of the above, the Tribunal was satisfied that that the Executive had made all reasonable efforts to ensure that the necessary documents had been properly served by post and by email on the Level 2 provider and that it had been made aware of the date of the Tribunal hearing.

28. The Tribunal also noted that various responses had been received from solicitors acting for one of the directors of the Level 2 provider and Mr Metta on behalf of the Level 2 provider.

29. The Tribunal then went on to consider whether it was fair to proceed in the absence of the Level 2 provider. The Tribunal noted that Mr Metta, in his response of 8 July 2021, had indicated that he did not wish to attend a Tribunal. The Tribunal further noted that the solicitors acting for the other director had not indicated that he wished to attend the Tribunal. When questioned, the Executive also confirmed that no further response had been received from the Level 2 provider.

30. Taking all of the circumstances into account, the Tribunal decided that it was fair to proceed in the absence of the Level 2 provider. The Tribunal was of the view that the Level 2 provider had been properly notified of the date and time of the Tribunal and that it had not given any indication that it wished to attend. Accordingly, the Tribunal was of the view that an adjournment was unlikely to secure the attendance of the Level 2 provider and that it was therefore fair and in the interests of justice to proceed.

## Submissions and conclusions

### 31. Alleged breach 1

#### Rule 2.3.1

*“Consumers of PRS must be treated fairly and equitably.”*

32. The Executive stated that the Level 2 provider had breached rule 2.3.1 of the Code as subscribers to the Service were charged but not provided with adequate access to the service.
33. In support of its argument, the Executive relied on the Service text message logs and the Level 2 provider’s response to the informal enquiry.
34. The Executive asked the Level 2 provider how consumers interacted with the Service:  
*“if the user accesses the site through mobile data and we recognise that he is a valid subscriber, he will be able to access the content straight away without any further verification required. If the user is accessing via wifi, he will have to enter his mobile number and we then recognize that he is a subscriber and let him have access to the content.”*
35. However, when the Executive obtained the Service text message logs (as set out below) it noted that none of the supplied message logs between the Level 2 provider and the mobile telephone numbers signed (‘MSISDNs’), displayed any messages containing a link to access the Service. Therefore, if the consumers did not save the landing page link at the point of subscription, they were charged £3.00 or £2.99 per week for a service which they had no means of accessing.

Logs for value chain 1



Filter by Sms Date

1 SEPTEMBER 2017 - 31 JULY 2018

OPERATOR

MERCHANTS

Content Type

Type

447895600401

SUBMIT

EXEC

Showing 1 to 15 of 15 entries

100
records

Search:

ID	Merchant	Product ID	Product	Operator	Msid	Content	Content Type	Type	Date
327314	ITECHLOGIC	1038	FiguruTV	EE		You have subscribed to FiguruTV for £2.99 p/w.Free first 24hrs.Send STOP RTGURU to 80206 to cancel.Help? 03332124631 T&Cs <a href="https://geo.gigamonadsfc(FreeMsg">https://geo.gigamonadsfc(FreeMsg</a>	welcome	mt	2017-09-30 17:33:31
345917	ITECHLOGIC	1038	FiguruTV	EE		You have subscribed to FiguruTV for £2.99 p/w.Free first 24hrs.Send STOP RTGURU to 80206 to cancel.Help? 03332124631 T&Cs <a href="https://geo.gigamonadsfc(FreeMsg">https://geo.gigamonadsfc(FreeMsg</a>	welcome	mt	2017-10-28 15:55:25
348337	ITECHLOGIC	1038	FiguruTV	EE		FreeMsg: Reminder - You are subscribed to FiguruTV for £2.99 per week. Un-subscribe? Text STOP FITGURU to 80206. Help? Call 03332124631	reminder	mt	2017-10-30 17:09:23
407924	ITECHLOGIC	1038	FiguruTV	EE		FreeMsg: Reminder - You are subscribed to FiguruTV for £2.99 per week. Un-subscribe? Text STOP FITGURU to 80206. Help? Call 03332124631	reminder	mt	2017-11-29 17:07:30
406562	ITECHLOGIC	1038	FiguruTV	EE		FreeMsg: Reminder - You are subscribed to FiguruTV for £2.99 per week. Un-subscribe? Text STOP FITGURU to 80206. Help? Call 03332124631	reminder	mt	2017-11-30 17:07:55
475604	ITECHLOGIC	1038	FiguruTV	EE		FreeMsg: Reminder - You are subscribed to FiguruTV for £2.99 per week. Un-subscribe? Text STOP FITGURU to 80206. Help? Call 03332124631	reminder	mt	2017-12-28 17:07:11
476655	ITECHLOGIC	1038	FiguruTV	EE		FreeMsg: Reminder - You are subscribed to FiguruTV for £2.99 per week. Un-subscribe? Text STOP FITGURU to 80206. Help? Call 03332124631	reminder	mt	2017-12-30 17:07:33
514323	ITECHLOGIC	1038	FiguruTV	EE		FreeMsg: Reminder - You are subscribed to FiguruTV for £2.99 per week. Un-subscribe? Text STOP FITGURU to 80206. Help? Call 03332124631	reminder	mt	2018-01-28 17:06:11
515742	ITECHLOGIC	1038	FiguruTV	EE		FreeMsg: Reminder - You are subscribed to FiguruTV for £2.99 per week. Un-subscribe? Text STOP FITGURU to 80206. Help? Call 03332124631	reminder	mt	2018-01-30 17:06:40
540990	ITECHLOGIC	1038	FiguruTV	EE		FreeMsg: Reminder - You are subscribed to FiguruTV for £2.99 per week. Un-subscribe? Text STOP FITGURU to 80206. Help? Call 03332124631	reminder	mt	2018-02-28 17:05:49
551039	ITECHLOGIC	1038	FiguruTV	EE		FreeMsg: The service FiguruTV has been suspended and no further charges will take place.	suspend	mt	2018-03-15 09:30:31
558722	ITECHLOGIC	1038	FiguruTV	EE		FreeMsg: Reminder - You are subscribed to FiguruTV for £2.99 per week. Un-subscribe? Text STOP FITGURU to 80206. Help? Call 03332124631	reminder	mt	2018-03-30 17:05:58
573043	ITECHLOGIC	1038	FiguruTV	EE		FreeMsg: Reminder - You are subscribed to FiguruTV for £2.99 per week. Un-subscribe? Text STOP FITGURU to 80206. Help? Call 03332124631	reminder	mt	2018-04-30 17:09:52
573285	ITECHLOGIC	1038	FiguruTV	Unknown		STOP DIRECTCALL		mo	2018-05-01 11:38:41
573296	ITECHLOGIC	1038	FiguruTV	EE		FreeMsg: You have successfully unsubscribed from FiguruTV and no longer will be charged for this service.Help? Call 03332124631	exit	mt	2018-05-01 11:58:41

A	B	C	D	E	F	G	H	I	J
Date & Time	Direction	Shortcode/Sender	Mobile Number	Keyword	Client	Message GUID	Gateway Status	Final Status	Message Body
11/05/2018 13:43	DR	64555	[REDACTED]	/A	MG431	71d34c16-2979-4c6e-816a-d04c83aa046d		Delivered	
11/05/2018 13:43	DR	64555	[REDACTED]	/A	MG431	71d34c16-2979-4c6e-816a-d04c83aa046d	sent	Delivered	FreeMsg: Thank You. You have been successfully unsubscribed from figuru, provided by Taptronic HELP? 6330221099.
11/05/2018 13:42	MO	64555	[REDACTED]	STOP	MG000	0c6ef616-1960-4d9e-8b46-5d8ce13453f1		Received	STOP
09/05/2018 11:19	DR	RECEIPT	[REDACTED]	/A	MG431	9821fb9-3819-44de-a537-e805a1ee30ab		Delivered	
09/05/2018 11:19	MT	RECEIPT	[REDACTED]	/A	MG431	9821fb9-3819-44de-a537-e805a1ee30ab	sent	Unknown	FreeMsg: Thank you for subscribing to figuru for £3.00 per week from Taptronic until you text STOP to 64055. HELP? 0330221099

	A	B	C	D	E	F	G	H
1	Number	Datetime	Unsubscribed	Accessed	Accessed 2	Accessed 3	Accessed	Accessed 4
2		2018-05-18 15:34:46	25/05/2018 16:34					
3		2018-05-25 13:42:54	01/06/2018 14:42					
4		2018-06-11 17:51:41	18/06/2018 18:51					
5		2018-06-11 16:12:44	18/06/2018 17:12					
6		2018-06-09 13:11:16	16/06/2018 14:11					
7		2018-06-08 12:52:25	15/06/2018 13:52					
8		2018-07-12 07:51	19/06/2018 07:51					
9		2018-05-25 14:28:2018-06-08 14:11	6/1/2018 2:28:00 PM, 15 Jun 18 14:11					
10		2018-05-15 04:02:18	26/06/2018 05:02					
11		2018-06-14 07:02:152018-07-10 16:57:32	21/06/2018 08:02					
12		2018-06-08 14:27:20	30/06/2018 15:37	10/06/2018 06:44	11/06/2018 18:19			
13		2018-06-08 12:39:252018-06-27 09:33:22	6/22/2018 1:39:00 PM, 04 Jul 18 10:33					
14		2018-06-08 12:17:43	06/07/2018 13:17	11/06/2018 07:20	14/06/2018 14:01	21/05/2018 10:00		
15		2018-06-21 20:21	05/07/2018 20:21					

38. The Level 2 provider denied the breach in a response to the Executive by way of a letter dated 8 July 2021.
39. In this response, the Level 2 provider stated that the subscribers of Fitguru service were given a widget which was installed on their phones and opened *"the specific member area of the site"*. The provider further stated that *"their service flow directed the user to the members area of the site up on a valid subscription"*
40. The Level 2 provider did not accept the breach of Rule 2.3.1 as in its view it wasn't necessary to send the link to subscribers while the widget to access the Service was provided. Additionally, the Level 2 provider claimed that the message format used was in keeping with the template approved and provided by the Level 1 providers and approved by the mobile networks.
41. The Tribunal carefully considered all of the evidence before it, including responses written by the Level 2 provider.
42. The Tribunal noted that the access logs clearly demonstrated that 85% complainants were unable to access the service, yet they had been charged weekly. Additionally, the Tribunal observed that there was no other evidence of consumers accessing the Service in any of the logs supplied by the Level 2 provider.
43. The Tribunal considered that it had not been provided with any evidence to suggest that consumers had accessed the Service, notwithstanding the explanation provided by the Level 2 provider. The Tribunal was of the view that on the evidence that it had before it, it was more likely than not that consumers had been unable to access the Service despite being charged. The Tribunal accordingly concluded that consumers had not been treated fairly.
44. In light of the above, the Tribunal was therefore satisfied on the balance of probabilities that a breach of rule 2.3.1 of the Code had occurred.

Decision: UPHELD

## **Alleged breach 2**

### **Rule 2.3.3**

*"Consumers must not be charged for PRS without their consent. Level 2 providers must be able to provide evidence which establishes that consent."*

45. The Executive asserted that the Level 2 provider had breached rule 2.3.3 of the Code because it had failed to provide robust evidence that established consent to charge had been obtained from the consumers. The Executive relied on the following evidence:

## **Complainant accounts**



46. The Executive relied on 410 complaints from members of the public in support of its case. The Executive noted for example, that complainants consistently asserted that they had not agreed to be charged by the Service and did not know how the Level 2 provider obtained their MSISDNs. In addition to this, four complainants stated that they had not been using their devices at the time that they had allegedly signed up to the Service.
47. The Executive noted from the Level 2 providers responses that to consent and sign-up to the Service consumers would have to do the following:
- **Consumers on a Wi-Fi connection** must be issued a PIN or code after entering their mobile telephone number onto the Service website and in turn enter the PIN onto the Service website when prompted.
  - **Consumers connected via 3G/4G** must confirm that they consent to charges via the double opt-in method.
47. The Executive noted from the above flow chart, that to opt into the Service, the consumer would have had to; input their MSISDN into the first page of the Service website, then they would have received a text message (SMS) which supplied a PIN/code that they would have had to input into the second page of the Service website to verify their opt-in and consent to be subscribed and charged by the Service.
48. On 12 November 2019, the Executive sent a consumer survey to the 405 complainants who had complained about the Service at that time. The survey contained screenshots of the promotional material and the flow that consumers would have seen when subscribing for both the EE and the Vodafone/3/O2 flows. 97 complainants responded to the survey, however only 93 contained a substantive response. In summary:
- 91 complainants confirmed that they had not seen any of the promotional material. One complainant could not remember, and one complainant did not answer the question.
  - none of the 93 complainants could recall entering their telephone number into an online promotion.
  - three complainants recalled receiving a PIN. One did not enter it and the other two could not recollect whether they entered it or not.

### Monitoring evidence

49. On 24 December 2018, the Executive captured a covert opt into the Service without consent. The opt into the Service occurred while the handset was locked and in an idle state.

50. The monitoring handset's mobile data network traffic activity was captured during the covert subscription initiation. This was done via a forensic tool on the handset which created a PCAP file that documented all the network traffic activity. The Executive's analysis of this file led it to conclude that the opt into the Service was as a result of DCBM which was capable of stimulating interactions with the Level 2 provider and the Level 1 provider's (in this case mGage) payment platform to create opt ins without any user interaction.
51. As part of its analysis into DCBM, the Executive noted that a particular operating system on mobile telephones was more susceptible to DCBM. The Executive further noted that 356 complainants out of 410 used mobile phones with the operating system that was more susceptible to malware despite the overall market share of this operating system being approximately 50%.

### **Multi subscriptions**

52. The Executive noted from both the complainant records and the bills that the complainants had sent in that at least 52 complainants had been subscribed to more than one premium rate service. The majority of these consumers were using shortcode 64055. One complainant for example had been subscribed to seven different services on the 64055 shortcode.
53. The Executive was of the view that complainants being signed up to multiple subscription services without their knowledge or consent was a strong indication of DCBM being present.

### **Re-subscriptions**

54. In addition to all of the above, the Executive noted that 24 complainants reported they had been re-subscribed into the Service after opting out. In addition to this, the Executive also noted that the message logs also indicated that consumers were being re-subscribed to the Service without their consent as set out below for example in relation to one MSISDN:

MIG431	Q2 UK	NotProvided	I thank you for subscribing to fitguru for £3.00 per week from Taptronic until you text STOP to 64055. HELP? 03302231099	Sent	Billed	0
MIG431	Q2 UK	NotProvided	Thank you for subscribing to fitguru for £3.00 per 1 week from Taptronic until you text STOP to 64055. HELP? 03302231099	Sent	Billed	0
MIG431	Q2 UK	NotProvided	Thank you for subscribing to fitguru for £3.00 per 1 week from Taptronic until you text STOP to 64055. HELP? 03302231099	Sent	Billed	0
MIG431	Q2 UK	NotProvided	Thank you for subscribing to fitguru for £3.00 per 1 week from Taptronic until you text STOP to 64055. HELP? 03302231099	Sent	Billed	0
MIG431	Q2 UK	NotProvided	Thank you for subscribing to fitguru for £3.00 per 1 week from Taptronic until you text STOP to 64055. HELP? 03302231099	Sent	Billed	0
MIG431	Q2 UK	NotProvided	FreeMsg: Reminder. You are subscribed to fitguru for £3.00 per 1 week from Taptronic until you text STOP to 64055. HELP? 03302231099	Sent	Free	0
MIG431	Q2 UK	NotProvided	Thank you for subscribing to fitguru for £3.00 per 1 week from Taptronic until you text STOP to 64055. HELP? 03302231099	Sent	Billed	0
MIG431	Q2 UK	NotProvided	Thank you for subscribing to fitguru for £3.00 per 1 week from Taptronic until you text STOP to 64055. HELP? 03302231099	Sent	Billed	0
MIG431	Q2 UK	NotProvided	Thank you for subscribing to fitguru for £3.00 per 1 week from Taptronic until you text STOP to 64055. HELP? 03302231099	Sent	Billed	0
MIG431	Q2 UK	NotProvided	Thank you for subscribing to fitguru for £3.00 per 1 week from Taptronic until you text STOP to 64055. HELP? 03302231099	Sent	Billed	0
MIG431	Q2 UK	NotProvided	FreeMsg: Reminder. You are subscribed to fitguru for £3.00 per 1 week from Taptronic until you text STOP to 64055. HELP? 03302231099	Sent	Free	0
MIG000	Q2 UK	STOP	STOP	(null)	Billed	(n
MIG431	Q2 UK	NotProvided	FreeMsg: Thank You. You have been successfully unsubscribed from fitguru, provided by Taptronic. HELP? 03302231099.	Sent	Free	0
MIG431	Q2 UK	NotProvided	Thank you for subscribing to fitguru for £3.00 per week from Taptronic until you text STOP to 64055. HELP? 03302231099	Sent	Billed	0
MIG431	Q2 UK	NotProvided	Thank you for subscribing to fitguru for £3.00 per 1 week from Taptronic until you text STOP to 64055. HELP? 03302231099	Sent	Billed	0
MIG431	Q2 UK	NotProvided	Thank you for subscribing to fitguru for £3.00 per 1 week from Taptronic until you text STOP to 64055. HELP? 03302231099	Sent	Billed	0
MIG431	Q2 UK	NotProvided	Thank you for subscribing to fitguru for £3.00 per 1 week from Taptronic until you text STOP to 64055. HELP? 03302231099	Sent	Billed	0
MIG431	Q2 UK	NotProvided	Thank you for subscribing to fitguru for £3.00 per 1 week from Taptronic until you text STOP to 64055. HELP? 03302231099	Sent	Billed	0
MIG431	Q2 UK	NotProvided	FreeMsg: Reminder. You are subscribed to fitguru for £3.00 per 1 week from Taptronic until you text STOP to 64055. HELP? 03302231099	Sent	Free	0
MIG000	Q2 UK	STOP	STOP	(null)	Billed	(n
MIG431	Q2 UK	NotProvided	FreeMsg: Thank You. You have been successfully unsubscribed from fitguru, provided by Taptronic. HELP? 03302231099.	Sent	Free	0
MIG000	Q2 UK	STOP	STOP	(null)	Billed	(n

## Service content access logs

55. As part of its investigation, the Executive analysed the access logs provided by the Level 2 provider in relation to the complainants that had been received. At the time there were 383 complainants and 325 of these access logs evidence that there was no date/timestamp in the "Accessed" column, which in turn indicates that around 85% the complainants MSISDNs never accessed the Service after the initial opt-in.
56. The Level 2 provider asserted that the absence of the time and date stamp was due to the subscribers to the Service choosing not to use it. However, the Executive noted that the user flow provided by the Level 2 provider indicated that any subscriber would be automatically re-directed to the Service on signing up. The Executive therefore asserted that this was further evidence of consumers not having signed up to the Service using the user flow.
57. The Executive further noted that on 29 January 2020, the Level 2 provider had been asked to provide details of its entire subscriber base. The Executive noted that there were 72,262 rows and the Level 2 provider confirmed that each row represented an individual opt-in. At the same time, the Level 1 provider mGage was asked to provide the same data, however its records indicated that there were 71,269 individual subscribers. No explanation was provided as to this discrepancy in relation to value chain 2.

## Responses from the Level 2 provider

58. In addition to the above, on 3 April 2020 the Executive asked the Level 2 provider to provide some additional columns of data in relation to the data that it had already provided regarding the subscriber database. The Level 2 provider submitted this data

however, the Executive noted that the subscriber database had decreased from 72,262 to 69,267 without any explanation.

59. On 6 July 2018, the Level 2 provider was asked to provide evidence of how it had robustly verified consent to charge in relation to ten MSISDNs. The Level 2 provider responded by providing information such as the date of the opt-in and the app that the promotional flows ran through.
60. The Level 2 provider also asserted in a response dated 6 September 2020 that it had engaged two independent third parties to monitor the Service and to provide compliance advice. The Level 2 provider also confirmed that it did not use any marketing partners or affiliates to promote the Service.
61. The Level 2 provider also provided evidence that it had identified a number of issues with the Service which it had addressed appropriately. For example, in September 2018 when it became aware that the Service was being advertised in apps that were aimed at children, it acted to stop these promotions and refunded any affected consumers. In December 2018, as a result of increased complaints, it had also temporarily suspended all marketing and had unsubscribed and refunded 42 consumers due to the unusual nature of their subscriptions. In addition to this, the Level 2 provider also stated that when it was sent a monitoring notification in March 2019 by the Executive regarding the handset that had been covertly signed up to the Service by an app called “com.nitroxenon.okplayer” it unsubscribed and refunded 52 users.
62. On 29 January 2020, the Executive asked the Level 2 provider to provide evidence of how the 410 complainants’ MSISDNs were opted into the Service. The Level 2 provider provided access logs and responded as follows:
- “In all cases the user has followed the double opt-in process and we couldn’t find anything untoward from the user agent information that we got. The pattern of the subscriptions was normal, the click to conversion ratio was normal and we couldn’t find any unusual behaviour regarding the times of the subscriptions. As a result we believe that the given consent was obtained in the correct manner. Also we would like to mention that [third party’s] blacklist of websites and DCBM apps is always carefully implemented across all our campaigns to ensure that we are not displaying our ads in any of the blacklisted websites or apps”*
63. The Executive submitted that the information provided by way of the message logs and the data regarding the time and date of the MSISDN opt-ins was not sufficient evidence of robust consent to charge. In addition to this, the Executive further asserted that the evidence from the complainants, coupled with its monitoring which demonstrated the presence of DCBM that had signed up consumers without their consent, meant that a breach of the Code had occurred.
64. The Level 2 provider denied the breach. In its response to the Warning Notice dated 8 July 2021 it made the following points:

- in relation to the monitoring evidence, the Level 2 provider asserted that it had used only well-established digital marketing channels and that its engagement of their parties that assisted with compliance and monitoring meant that it was not using any marketing that it was known to be non-compliant. The Level 2 provider asserted that when it had become aware of any issues as a result of the com.nitroxenon.okayplayer app, it had taken action to block the app and provided refunds.
- in relation to the over-representation of one type of operating system, the Level 2 provider stated that its marketing was aimed at users of this type of system
- regarding the re-subscriptions and multi subscriptions, the Level 2 provider asserted that they had no visibility of the MSISDNs subscribing and could not therefore be held responsible for this occurring
- the Level 2 provider submitted that in all cases it had provided the date of opt-in, the app that ran the promotions, the user agent data which included the users IP address, make of handset, location including latitude and longitude and city. The Level 2 provider reiterated that this was the only information that was available to it.

65. In questioning, the Executive clarified that it was of the view that despite the assertions of the Level 2 provider, it was likely that affiliate marketing had been used as this was normally the case where DCBM was present. The Executive also clarified that it considered that all providers of premium rate services had a responsibility to ensure that any consumers were not adversely affected by DCBM and that they should have had safeguards in place to ensure that consumers were not opted into the Service as a result of DCBM.

66. The Tribunal carefully considered all of the evidence before it, including the responses submitted by the Level 2 provider.

67. The Tribunal found the complainant evidence to be credible. The Tribunal noted that a high volume of consumers had all raised similar concerns around not having been signed up to the Service. The Tribunal also found the monitoring evidence submitted by the Executive to be compelling, particularly the evidence in relation to the covert sign up of the locked, idle handset to the Service. In addition to this, the Tribunal also noted the findings of the Executive's monitoring report into the presence of malware and was of the view that this issue was likely to have contributed to consumers being signed up to the Service without their knowledge or consent.

68. The Tribunal observed that in some cases, consumers appeared to have sent the STOP message but then became re-subscribed to the Service. The Tribunal was of the view that it was highly improbable that a consumer would try to exit the Service through sending the STOP message only to re-join the Service afterwards.

69. The Tribunal considered the response by the Level 2 provider. The Tribunal was of the view that the response submitted by the Level 2 provider failed to demonstrate that it

had any robust evidence of consent to charge. The Tribunal did not consider the use of any third parties for monitoring and compliance to be relevant as to the issue of consent to charge. The Tribunal further noted that while the Level 2 provider had provided message logs and information as to the time and date that a MSISDN had become subscribed to the Service, it had also stated that it had “no visibility of the subscribing MSISDN” and that there were a number of discrepancies within the logs as to the numbers of subscribers of the Service. Accordingly, the Tribunal was of the view that the Level 2 provider had failed to provide evidence of robust evidence of consent to charge.

70. In light of all of the above, the Tribunal concluded that on the balance of probabilities a breach of Rule 2.3.3 had occurred.

Decision: UPHELD

### **Alleged breach 3**

#### **Rule 2.6.1**

*“Level 2 providers must ensure that consumers of their services are able to have complaints resolved quickly, easily and fairly and that any redress is provided quickly and easily”*

71. The Executive relied on 65 complainant reports all of which stated that complainants had experienced difficulties in resolving their complaint via the customer service telephone number provided on the text messages that had been sent to them. Examples included:

*“I received the first text on the 13th of June and replied STOP. I received the exact same message again today (27th) and replied STOP again. I then checked my credit with Giffgaff and noticed that £3 had been taken on the 13th even though I replied STOP. I think I'll be charged again as it doesn't seem to matter if I text stop. I have tried ringing the help number these texts provide, but it goes through to an answer machine only and I've yet to receive a response from them.”*

*“I recieved the message on friday saying I subscribed to something that I did not. I then rang my Network provider in order to sort the issue and they told me to ring the number provided on the text message, I did this but they were only taking messages and their mail box was full. I was also told to ring 03333352630, I did this and they told me that they do not deal with the company that has charged me. I also tried to text STOP to the company but then they told me that i would have to pay for this message, I did not do this as i did not want to pay another charge for something that wasn't my fault. Vodafone then gave me your number as you are the platform that the charge comes through. The amount of the bill is £3 every week. I would like you to stop this subscription as I am being charged for something that I did not subscribe to. I would like you to notify me as soon as you have stopped this charge.”*

*“I have received the text message on 11 June 2018, stating that I had subscribed to "fitguru" by Taptronic, which would charge me £3 per week. I have been charged once so far. I never subscribed to such service. I was unable to speak with anyone from that company. My phone operator (GiffGaff)*



*asked me to raise an inquiry with the Phone-Paid Services Authority.”*

72. As well as the initial complainant accounts, the Executive also relied on the answers provided by the 93 complainants who responded substantively to the consumer survey that was sent to them as set out below:

- 59 complainants confirmed that they raised a complaint with the provider via telephone/webform/email/letter/txt. Of the 59 consumers:
- 12 of the subscribers had attempted to contact the Level 2 provider via multiple means
- 12 consumers were offered a refund, one of which did not feel comfortable giving their bank details. One subscriber was offered a partial refund. One subscriber was offered a refund which they never received.
- 32 of the subscribers did not receive a reply to their complaint
- two subscribers were told they were not on their database
- two complainants stated they were hung up on by the Level 2 provider
- one complainant stated it had to track down the owner of the Level 2 provider directly via email in order to receive their refund
- one complainant stated that the telephone representative did not believe the consumer had a valid complaint.

73. The Executive asserted that while there was some evidence to suggest that the Level 2 provider had dealt with some consumer complaints, this had not been done consistently. The Executive therefore submitted that a breach had occurred as the complainant evidence clearly demonstrated that complainants had not had their complaints resolved quickly, easily or fairly.

74. The Executive noted that on 20 October 2019, the Level 2 provider had provided data which showed the number of calls and emails that were received by their call centre from July 2018 until October 2019. In total, the Level 2 provider received 1,596 telephone calls and 3,445 emails.

75. The Executive also directed the Level 2 provider to submit evidence of how it handled complaints in relation to 47 MSISDNs for complainants who had referenced attempting to contact the Level 2 provider in their complaint. Out of these 47 reports, the Level 2 provider only had evidence of how it had dealt with 15 of the complaints. When asked about its complaint process, the Level 2 provider stated the following:

*“When our CS team receives a complaint [our] they are conducting a short investigation by looking at the logs, the way the subscription happened, time and date and all this information is provided to the user. If the users are unhappy or they decide for any reason to cancel the subscription we are unsubscribe them from Fitguru service*

*and also we provide the refund. Furthermore, for underage or senior user the refund is processed straight away.”*

76. The Level 2 provider was also asked to provide evidence that the 53 consumers who had been signed up to the Service through the com.nitroxenon.okplayer app which was associated with the malware were refunded. The Level 2 provider submitted evidence that refunds were sent to the 53 consumers, however only 28 consumers cashed in their refunds.
77. The Executive also observed that out of 27 complainants whom the Level 2 provider had agreed to refund, the Level 2 provider was able to provide evidence in respect of 26. It stated that four had not requested a refund, 21 had received a refund and that one had not cashed in their refund.
78. The Level 2 provider denied the breach in its written response to the Warning Notice. The Level 2 provider stated that it had a call centre which was available between 9am and 5pm Monday to Friday and that out of hours consumers could leave details for a call back.
79. The Level 2 provider submitted that it issued a number of refunds to consumers in line with its refund policy. In terms of the process, the Level 2 provider stated that it used a system provided by a third party which was standard in the industry. The Level 2 provider explained that the third party was instructed to issue refunds via a spreadsheet completed by the call centre and that consumers could pick up their refund at the post office. The Level 2 provider indicated that all consumers were sent a text message and reminders to inform them that they had 28 days to pick up their refund after which time it would expire.
80. In relation to the one complainant that the call centre allegedly hung up on, the Level 2 provider accepted that this had occurred but explained that this had happened as the complainant had become abusive.
81. The Tribunal carefully analysed all of the evidence before it, including the submissions made by the Level 2 provider in respect of the breach.
82. The Tribunal accepted the Level 2 provider's assertions that some refunds had been provided to consumers and that it had a process in place for issuing refunds. However, the Tribunal was mindful that Rule 2.6.1 of the Code required providers to ensure that consumers had complaints resolved quickly, easily and fairly which meant that it required more from providers than just the issuing of refunds to some consumers.
83. The Tribunal was of the view that the complainant evidence from a number of different consumers clearly demonstrated that the Level 2 provider had not resolved complaints quickly, easily, or fairly and that the issue was widespread and not isolated to one or two consumers. The Tribunal was particularly concerned that the Level 2 provider only appeared to have records for 15 out of the 47 complainants that had attempted to

contact it. The Tribunal was of the view that this evidence meant that it was clear that not all complaints were recorded and dealt with as they should be. The Tribunal was therefore unable to accept the assertions of the Level 2 provider that no breach had occurred.

84. For all of the reasons set out above, the Tribunal found that on the balance of probabilities a breach of Rule 2.6.1 of the Code had occurred.

Decision: UPHELD

#### **Alleged breach 4**

##### **Paragraph 3.4.14**

*“Level 2 providers must, within two working days of the service becoming accessible to consumers, provide to the PSA relevant details (including any relevant access or other codes) to identify services to consumers and must provide the identity of any Level 1 providers concerned with the provision of the service.”*

85. On 14 June 2018 the Executive sent the Level 2 provider a service registration notification following complainant reports regarding the Service operating on shortcodes 64055 and 80206. Neither shortcode was registered.

86. The Level 2 provider registered shortcode 64055 on 15 June 2018 though it had been operational since May 2018. Shortcode 80206 remained un-registered by the Level 2 provider.

87. The Executive asserted that a breach of paragraph 3.4.14 had occurred as the Level 2 provider failed to register shortcode 64055 within two working days of the Service becoming active and failed to register shortcode 80206 for the entire time that the Service operated.

88. The Level 2 provider admitted the breach in part. The Level 2 provider accepted that it should have registered shortcode 64055 earlier and that this had been a mistake which had occurred as a result of a misunderstanding between the Level 2 provider and the relevant Level 1 provider. However, the Level 2 provider denied that the Service was operating on the second shortcode and stated that this shortcode was merely an additional opt-out mechanism. The Level 2 provider was therefore of the view that this shortcode did not need to be registered.

89. The Tribunal gave consideration to all of the evidence before it, including the representations by the Level 2 provider. The Tribunal was of the view that the Level 2 provider in effect admitted the breach in respect of shortcode 64055 and that as a result of this and the evidence submitted by the Executive the breach was made out.

90. In relation to shortcode 80206, the Tribunal noted that factually there was no dispute between the parties as it was agreed that this shortcode had not been registered. The Tribunal considered that the Code required providers to register “*all relevant access or other codes*” regardless of how they were being used. The Tribunal therefore considered that there was a duty on the Level 2 provider to register the shortcode 80206.

91. In light of the above, the Tribunal found the breached proved on the balance of probabilities in respect of both shortcodes.

Decision: UPHELD

## **Alleged breach 5**

### **Paragraph 4.2.2**

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

92. The Executive asserted that the Level 2 provider had acted in breach of Paragraph 4.2.2 of the Code as it had provided misleading and false information by way of message logs in relation to 22 consumers. The Executive submitted that the message logs had been altered to make it appear as though consumers’ opt-in dates occurred later than they did and/or to remove information which showed that consumers had opted out of the Service but were then re-subscribed.

93. The Executive relied on the billing information provided by the consumers in question, the message logs provided by the Level 1 provider, and the logs provided by the Level 2 provider.

94. The Executive highlighted a number of examples of the discrepancies that had occurred. For example, in respect of one consumer, their billing information indicated that they had opted into the Service on 25 May 2018. The message logs provided by the Level 1 provider mGage in respect of the same consumer also showed that the consumer’s subscription began on this date. However, the message logs provided by the Level 2 provider indicated that the subscription only began on 30 November 2018, almost six months later.

95. In relation to a second consumer, their billing information and the message logs provided by the Level 1 provider mGage both indicated that the consumers subscription started on 13 June 2018, however the Level 2 provider’s message logs indicated that the subscription began later on 12 September 2018.

96. In relation to a third consumer, though the opt-in dates on the Level 2 provider’s logs were consistent, the message logs provided by the Level 2 provider did not indicate that the consumer had sent STOP on 7 July 2018 and been unsubscribed only to become re-subscribed on 15 July 2018, whereas the Level 1 provider message logs clearly indicated that this had occurred.

97. The Level 2 provider denied the breach in its written response of 8 July 2021. The Level 2 provider indicated that it did not hold any MSISDNs on its database as the Level 1 provider would give each MSISDN an “alias”. The Level 2 provider explained that it would request the alias each time that the Executive requested it to provide message logs and that a mismatch must have occurred which explained the discrepancies as the same alias could be given to multiple MSISDNs.
98. The Level 2 provider asserted that it had no intention to conceal information from the Executive and that it had co-operated with the investigation fully.
99. The Tribunal carefully considered all of the evidence before it, including the Level 2 provider’s response. The Tribunal was of the view that it was clear that there were discrepancies between the message logs that were provided by the Level 2 provider, the message logs provided by the Level 1 provider, and the consumers’ billing information. The Tribunal was of the view that given the consumers’ billing information was consistent with the Level 1 provider’s message logs, there could be little doubt that the logs supplied by the Level 2 provider were incorrect.
100. The Tribunal noted that the Executive queried the situation in relation to the “alias” MSISDNs with the Level 1 provider. The Tribunal noted that the Level 1 provider confirmed that it was not possible for the same alias to be given to multiple MSISDNs. The Tribunal considered the explanation provided by the Level 1 provider regarding the system used for the “alias” MSISDNs to be credible. In addition to this, the Tribunal noted that it had not been provided with any evidence by the Level 2 provider which showed that multiple MSISDNs could have the same alias. For these reasons the Tribunal was unable to accept the assertions by the Level 2 provider that this was the cause of the discrepancy. The Tribunal therefore concluded that the Level 2 provider had knowingly provided message logs that were false and misleading.
101. Accordingly, the Tribunal found that on the balance of probabilities the breach was made out.

Decision: UPHELD

## **Alleged breach 6**

### **Paragraph 4.2.2**

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

102. The Executive asserted that a breach had occurred as the Level 2 provider had stated that it had suspended marketing for the Service between 2 January 2019 and 20 February 2019, but the subscriber logs indicated that consumers were still being subscribed to the Service during this period. The Executive submitted that the new subscriptions demonstrated that the Service was still promoting as otherwise new subscribers could not have signed up.
103. The Level 2 provider denied the breach. The Level 2 provider submitted that it had suspended marketing in this time period. It asserted that subscribers could have signed up to the Service after seeing earlier promotions as the Level 1 provider mGage had not suspended new subscribers from signing up.
104. In considering this breach, the Tribunal noted that it had seen clear evidence from the Executive that subscribers could be opted into the Service covertly as a result of malware. The Tribunal therefore questioned the Executive as to whether it was possible for promotions to have ceased but for consumers to nonetheless be signed up to the Service as a result of the malware. The Executive conceded that it was.
105. The Tribunal noted that the Level 2 provider had not asserted in its responses to the Executive that it had suspended the Service or stopped new subscribers from opting in, only that it had stopped promotions. The Tribunal also observed that the Executive had not provided any evidence to show that the Level 2 provider had continued promotions during this time (for example through monitoring of the Service) and that it was relying solely on the evidence of new subscribers in respect of the breach.
106. The Tribunal was of the view that it could not infer that the Service continued to be promoted solely as a result of the new subscribers to the Service particularly if it was possible for subscribers to have been subscribed covertly.
107. In light of the above the Tribunal decided that there was insufficient evidence to demonstrate that the Level 2 provider had knowingly or recklessly provided false and misleading information on the balance of probabilities.

Decision: NOT UPHOLD



## Alleged breach 7

### Paragraph 4.2.2

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

108. The Executive submitted that a breach had occurred as the Level 2 provider had falsely submitted that it was not the Level 2 provider for the Service until April 2018 when it had fact been part of the value chain from the outset.
109. The Executive noted that the Level 2 provider stated throughout the investigation that it became the sole Level 2 provider for the Service from April 2018 onwards and that another Level 2 provider, Itech Logic Limited, were historically the Level 2 provider from August 2017 to April 2018.
110. The Level 2 provider submitted a transfer of services in support of this assertion. However, bank statements from the Level 2 provider showed that it received all the revenue that the Service had generated from the time that the Service had first become operational.
111. The Executive received two different versions of the contractual agreement between Level 2 provider and Trendtech/Payguru, one of the Level 1 providers, both contracts were dated 4 May 2017. On the first page of both agreements, it was stated that the contract was between “Trendtech Ltd” and “Taptronic FZC”. One was signed by Ravi Kumar Metta on 4 May 2017 and detailed Itechlogic Ltd’s information in the schedule, the other was signed by another director on 4 May 2017 and detailed Taptronic FZC’s information in the schedule.
112. On 20 May 2021, the Executive sought further clarification from Payguru/Trendtech regarding the value chain. Payguru/Trendtech provided evidence to show that Ravi Kumar Metta requested a change of entities on 3 November 2017 as set out below:

 Re: Legal entity confirmation



Ravi Kumar Metta <ravi@itechlogic.net>

Friday, 3 November 2017 at 11:48

To: [REDACTED]

← You replied to this message on 03/November/2017, 18:03.

⚠ To protect your privacy, some pictures in this message were not downloaded.

Hi [REDACTED]

Please find the requested details.

company name: Taptronic FZC

company Number: 6006686

address:

PO Box: 331282

Ras Al Khaimah

UAE

KR

Ravi Metta

On Fri, Nov 3, 2017 at 10:33 AM, [REDACTED] <[\[REDACTED\]@payguru.com](mailto:[REDACTED]@payguru.com)> wrote:

Hi Ravi,

Can you share your Dubai-based legal entity details so I can send you the Sept. settlement report upon which you will be able to invoice me.

Thanks

[REDACTED]

September 2017 Invoice



Ravi Kumar Metta <ravi@itechlogic.net>

Friday, 17 November 2017 at 11:38

To: [REDACTED]

Cc: [REDACTED]

📎 IL-PGR90001.pdf (119.6 KB); 📎 PayguruGLOBAL\_Payment Agreement\_Taptronic FZC\_May2017.pdf (350.5 KB) [Preview All](#)

- You replied to this message on 12/January/2018, 12:42.

⚠ To protect your privacy, some pictures in this message were not downloaded.

Dear [REDACTED]

Hope your doing well .

Please find the attached invoice for our September 2017 traffic.

Please also find the attached signed Taptronic FZC contract.

113. The Executive submitted that the correspondence was clear in demonstrating that the Level 2 provider was the entity providing the Service. The Executive therefore submitted that in claiming that it had only operated the Service from April 2018, the Level 2 provider had knowingly provided false and misleading information.

114. The Level 2 provider denied the breach. In its response dated 8 July 2021, the Level 2 provider stated that the Level 2 provider was only incorporated on 24 May 2017. The Level 2 provider also stated that the individual who signed the contract had been employed elsewhere until 31 May 2017, so it was unclear as to how he could have signed the contract dated 4 May 2017. The Level 2 provider also asserted that it only started trading in October 2017, but this had been in the Indian and Asian markets only.

115. The Tribunal carefully considered all of the evidence before it, including the response by the Level 2 provider. The Tribunal noted that the evidence relied on by the Executive in relation to the breach was clear and that it clearly showed that the Level 2 provider had involvement in the Service from 2017 as opposed to from April 2018. The Tribunal was particularly persuaded by the evidence of revenue and the email correspondence provided by Payguru/Trendtech.

116. The Tribunal observed that while the Level 2 provider had submitted some documents which demonstrated the novation of the Service, it had provided no explanation as to why the Level 2 provider had received the revenue from the Service.

117. Having analysed all of the evidence before it, the Tribunal concluded that there was sufficient evidence to demonstrate that the Level 2 provider had been part of the value chain from the outset. The Tribunal decided that it followed on from this that in asserting that it had only become involved in the Service from April 2018, the Level 2 provider had knowingly provided false and misleading information to the Executive.

118. The Tribunal therefore found that on the balance of probabilities that a breach had occurred.

Decision: UPHELD

## Sanctions

### Representations on sanctions made by the Executive

#### Assessment of breach severity

119. The Tribunal's initial assessment of the breaches of the Code was that they were, overall, **very serious**. In making this assessment, the Tribunal found the following:

#### Rule 2.3.1

This breach was **very serious**.

The Tribunal considered that the breach was likely to damage confidence in the premium rate services and that it had occurred over a lengthy period of time.

The Tribunal also considered that as the Service was not accessible, it was incapable of providing any value to consumers, and that it presented a fundamental disregard for the requirements of the Code.

The Tribunal was also of the view that the breach had occurred over a significant period of time.

#### Rule 2.3.3

This breach was **very serious**.

The Tribunal considered that the breach had a clear and highly detrimental impact directly on consumers who may unknowingly and unwillingly be being signed up, and charged, for the service.

The Tribunal considered that consumers had incurred a wholly unnecessary costs as they did not intend to sign up for the service. The Tribunal also considered that the breach occurred over a lengthy period of time.

In addition to this, the Tribunal was of the view that the breach was likely to severely damage consumer confidence in premium rate services given that in this case, the presence of malware had meant that some consumers had been signed up to the Service covertly.

#### **Rule 2.6.1**

This breach was **very serious**.

The Tribunal was of the view that while there was some evidence of the Level 2 provider refunding some consumers, it was clear from the evidence that the Level 2 provider did not have details of how it had dealt with some consumers complaints.

The Tribunal noted that the Executive had recommended that this breach was serious however, the Tribunal was of the view that this had clearly had a highly detrimental and direct impact on consumers, and that it was likely to severely damage consumer confidence. In addition to this, the Tribunal considered that the breach had occurred over a lengthy duration. For these reasons, the Tribunal was of the view that the breach was very serious.

#### **Paragraph 3.4.14**

This breach was **very serious**.

The Tribunal noted that the Executive had only recommended that this breach be considered as serious.

However, the Tribunal was of the view that the Level 2 provider had only registered one shortcode when it was reminded to by the Executive, and, that it still did not accept that it was under a duty to register the second shortcode at all. The Tribunal was of the view that the breach in the circumstances of this particular case represented a fundamental disregard for the requirements of the Code and that it had occurred over an exceptionally lengthy duration given that the second shortcode remained unregistered.

For these reasons the Tribunal found the breach to be very serious.

#### **Paragraph 4.2.2**

This breach was **very serious**.

The Tribunal was of the view that the Level 2 provider had deliberately supplied message logs that it knew to be false and misleading. It considered that this breach had the potential to severely damage confidence in the premium rate services industry and that it presented a fundamental disregard for the requirements of the Code.

## Paragraph 4.2.2

This breach was **very serious**.

The Tribunal considered that the Level 2 provider deliberately misled the Executive regarding its involvement in the Service and that this presented a fundamental disregard for the requirements of the Code.

### Initial overall assessment

120. The Executive's initial assessment of sanction before any potential uplift or downgrade in light of aggravating or mitigating factors, was that the following sanctions were appropriate:

- a formal reprimand
- a prohibition on the Level 2 provider from providing, or having any involvement in, any premium rate service for a period of six years, starting from the date of publication of the Tribunal decision, or until all sanctions imposed have been complied with, whichever is the later
- a requirement that the Level 2 provider must refund all consumers who claim a refund for the full amount spent by them on the Service, within 28 days of their claim, save where there is good cause to believe such claims are not valid, and provide evidence to the PSA that such refunds have been made
- a fine of £1,525,000.00 broken down as follows:
  - Breach 1 Rule 2.3.1 - £250,000
  - Breach 2 Rule 2.3.3 - £250,000
  - Breach 3 Rule 2.6.1 - £100,000
  - Breach 4 Paragraph 3.4.14 - £175,000
  - Breach 5 Paragraph 4.2.2 - £250,000
  - Breach 6 Paragraph 4.2.2 - £250,000 (not proved)
  - Breach 7 Paragraph 4.2.2 - £250,000.

121. The Level 2 provider did not make representations in relation to the proposed sanctions.

122. The Tribunal considered the sanctions recommended by the Executive and was broadly in agreement. However, the Tribunal was particularly concerned about the circumstances of the case and in particular the presence of malware which had covertly signed up consumers to the Service. Having noted that the Service had been previously novated from a different Level 2 provider, the Tribunal was of the view that it should also impose a bar to accessing the Service in addition to the prohibition.



123. The Tribunal noted that this was an exceptional course of action. However, the Tribunal was of the view that the unique circumstances of this case merited the approach of not only restricting the Level 2 provider through the prohibition sanction but also restricting the access to the Service itself. The Tribunal was of the view that in line with the prohibition, the bar should be for a period of six years given the severity of the breaches.

124. The Tribunal also noted that it would need to adjust the proposed fine to take account of breach 6 not having been upheld. The Tribunal also considered that as it had increased the severity ratings of breaches 3 and 4, that the initial fine amounts should be uplifted to reflect this.

125. The Tribunal accordingly adjusted the initial assessment of sanctions to the following:

- a formal reprimand
- a prohibition on the Level 2 provider from providing, or having any involvement in, any premium rate service for a period of six years, starting from the date of publication of the Tribunal decision, or until all sanctions imposed have been complied with, whichever is the later
- a requirement that access is barred to the “Fitguru” Service for a period of 6 years
- a requirement that the Level 2 provider must refund all consumers who claim a refund for the full amount spent by them on the Service, within 28 days of their claim, save where there is good cause to believe such claims are not valid, and provide evidence to the PSA that such refunds have been made
- a fine of £1,450,000.00 broken down as follows:
  - Breach 1 Rule 2.3.1 - £250,000
  - Breach 2 Rule 2.3.3 - £250,000
  - Breach 3 Rule 2.6.1 - £250,000
  - Breach 4 Paragraph 3.4.14 - £200,000
  - Breach 5 Paragraph 4.2.2 - £250,000
  - Breach 7 Paragraph 4.2.2 -£250,000

## **Proportionality assessment**

### **Assessment of mitigating and aggravating factors**

#### **Aggravation**

126. The Tribunal noted that the Executive had advanced a number of aggravating factors in the case. The Tribunal was of the view that a number of those aggravating factors

were an inherent part of the breaches that it had found proved (for example the failure to follow guidance and the level of cooperation by the Level 2 provider). The Tribunal did not therefore consider these matters to be additional aggravating factors.

127. The Tribunal did however agree that it was an aggravating factor that the breaches continued after the Level 2 provider became aware of them and that while the Level 2 provider did not have a breach history, one of the directors had been previously prohibited by the Executive following an adjudication in respect of Itech Logic Ltd in respect of a different service.

### **Mitigation**

128. The Tribunal agreed with the Executive that it was a mitigating factor to the case that the Level 2 provider had provided refunds to some consumers (which had been evidenced).

### **Financial benefit/Need for deterrence**

129. The Executive stated that the Service had generated a total revenue of £992,170.55 across both value chains.
130. The Executive submitted that the revenue generated by the Level 2 provider flowed directly from the breaches of Rule 2.3.3. and 2.3.1 as consumers had not been able to access the Service even where they had knowingly subscribed to it and many complainants had been signed up to the Service without their knowledge. Given the severity of the breaches found proven, the Executive asserted that there was in this case a need to remove the entirety of the financial benefit from the Level 2 provider.
131. The Level 2 provider did not make any representations as to the proposed sanctions.
132. The Tribunal agreed that for the reasons advanced by the Executive that the revenue from the Service flowed directly from the breaches. The Tribunal also agreed that given the wide ranging and serious nature of the breaches (particularly in respect of consent to charge) there was a need to remove the entirety of the financial benefit from the Level 2 provider in order to send out a clear message that conduct of the kind found proven was unacceptable.

### **Sanctions adjustment**

133. The Tribunal considered that there was only minimal mitigation in the case and that the sanctions therefore remained. The Tribunal decided that while exceptional, the prohibition and bar on access to Service remained proportionate as they were necessary to ensure that any future consumer harm was prevented and to achieve the sanctioning objective of credible deterrence as well as maintain and uphold confidence in the industry.

134. The Tribunal did however note that the proposed fine exceeded the amount of revenue which the Service had generated. Although the Tribunal was not provided with any specific information in relation to the impact that the fine was likely to have on the Level 2 provider, it surmised that it would be likely to have a highly detrimental impact. The Tribunal therefore agreed with the Executive that the fine should be reduced to a total of £1,250,000 overall.

135. The Tribunal was of the view that this amount would remove the financial benefit from the Level 2 provider and that the additional uplift was proportionate and appropriate given the severity of the breaches found proved.

### Final overall assessment

136. The Tribunal concluded that the seriousness of the case should be regarded overall as **very serious**.

### Sanctions imposed

- formal reprimand
- a prohibition on the Level 2 provider from providing, or having any involvement in, any premium rate service for a period of six years, starting from the date of publication of the Tribunal decision, or until all sanctions imposed have been complied with, whichever is the later
- a requirement that the access to the Fitguru service is barred for a period of six years
- a requirement that the Level 2 provider must refund all consumers who claim a refund, for the full amount spent by them on 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 PSA that such refunds have been made
- a fine of £1,250,000 comprised of:
  - Breach 1 Rule 2.3.1 - £100,000
  - Breach 2 Rule 2.3.3 - £250,000
  - Breach 3 Rule 2.6.1 - £200,000
  - Breach 4 Paragraph 3.4.14 - £200,000
  - Breach 5 Paragraph 4.2.2 - £250,000
  - Breach 7 Paragraph 4.2.2 - £250,000

137. Administrative charge recommendation: 100%