

Tribunal meeting number 201

Case reference: 72403
Level 2 provider: Venture247 Limited
Type of service: Adult video subscription service
Level 1 provider: Veoo Ltd; mGage Europe Limited
Network operator: All Mobile Network operators

This case was brought against the Level 2 provider under Paragraph 4.5 of the Code of Practice (“the Code”)

Background

The case concerned an adult video subscription service operating on dedicated shortcodes 89320, 69988 and shared shortcode 89225 (the “**Service**”).

The Level 2 provider for the Service was Venture247 Limited (the “**Level 2 provider**”). The Level 2 provider has been registered with the Phone-paid Services Authority since 10 December 2013.

The Level 1 provider for Service shortcode 89320 was mGage Europe Limited (“**mGage**”). mGage has been registered with the Phone-paid Services Authority since 31 December 2013. The Level 1 provider for Service shortcodes 69988 and 89225 was Veoo Ltd (“**Veoo**”). Veoo has been registered with the Phone-paid Services Authority since 17 August 2011.

The Service

The Service was stated to be an adult video subscription service charged at £3 per week. The Level 2 provider confirmed that the Service commenced operation on 5 January 2014. The Level 2 provider stated in their response to an enquiry dated 7 April 2016 that they were not currently promoting any live services.

mGage confirmed that the Service commenced operation on shortcode 89320 in January 2014. Veoo confirmed that the Service commenced operation on shortcode 89225 on 5 April 2014 and on shortcode 69988 in 25 July 2015.

The Executive noted from message logs supplied by the Level 2 provider that users of the Service opted in to the Service on shortcode 89320. All Service users were then migrated to either Service shortcode 89225, or Service shortcode 69988. Further, the Executive noted that the user migration from shortcode 89320 to shortcode 89225 or 69988 was staggered over a period of time.

The Level 2 provider supplied a summary of the promotion and operation of the Service, which is attached at **Appendix A**.

Summary of complaints

The Executive received 70 complaints concerning the Service between 19 April 2015 and 19 December 2016. Complainants variously alleged that the Service charges were unsolicited.

A sample of complainant accounts is provided below:

I have not signed up for any services but have been charged for them sending me text messages asking for me to sign up to certain services.
the company is apparently called venture 247
£20.42 in one month

"A text message about a "mobile babes" website stating that if I don't text stop to a specific number I will be charged x amount of money. I don't text back because then these scammers know you exist. On my bill I have been charged four times at a rate of £2.50 for text messages received from this company. Are they having a f**king laugh?"

"I received unwanted text messages offering explicit services, I never requested these services or offered my number to this company. They would bill me every month for several messages usually at £3 per message

so far the total amount billed has been £50"

"the bill they have charged for, 4 text is 24 pounds

We don't know who they are they have now sent my grandson four text message's he opens the message does not know who they are and delete's and they chages my grand son is 11yrs old" [sic]

Complainant text message logs

As part of the standard request for information process, the Level 2 provider supplied text message logs for the complaints received. The Executive noted from the text message logs supplied by the Level 2 provider that:

- there was a high failure rate of chargeable Service messages following the purported consumers' opt-in; and
- the delivery status for Service messages was unclear.

In these logs, failed messages occurred from the date of the complainants' purported opt-in. The failed messages were later followed by successfully delivered chargeable messages.

Previous complaint resolution procedure

The Level 2 provider had a prior informal dealing with the Phone-paid Services Authority. On 7 January 2015, the Level 2 provider was sent a Track 1 action plan in respect of a breach of rule 2.3.3 of the Code, as the Level 2 provider accepted that it did not hold robust verification to establish consumers' consent to be charged prior to January 2015. On 15 January 2015, the Level 2 provider confirmed that it had implemented the required actions and had engaged the services of a third party verifier to provide robust evidence of consent to charge.

The breach allegations raised in this case relied on evidence gathered from complainants who first contacted the Executive after 15 January 2015, the date on which the Track 1 procedure was finalised.

The Investigation

In accordance with the transitional arrangements set out at paragraph 1.8 of the Code (14th Edition), the Executive conducted this matter as a Track 2 procedure in accordance with paragraph 4.5 of the Code of Practice (14th Edition).

The Executive sent a Warning Notice to the Level 2 provider on 19 December 2016 with a deadline for response of 5 January 2017. Within the Warning Notice the Executive raised the following breaches of the Code:

- Paragraph 4.2.4 – Provision of false / misleading information to the Phone-paid Services Authority
- Rule 2.3.3 – Consent to charge

On 6 February 2017, the Tribunal reached a decision on the breaches raised by the Executive. The Tribunal considered the following evidence in full:

- The complainants' accounts;
- Correspondence between the Executive and the Level 2 provider (including directions for information and the Level 2 provider's responses including supporting documentation);
- Correspondence between the Executive and Level 1 providers;
- Correspondence between the Executive and a third-party verifier;
- Correspondence between the Executive and the Verifier;
- Complainant message logs from the Level 2 provider and Level 1 provider;
- Extracts from Xpert360 logs (limited to the periods when the purported opt-ins occurred);

- Revenue information for the Level 2 provider's Service;
- The Warning Notice dated 19 December 2016, including attachments;
- The Level 2 provider's response, including attachments; and
- Information regarding refunds made (supplied to the Executive on 27 January and 3 February 2017).

Preliminary issue

The Tribunal noted that the Executive had received further evidence from the Level 2 provider on 27 January and 2 February 2017. The evidence included a table showing refunds made in respect of the Service. This evidence had been submitted the working day before the Tribunal took place, and substantially after the deadline for response to the Warning Notice.

In response to queries about the evidence, the Executive stated that it would not have had time to verify all the refunds claimed in the table. However it had been able to confirm that, of the 70 complainants to the Phone-paid Services Authority, the table stated that 45 had received and cashed refunds, 2 had been sent a refund but had not cashed it, and 23 were not present in the table.

The Tribunal considered whether it was in the interest of justice for it to exercise its discretion to admit the late evidence. Whilst the Tribunal understood that the Executive would not have had time to verify all the refunds on the list (and indeed understood there might be privacy concerns about cold calling consumers on this list), they considered there was no real prejudice to the Executive by its inclusion taking into account the nature of the evidence.

Submissions and Conclusions

Alleged Breach 1

Paragraph 4.2.4 – “A party must not knowingly or recklessly conceal or falsify information, or provide false or misleading information to the Phone-paid Services Authority (either by inclusion or omission).”

1. The Executive asserted that the Level 2 provider had breached paragraph 4.2.4 of the Code on the basis that the message logs supplied by the Level 2 provider were false. The Executive asserted that the failed chargeable Service messages listed in the Level 2 provider message logs were not sent (or attempted to be sent) to complainants.

The Executive relied on correspondence exchanged with the Level 2 provider, mGage, Mobile Enterprise Ltd and Xpert360 Ltd.

The Executive noted that the complaints received by the Phone-paid Services Authority following the Track 1 procedure spanned the period between April 2015 to October 2016. Further, it noted from complainant text message logs supplied by the Level 2 provider that the apparent opt-in date for those complainants was consistently shown in all message logs as occurring between August 2014 and November 2014, regardless of when the complaint was received. Yet in the complainant message logs the date of the first successfully charged Service message was significantly later than the purported date of Service opt-in.

As set out in the 'Background' section above, the Executive noted that it was common for

complainant text message logs to show several months of failed chargeable Service messages prior to the issuing of successfully charged Service messages. The Executive understood that consumers that only received failed messages following their opt-in would not have been charged. A summary of three example message logs is provided below:

Level 2 provider message log for mobile number *****2979

The Executive noted that the provided log shows that the initial opt-in to the Service occurred on 26 September 2014. The subscription confirmation message stated:

"FreeMsg: U have subscribed to hot-mobilebabes for £3 per week until you send STOP to 89320 ,Help:01138272094. SP Venture247 18+ New Videos available every week"

The Executive noted that, following the above entry in the message log, the status of all chargeable Service messages on shortcode 89320 were listed as either 'FAILED', or 'SENT'. The first Service message listed as 'BILLED' was on shortcode 89225 (after the Service had migrated to Veoo) and was delivered on 18 April 2015, more than seven months after the purported opt-in date.

Level 2 provider message log for mobile number *****4300

The Executive noted that the provided log shows that initial opt-in to the Service occurred on 3 October 2014. The subscription confirmation message stated:

"FreeMsg: U have subscribed to hot-mobilebabes for £3 per week until you send STOP to 89320 ,Help:01138272094. SP Venture247 18+ New Videos available every week"

The Executive noted that following the above entry in the message log, the status of all chargeable Service messages on shortcode 89320 were listed as 'FAILED', 'SENT' or 'ACCEPTED'. The first message listed as 'BILLED' was on shortcode 89225 (after the Service had migrated to Veoo) and was delivered on 9 May 2015, almost seven months after the purported opt-in date.

Level 2 provider message log for mobile number *****7360

The Executive noted that the provided log shows that initial opt-in to the Service occurred on 18 September 2014. The subscription confirmation message stated:

"FreeMsg: U have subscribed to hot-mobilebabes for £3 per week until you send STOP to 89320 ,Help:01138272094. SP Venture247 18 New Videos available every week"

The Executive noted that following the above entry in the message log, the status of all chargeable Service messages on shortcode 89320 were listed as either 'FAILED', 'ACCEPTED' or 'SENT'. The first message listed as 'BILLED' was on shortcode 89225 (after the Service had migrated to Veoo) and was delivered on 9 May 2015, almost eight

months after the purported opt-in date.

The Executive also relied on further examples of message logs supplied by the Level 2 provider which contain failed chargeable Service messages in the period immediately after the consumer's purported opt-in, followed by successfully delivered chargeable messages a significant period of time later.

In order to verify the message logs provided by the Level 2 provider, the Executive contacted the Level 1 provider, mGage, for a sample of complainant message logs.

Of the 30 messages logs requested from mGage, only one log was provided. mGage confirmed that, with the exception of one MSISDN (*****2542), the remaining MSISDNs had no interaction with the Service. The message log for MSISDN *****2542 indicated that the opt-in took place on 13 March 2014 which was before the primary complainant opt-in period of August 2014 and November 2014, and prior to the suspension of the Service by mGage.

The Executive submitted that the logs provided by the Level 2 provider, which revealed a purported opt-in on Service shortcodes followed by a series of failed messages, were not verified by the information received from the Level 1 provider.

In order to verify the message logs provided by the Level 2 provider, the Executive also contacted the Level 1 provider, Veoo, for a sample of complainant message logs. The logs supplied by Veoo confirmed that the first chargeable Service message on the Level 2 provider logs occurred after the Service had migrated to Veoo.

In order to obtain further clarification on the message failure issue, the Executive contacted Mobile Enterprise Ltd (the "**Verifier**") which has access to mobile data held by the Mobile Network operator Vodafone Limited ("**Vodafone**"). The Verifier was sent a sample of eight Vodafone complainant mobile numbers and was requested to supply message logs showing the interaction between the Service and the complainants' mobile numbers.

The Executive noted from the eight message logs supplied by the Verifier that generally the first message log entry occurred on the same date that successfully charged Service messages were shown within the Level 2 provider messages logs. For example the Verifier log for *****2979 listed the first Service message on 18 April 2015.

The Executive noted that the Verifier had confirmed that messages sent from the Service shortcodes with the status "failed" would appear in its text message logs.

The Executive contacted a third party verifier, PinChecked, in order to establish whether or not it could provide evidence that the complainants had opted in to the Service. PinChecked advised that the verification service that it provided had been taken offline and that records were no longer available.

The Executive asserted that the message logs supplied by the Level 2 provider cannot be accurate for the following reasons:

- The discrepancy between the logs supplied by the Level 2 provider and the information provided by mGage, the Verifier and Xpert360 Ltd (as explained above)
- The purported opt-ins occurred at a time when all services operating on the shortcode 89320 had been suspended by mGage
- The method of opt-in described by the Level 2 provider was not supported by the evidence; and
- Chargeable Service messages were purported to be have been sent at a time when the Service had been suspended

The purported opt-ins occurred at a time when all services operating on the shortcode 89320 had been suspended by mGage

The Executive noted that all the Level 2 provider's services were suspended by mGage from 27 March 2014. Based on the message logs received from the Level 2 provider, the primary complainant opt-in period was between August 2014 and November 2014.

The Executive asked mGage whether it would be possible for the Level 2 provider to opt in consumers while the Service had been suspended. mGage provided the following response:

“mGage: The L2 will not be able to opt a consumer into a service through the mGage gateway after the service has been suspended.”

In response to questioning by the Tribunal about how the Service came to be suspended, the Executive stated that it understood that, after the Service had been novated from the previous Service provider, the Level 1 provider would have been required to do risk assessment and control on the Service, including testing of the Service, and that mGage had found apparent discrepancies during this testing and dialogue, which was when the Service was suspended.

The Executive asked the Level 2 provider how consumers were able to subscribe to the Service during a period where the Service had been suspended. The Level 2 provider gave the following answer:

For a long period of time after our shortcode was suspended we attempted to work with mGage to get our code reactivated. Through a number of calls and emails at a number of stages we believed that several times we were very close to getting the code live again. The service flow that the Executive had seen at the time started with the inputting there msisdn into our online advertising pages and then be sent a further URL with terms and conditions of the service and could decide by clicking on the button if they wanted to initiate a service. This is all done without using the bulk route from mGage and this is how the consumer could opt-in the service.

The Executive asked the Level 2 provider to clarify what it meant by “bulk route from

mGage” and explain how the consumer could opt-in without using this bulk route. The Level 2 provider answered:

I would have fully expected the Executive to know and understand the key aspects of the Pinchecked service that they had approved as a 3rd party verification company. It is through the basic understanding of how this service worked that the executive would know that we do not need to use the bulk route provided by mGage.

The Executive noted that the Level 2 provider did not implement the use of Pinchecked until 15 January 2015, this being the date when the previous Track 1 procedure was agreed. However, the primary opt-in period was between August 2014 and November 2014. Therefore the Level 2 provider’s explanation would not explain why the consumers would be able to opt-in while the Service was suspended by mGage.

The Executive referred the Level 2 provider's assertion that consumers could opt into the Service outside of its gateway to mGage. The Executive asked mGage to confirm whether it would be possible for consumers to opt-in using the method as suggested by the Level 2 provider. mGage confirmed that it would not be possible for consumers to opt in using the method submitted by the Level 2 provider.

For the reasons outlined above, the Executive submitted that the purported opt-ins as detailed in the message logs supplied by the Level 1 provider did not occur as consumers would not have been able to opt-in to the Service while all services had been suspended by mGage.

The opt-in method described by the Level 2 provider is not supported by the evidence

The Level 2 provider has submitted a description of how consumers may opt-in to its Service currently via its website (**Appendix A**) after viewing an online banner advertisement. However, the message logs supplied by the Level 2 provider for all complainants indicate that the complainants opted in following the receipt of a direct marketing message.

The Executive noted that the Level 2 provider has previously stated that it used the direct marketing message method of promoting the Service. In response to a previous direction for information, the Level 2 provider supplied the following consumer journey:

1. *We operate our service using third party marketing data, where the customer has opted into one of our third party’s services and has agreed to receive further marketing messages of a similar nature.*
2. *We receive a MSISDN from our third party operator, to which we then send out our own free marketing wap message.*
3. *This arrives on customer’s phone, they then open up this wap message which leads them to our site. This will clearly highlight all our terms and conditions of the service that we are offering to the customer.*
4. *After reading all our Terms and Conditions the customer can then decide to subscribe to our*

- service by clicking ENTER, accepting all terms and conditions as well as costs involved.*
5. *The customer will then receive a join message which again highlights all costs that are involved in our service.*
 6. *To allow the customer the opportunity to change their mind or to make sure that they are satisfied with our terms and conditions and costs we allow a day before we bill the customer. This allows them to opt out at anytime and they will not be charged for the service.*
 7. *We then send out weekly billed messages and also send out monthly reminders to the customers. They can text STOP at anytime and this will cease their subscription with no further costs.*

The Executive understood that this method of subscribing to the Service would be dependent on the consumer receiving the initial marketing message. In order to verify the message logs provided by the Level 2 provider, the Executive contacted the Level 1 provider, mGage, for a sample of complainant message logs. Of the 30 logs requested, only one log could be provided. The Executive noted that the log supplied by mGage did not contain the opt-in message.

In order to obtain further verification of the message logs provided by the Level 2 provider, the Executive contacted Xpert360 Ltd (“**Xpert360**”), which has access to mobile data held by Vodafone. Xpert360 was sent a sample of seven complainant mobile numbers and was requested to supply message logs showing all the traffic on the MSISDNs.

The Executive noted from the six message logs supplied by the Xpert360 that there was no traffic on the MSISDNs on the dates when the purported opt-in messages were sent. Therefore, the Executive asserted that the message logs supplied by the Level 2 provider were false.

Level 2 provider message log for mobile number *****2979

The Executive noted that the provided log showed that the initial opt-in to the Service occurred on 26 September 2014. The Level 2 provider’s log indicated that a marketing message was sent on this date at 18.42, which was followed by a text message at 18.45 confirming that the consumer had been subscribed to the Service (**Appendix C**).

The Executive noted that when compared to the message log from Xpert360 for the month of September 2014, the above messages cannot be found.

Level 2 provider message log for mobile number *****5133

The Executive noted that the provided log shows that the initial opt-in to the Service occurred on 5 September 2014. The Level 2 provider’s log indicated that a marketing message was sent on this date at 16.21, which was followed by a text message at 16.24 confirming that the consumer had been subscribed to the Service (**Appendix C**).

The Executive noted that when compared to the message log from Xpert360 for the month of September 2014, the above messages cannot be found.

For the reasons outlined above, the Executive asserted that the opt-in messages found within the Level 2 provider logs are false.

Chargeable Service messages were purported to be have been sent at a time when the Service had been suspended

The Executive had directed the Level 2 provider to provide an explanation for the high failure rate of chargeable Service messages. On 20 April 2016 the following response was received from the Level 2 provider:

As detailed above, throughout all the email and telephone correspondence between us and ... head of compliance at mGage, we believed we were very close to getting our code live again. We had no reason to think that this was not going to happen promptly at anytime and so we did not change the routes that had been very successful for us in the past, the only analogy that we can think of is a light switch remaining on whilst there's no bulb in the light fitting.

The Executive noted that, in contrast to the Level 2 provider's explanation, mGage confirmed that no billing attempts would be made during the suspension of the Service.

The Executive noted that the Level 2 provider had indicated that it attempted to send Service messages in spite of the suspension by mGage of all services operating on shortcode 89320. The Executive noted from the message logs supplied by the Level 2 provider that the status of the Service messages were variously described as 'FAILED', 'ACCEPTED', 'BILLED' or 'SENT'. The Executive requested clarification regarding the message statuses. The Level 2 provider supplied the following information:

FAILED – Is where the attempted message that was sent has not reached the handset.

BILLED – Is where the attempted message that was sent has reached the handset.

ACCEPTED – Is where our server has attempted to send the correct message but for a number of reasons it may not have yet left our server.

SENT – Is where our server is aware that we have attempted to send the correct message but we have not received a Delivery Receipt (DR) to acknowledge if it has FAILED or BILLED.

The Level 2 provider confirmed that messages with a 'FAILED' status are messages where it had received a 'Delivery Receipt' to acknowledge that it has failed. The Executive asked mGage to confirm whether, if an attempt was made to bill a consumer during service/gateway suspension and the message failed, would the Level 2 provider and mGage be notified of such a failure (and if so, how). The Level 1 provider responded as follows:

"No there would be no billing attempts made."

When asked to clarify its answer, mGage confirmed that no notification would be sent to

the Level 2 provider. The Executive submitted that messages within the logs with a 'FAILED' status cannot be genuine on the basis that such messages would not have received a Delivery Receipt while the gateway was suspended.

In response to questioning by the Tribunal about whether it was conceivable that the "freemsgs" were sent by a third party other than mGage, the Executive stated that this had not been asserted by the Level 2 provider in its response, and the Level 2 provider had not provided the name of a third party sending messages on its behalf other than mGage, so this was not known to them. The Executive clarified that it would expect to see all messages on mGage's logs which went across their platform, including any "freemsgs", and noted that mGage had in fact only been able to provide one log in respect to all of the complainants whose logs had been requested.

The Executive noted from the previous Track 1 procedure that the Level 2 provider had accepted that it did not have robust verification prior to 12 January 2015. The Executive submitted that the Track 1 procedure was created in part to address the issue of consent to charge that had occurred during the third and fourth quarters of 2014. The Executive noted however that it continued to receive complaints about consent to charge well into the third quarter of 2015. The Executive's view was that by inserting failed messages into logs and creating artificial opt-in dates in the period prior to closure of the Track 1 procedure, the Level 2 provider had attempted to persuade the Executive that a consent to charge breach arose only in a limited period, and that the scope of such a breach was confined to a lack of independent third party verification, as opposed to a wider allegation of unsolicited charges.

In light of the evidence provided by mGage, the Verifier and Xpert360, the Executive considered that the message logs supplied by the Level 2 provider were incorrect, and the Executive had been provided with false information.

The Executive asserted that, for all the reasons stated above the Level 2 provider had provided false or misleading information to the Phone-paid Services Authority during the Executive's investigation into the Service. Accordingly, the Executive asserted that the Level 2 provider had breached paragraph 4.2.4 of the Code.

2. The Level 2 provider denied the breach. The Level 2 provider asserted that the Executive had gone to a lot of needless effort to attempt to prove that messages were not sent, but had failed to understand a system that they themselves recommended on their website as a form of third party verification.

The Level 2 provider stated that the Service had been novated to it from the previous Service provider, whom at the time had an account with Pinchecked. The Level 2 provider continued to attempt to integrate this into all our services. The Level 2 provider had confirmed as part of its previous Track 1 procedure that robust verification was not in place for every service, but going forward any new subscriber would be subscribed using this service which allowed the Track 1 procedure to be closed. The Level 2 provider stated that the Executive at that time were aware that previous subscribers were not all

subscribed to its Pinchecked services as it had issues fully implementing it into every service. The Level 2 provider stated that this did not mean that it had no service using it, and the Level 2 provider produced a purchase order for additional top up PINs, dated 17 November 2014. The Level 2 provider stated that this proved that it was promoting this service and using PINs prior to that date, which would include August to October 2014.

The Level 2 provider stated that its Pinchecked service flow was as follows:

- “Venture247 placed promotional banners on appropriate websites
- Customer clicks on banner advertisement
- Customer is then directed to our Pinchecked integrated landing page
- Customer inserts their MSISDN
- Pinchecked sent customer unique confirmation page with pin
- Customer enters pin and subscribes
- Pinchecked kept records on opt-in for verification
- Venture247 sends join message – subscription messages “

The Level 2 provider explained that when it advertised online and a customer inserted a MSISDN, they were then sent a further message from the Pinchecked platform to allow for them to be able to verify robustly if the customer then proceeds into the service (meaning that this can't be tampered with). The Level 2 provider explained that if the customer decided to subscribe, its platform then attempts to send out the join message.

The Level 2 provider asserted that, at the time of advertising from March 2014 onwards, it was in constant communication with mGage attempting to get its code suspension lifted. The Level 2 provider asserted that because it believed this was very close to occurring, it never stopped its advertising spend to gain subscribers. The Level 2 provider asserted that, when its code was suspended by mGage it would stand to reason that if its message attempts failed before they even reached the Level 1 provider, they will automatically not be seen by Mobile Enterprise Ltd or Xpert360 Ltd.

The Level 2 provider asserted that when it realised that it would no longer be getting its code suspension lifted, it then started the process of migration to another Level 1 provider. The Level 2 provider stated that as part of the migration process, it was required by its aggregator to provide random sample opt-in details for each batch of numbers, as all numbers were verified by Pinchecked. The Level 2 provider invited the Executive to verify this with Veoo. The Level 2 provider stated that it was able to complete this reasonably easily, but it had an initial effect on a small number of subscribers who for one reason or another questioned their subscription which resulted in a small spike in complaints which it believed had caused this investigation. The Level 2 provider asserted that when this was brought to its attention in April 2016, it took internal decisions to cease attempting migrations and it had since seen a dramatic decrease in complaints.

The Level 2 provider submitted that it was strange that the Executive mentioned the MSISDNs *****2979, *****4300 and *****7360, and that they started billing on

18th April 2015 and 9th May 2015 respectively, since the initial assessment from the Executive was sent on 26th May 2015, and the Level 2 provider submitted that the case had already been pre-decided as an effort to target the Level 2 provider.

3. The Tribunal considered the Code and all the evidence before it.

The Tribunal considered the Executive's evidence, including in particular the nature of the complaints, the type and nature of the discrepancies between the Level 2 provider's logs and the Level 1 provider, Xpert360 and Verifier logs, and the relevant correspondence. The Tribunal noted that the Executive had advanced four separate grounds, as a result of which the Level 2 provider's logs appeared to be false or misleading. The Level 2 provider had been given the opportunity to answer each of these grounds but had failed to do so adequately or at all, and had failed to provide supporting evidence for any such explanation.

In the absence of credible explanations supported by reliable evidence the Tribunal found that there was a compelling body of cogent evidence to show, on a balance of probabilities, that the Level 2 provider had produced false message logs which it had submitted to the Executive. Consequently, the Tribunal was satisfied, on the balance of probabilities, for each of the reasons advanced by the Executive, that the Level 2 provider had provided false and misleading information to the Executive. Accordingly, the Tribunal upheld a breach of paragraph 4.2.4 of the Code.

Decision: UPHELD

Alleged Breach 2

Rule 2.3.3. - "Consumers must not be charged for premium rate services without their consent. Level 2 providers must be able to provide evidence which establishes that consent."

1. The Executive asserted that the Level 2 provider had breached rule 2.3.3 of the Code as consumers had been charged without their consent, and the Level 2 provider had been unable to provide evidence which established that consent.

The Executive referred to the allegations made of breach of paragraph 4.2.4, asserting that complainant message logs supplied by the Level 2 provider, which purported to demonstrate that consumers opted-in to the Service in a period when the Level 2 provider did not have operational robust verification of consent to charge, were false.

The Executive had requested that mGage provide message logs for 30 complainants. The Executive noted that mGage could only provide one message log that showed interaction with the Service. Referring to the alleged breach of paragraph 4.2.4, the Executive noted that the Level 2 provider attributed the failed messages to the fact that the messages were being sent at a time when mGage had suspended its gateway to the Level 2 provider. The Executive noted that mGage has confirmed that consumers could not opt-in to the Service via its gateway while the Service was suspended. Accordingly, the Executive submitted that as the complainant message logs provided by the Level 2 provider purportedly showing consumers' opt-ins to the Service were false, there was

no valid evidence of opt-in to the Service and accordingly the complainants could not have consented to Service charges.

The Executive submitted that message logs which showed a 'FAILED' status for messages sent during the suspension period were false. The Executive noted that the Level 2 provider had indicated that messages with a 'FAILED' status are ones where it has received a Delivery Receipt from the Level 1 provider, but mGage has advised that such notifications would not be provided when its gateway to the Level 2 provider had been suspended. Furthermore, messages with a 'FAILED' status also appeared on the message logs when the agreement between mGage and the Level 2 provider had been terminated. The Executive therefore submitted that the messages listed in the Level 2 provider message logs with a 'FAILED' status were not sent (or attempted to be sent) to complainants.

Referring to the alleged breach of paragraph 4.2.4, the Executive's view was that by inserting failed messages into logs and creating artificial opt-in dates in the period prior to closure of the Track 1 procedure, the Level 2 provider had attempted to persuade the Executive that the consent to charge breach arose only in a limited period, and that the scope of the breach was confined to a lack of independent third party verification rather than a more serious allegation of unsolicited charges.

In response to questioning by the Tribunal about whether the previous Track 1 action plan stipulated that the Level 2 provider must re-opt-in all its existing subscribers, the Executive confirmed this wasn't stipulated in the plan devised at the time.

The Executive submitted that, in any event, the Level 2 provider had charged consumers in the period after 15 January 2015 whilst knowing that it did not have the required robust third party verification of consent to charge in respect of those consumers. The Executive submitted that even if consumers had opted-in prior to this date, at the time the charges were made, the Level 2 provider was aware that it did not hold the required robust third party verification of consent to charge for those consumers.

For the reasons set out above the Executive asserted that the Level 2 provider did not have consent to charge complainants. Accordingly, the Executive submitted that the Level 2 provider had acted in breach of rule 2.3.3 of the Code.

2. The Level 2 provider denied the breach. The Level 2 provider noted that the case was opened on 25 May 2015 but the Executive did not contact them until 7 April 2016, which they submitted left them in an impossible position to prove that it held consent to charge as the company Pinchecked went offline prior to this date. The Level 2 provider asserted that the Executive would have been aware of this and contacted it almost immediately. The Level 2 provider submitted that, as it had not heard anything after 25 May 2015, it would naturally be presumed that there were no further questions. The Level 2 provider confirmed that after March 2016, it stopped every promotion and had not had any new subscribers.

3. The Tribunal considered the Code and all the evidence before it, including the consumer complaints.

The Tribunal noted the consumer complaints, which in summary, stated that the consumers had not consented to be charged for the Service. The Tribunal found that there was no reliable evidence that complainants referred to in this case had consented to be charged for the Service by opting in to the Service (prior to the conclusion of the Track 1 procedure, or at all).

The Tribunal noted that the complainants in this case had contacted the Executive in relation to charges which they had started receiving after the conclusion of the Track 1 procedure. The Tribunal found that, at the time the charges were made, the Level 2 provider had been aware that it did not hold the required robust third party verification of consent to charge for the consumers it had charged, but had not made any attempt to obtain robust evidence of their consent before charging them. The Tribunal did not consider that it was a defence to say that the Executive had not specifically included a requirement to unsubscribe existing consumers in the previous Track 1 action plan.

The Tribunal noted that the Level 2 provider had submitted that it would have been able to show evidence for “a high number” of subscribers if PinChecked were still active, and that Veoo held a sample of consents obtained in respect of the Service. The Tribunal commented that, whether this was true or not, it fell short of the requirement to hold robust evidence for all subscribers.

The Tribunal noted the Level 2 provider’s submission that it had understood the Service to be compliant following its responses to the Track 1 procedure and the Executive’s correspondence of 25 May 2015, as the Executive had no further correspondence with it until 7 April 2016. The Tribunal commented that it was the Level 2 provider, and not the Executive, who was responsible for taking pro-active steps in order to comply with the Code.

The Tribunal expressed its concern that it appeared that once the Level 2 provider had established that its Service would not be resumed via mGage due to concerns over consent to charge, the Level 2 provider moved its Service to another Level 1 provider rather than addressing those concerns.

Consequently, for both of the reasons advanced by the Executive, the Tribunal was satisfied that the Level 2 provider had not provided evidence which established consumers’ consent to be charged for the Service, and that consumers had been charged without their consent. Accordingly, the Tribunal upheld a breach of rule 2.3.3 of the Code.

Decision: UPHELD

SANCTIONS

Representations on sanctions

1. The Executive submitted that the following sanctions were appropriate:
 - a formal reprimand;
 - a requirement that the Level 2 provider remedy the breach by ensuring that it has robust verification of each consumer's consent to be charged before making any further charge to the consumer, including for existing subscribers to the Service;
 - a fine of £250,000; and
 - 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 the Phone-paid Services Authority that such refunds have been made.

based on a preliminary assessment of breaches 1 and 2 as "very serious".

2. The Level 2 provider submitted that, if the breaches were upheld, it was nevertheless not appropriate to apply a remedy the breach sanction, as the PinChecked platform (which had previously been recommended by the Executive as a verification service) was no longer available. Regarding the fine sanction, the Level 2 provider noted that this figure had been imposed on other companies in similar cases, but submitted that its complaints and proactivity in addressing any concerns did not merit this type of fine. The Level 2 provider submitted that the Executive's approach, in taking two years to investigate and only asking for information four times, showed this was not a serious case. The Level 2 provider accepted the imposition of a refund sanction was appropriate if the breaches were upheld and commented that it was committed to providing refunds to any unsatisfied consumer.

Initial overall assessment

The Tribunal's initial assessment of the breaches of the Code was as follows:

Paragraph 4.2.4 – Provision of false / misleading information to the Phone-paid Services Authority

The initial assessment of the breach of paragraph 4.2.4 of the Code was **very serious**. In determining the initial assessment for this breach of the Code the Tribunal applied the following criteria:

- The Level 2 provider had deliberately supplied inaccurate, false or misleading information. In coming to this conclusion, the Tribunal noted in particular the Executive's submissions regarding why the Level 2 provider may have chosen to submit the information, and noted the Level 2 provider had failed to provide evidence to satisfactorily answer this allegation;

- The nature of the breach was likely to severely damage consumer confidence in premium rate services; and
- The breach demonstrated fundamental non-compliance with the Code.

Rule 2.3.3 – Consent to Charge

The initial assessment of the breach of rule 2.3.3 of the Code was **very serious**. In determining the initial assessment for this breach of the Code the Tribunal applied the following criteria:

- The Level 2 provider charged consumers without having reliable evidence of consent to charge;
- The case had a clear and highly detrimental impact on consumers;
- Consumers have incurred an unnecessary cost as a result of the breach; and
- The nature of the breach, and/or the scale of harm caused to consumers, was likely to severely damage consumer confidence in premium rate services.

The Tribunal's initial assessment was that, overall, the breaches were very serious.

Final overall assessment

The Tribunal paid regard to the parties' submissions regarding aggravating and mitigating factors.

In determining the final overall assessment for the case, the Tribunal took into account the following aggravating factors:

- The Level 2 provider had previously been subject to a Track 1 procedure, which had included requirements regarding consent to charge; and
- The breaches (including in particular the charging of consumers without consent) continued for at least 7 months after prior notice had been given to industry, in the form of a series of adjudications commencing in January 2016, in respect of similar services and issues. The Level 2 provider, whilst they stated that they had ceased promoting live services in March 2016, had not confirmed when (if at all) they had stopped charging existing subscribers for whom they did not hold evidence of consent.

In determining the final overall assessment for the case, the Tribunal took into account the following mitigating factor:

- There was evidence that the Level 2 provider had adopted a proactive approach to refunding users, including complainants, which was effective in relieving some consumer harm arising from the breach.

However the Tribunal noted that the value of the mitigation accorded to this factor was subject to the following concerns: (a) the list of refunds contradicted the Level 2 provider's other evidence regarding the number of complaints received in respect of the Service after 7 April 2016, and the high number of refunds suggested that the issues with the Service were broader than those which could be perceived from the complaints sent to the PSA; and (b) there was

some concern with the credibility of the evidence submitted (which included a number of refunds for “0”, for instance), which given the late submission of the evidence could not be tested.

The Level 2 provider’s evidenced revenue in relation to the Service in the period from January 2015 to August 2016 was in the range of Band 2 (£500,000 to £999,999).

Having taken into account the circumstances of the case, the Tribunal concluded that the seriousness of the case should be regarded overall as **very serious**.

Sanctions imposed

Having regard to all the circumstances of the case, the Tribunal decided to impose the following sanctions:

- a formal reprimand;
- a fine of £350,000;
- a requirement that the Level 2 provider remedy the breach by ensuring that it has robust verification of each consumer’s consent to be charged before making any further charge to the consumer, including for existing subscribers to the Service; and
- 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.

Regarding the fine, the Tribunal would have imposed a fine of £250,000 in respect of the breach of paragraph 4.2.4 and £150,000 in respect of the breach of rule 2.3.3 had the matters been brought separately. However, having considered the Level 2 provider’s revenue, the degree of overlap in the mischief of the two breaches, and the principle of proportionality, the Tribunal determined that the fine overall should be reduced *pro rata* to £350,000.

Administrative charge recommendation: 100%

The decision of a previous Tribunal on 28 July 2016 to impose interim measures is attached at Appendix B.

Appendix A

“As stated in previous reply to case 40570 we now only operate our business via online banner advertisement. We promote a service where following our online banner advertisement a customer can have access to adult videos for a weekly subscription. Terms and conditions are very important to our services and very well highlighted to any customer before they enter into any weekly subscription based service that we operate this can be seen in screenshot that I have copied in below.



Full customer journey

- Online banner Advertisement set live by venture247.
- Customer looking on browser for glamour / adult content will see our banner.
- Customer will click on our online banner.
- Customer will be directed to our landing page (as above).
- Customer will be asked to read full terms and conditions

- Customer will be asked to enter mobile number.
- Customer will also be asked to tick that they are over 18.
- Customer will then be directed to 2nd landing page.
- Customer will be asked to again read terms and conditions.
- Customer will be asked to agree to our terms and conditions by clicking enter.
(After track 1 and case closure this is now verified by pincheck platform)
- Customer will receive Free join message.
- Customer will receive weekly subscription cost messages.
- Customer will receive Free monthly reminder messages.
- Customer can at anytime cease subscription by texting in STOP or contacting us directly.
- Customer will receive nothing further when subscription cancelled.”

Appendix B



Application for interim measures pursuant to Code of Practice paragraph 4.6

Case ref: 72403
Service: 'Hot-mobilebabes' glamour/adult video subscription service
Level 2 provider: Venture247 Limited
Level 1 provider: Veoo
Cost: £3 per week
Shortcode: 89320, 69988 and 89225
Shortcode to send 'STOP' if different

Tribunal number: 188

Adjudication

- The Tribunal has paid full regard to the material supplied by the Executive. In respect of this material the Tribunal noted in particular:
 - a) the consistency of the complaints, and the admission that prior to the Track 1 procedure the Level 2 provider did not obtain robust consent to charge evidence, and that this was the period in which the Level 2 provider said the complainants had opted into the service; the complainants had nevertheless been charged since the Track 1 procedure;
 - b) regarding the Executive's debt collection assessment, the Tribunal did not consider that the lack of a credit rating, or the fact that only one set of accounts had been filed, constituted relevant risk factors in the context of this case, without further explanation;
 - c) the credit report showed two previous dissolution procedures had been commenced (and suspended) against the company.
- The Tribunal has paid full regard to the representations provided by the relevant party. In respect of this material the Tribunal noted in particular:
 - a) the submissions made regarding the effect on this business of a withhold, although the Tribunal noted that these submissions were not supported by objective analysis of the current financial status of the company and evidence;
 - b) the Level 2 provider's stated intent to cooperate with the Executive. Regarding the submission that this matter had not been raised for a year, the Tribunal noted that it is a Level 2 provider's obligation to comply with the Code of Practice and that duty is on-going. The Level 2 provider was on notice of the requirements on consent to charge due to complaints received, and the previous Track 1 procedure;
 - c) the Level 2 provider's statement that its financial records could be in a far more positive position.

- The Tribunal has paid regard to the Supporting Procedures, including the factors set out at paragraph 80 and 91.

Having considered the evidence before it, the Tribunal has made the following determinations:

- 3) At first appearance (and subject to evidence, arguments or information being later supplied and/or tested), there appears to be sufficient evidence that could support a breach of the Code of Practice rule 2.3.3
- 4) The Tribunal considers that the Level 2 provider will not be able or willing to pay such refunds, administrative charges and/or financial penalties that may be imposed by a Tribunal in due course. The Tribunal notes in particular:
 - a) the Executive's comments in its Debt Collection Withhold Assessment regarding:
 - i) the Level 2 provider's latest balance figures
 - ii) the potential seriousness of the breach, service revenue, and the previous Track 1 procedure in respect of consent to charge, which could result in a higher level of fine; and
 - iii) the history of dissolution actions commenced (albeit suspended).
- 5) The Tribunal is satisfied that PhonepayPlus has made reasonable endeavours to notify the relevant party of its initial findings and the proposed interim measures.
- 6) The Tribunal considers, based on the application before it, that the alleged breach might be more serious than a recent 2.3.3 case in which a fine of £150,000 was imposed (taking into account the potential aggravating and mitigating factors in this case), but a sole alleged breach might make this case less serious than other recent 2.3.3 cases in which fines of £250,000 were imposed. The Tribunal noted that its preliminary views would not bind any subsequent Tribunal. Taking a holistic view of the matter, the Tribunal considers that the measures set out below are appropriate and proportionate to take in the circumstances of this case.
- 7) Accordingly, the Tribunal hereby directs that:
 - a) PhonepayPlus is authorised to direct a withhold of up to £217,000.
 - b) The sums directed to be withheld may be allocated and re-allocated between any Network operators or Level 1 providers for the Service as the Executive sees fit from time to time, provided that the total sum withheld by all providers does not exceed the maximum sum authorised in this decision.
 - c) The Executive is given discretion to vary the total directed to be withheld downwards in the event that it is provided with alternative security which is, in its view, sufficient to ensure that such refunds, administrative charges and/or financial penalties as it estimates a CAT may impose in due course are paid.
 - d) Such interim measures are to be revoked upon the case being re-allocated to Track 1 or otherwise discontinued without sanction.

Mohammed Khamisa QC
28 July 2016

Appendix C

Level 2 provider message log for mobile number *****2979

Message Identifier I.E.Free or Premium	Message	Log Date and Time	Destination MSISDN	Shortcode	Tariff	State
FREE	http://hot-mobilebabes.com/?secret=b4aa223b5	26/09/2014 18:42		89320	£0.00	DELIVERED
FREE	Client opens wap marketing message reads terms and clicks ENTER to subscribe.	26/09/2014 18:45		89320	£0.00	RECEIVED
FREE	FreeMsg: U have subscribed to hot-mobilebabes for £3 per week until you send STOP to 89320 ,Help:01138272094. SP Venture247 18+ New Videos available every week	26/09/2014 18:45		89320	£0.00	DELIVERED

Level 2 provider message log for mobile number *****5133

Message Identifier I.E.Free or Premium	Message	Log Date and Time	Destination MSISDN	Shortcode	Tariff	State
FREE	http://hot-mobilebabes.com/?secret=1864096b4	05/09/2014 16:21		89320	£0.00	DELIVERED
FREE	Client opens wap marketing message reads terms and clicks ENTER to subscribe.	05/09/2014 16:24		89320	£0.00	RECEIVED
FREE	FreeMsg: U have subscribed to hot-mobilebabes for £3 per week until you send STOP to 89320 ,Help:01138272094. SP NSMSM 18+ New Videos available every week	05/09/2014 16:24		89320	£0.00	DELIVERED