Tribunal meeting number 182 / Case 1

Case reference:	**71971**
Level 2 provider:	**Intrugo Limited (UK)**
Type of service:	**'Hot New Babes', 'Unlimited Babes', 'Hot Mobi Babes' and 'Hot New Babe' glamour video subscription service**
Level 1 provider:	**IMImobile Europe Limited (UK); Zamano Solutions Limited (Ireland); Veoo Ltd (UK)**
Network operator:	**All Mobile Network operators**

THIS CASE WAS BROUGHT AGAINST THE LEVEL 2 PROVIDER UNDER PARAGRAPH 4.4 OF THE CODE

BACKGROUND

The case concerned a glamour video subscription service, charged at £3 per week, operating on shared shortcodes 80208, 88222, 80252, 66033, 81300, 88150 and 82999 (the "**Service**").

The Level 2 provider for the Service was Intrugo Limited (the "**Level 2 provider**"). The Level 1 provider for Service shortcode 66033 was Zamano Solutions Limited. The Level 1 provider for Service shortcodes 81300, 82999 and 88150 was Veoo Ltd ("**Veoo**"). The Level 1 provider for Service shortcodes 88222, 80208 and 80252 was IMImobile Europe Limited **("IMImobile")** (and subsequently Wireless Information Network Ltd).

Between 19 March 2015 and 20 January 2016, the Executive received 329 complaints concerning the Service. Complainants variously alleged that the Service charges were unsolicited.

The Service

The Service was stated to be a glamour video subscription service charged at £3 per week. The Level 2 provider confirmed that the Service commenced operation in April 2013 and was currently operational. IMImobile stated that the Service commenced operation in February 2009. Zamano confirmed that the Service commenced operation on shortcode 66033 in August 2013. Veoo confirmed that the Service commenced operation on shortcode 81500 in April 2013, on shortcode 82999 in January 2015 and shortcode 81300 in May 2015.

In relation to shortcode 66033, the Executive noted from message logs supplied by the Level 2 provider that users of the Service opted in on this shortcode, and that some Service users were then migrated to either Service shortcode 88150, or Service shortcode 82999.

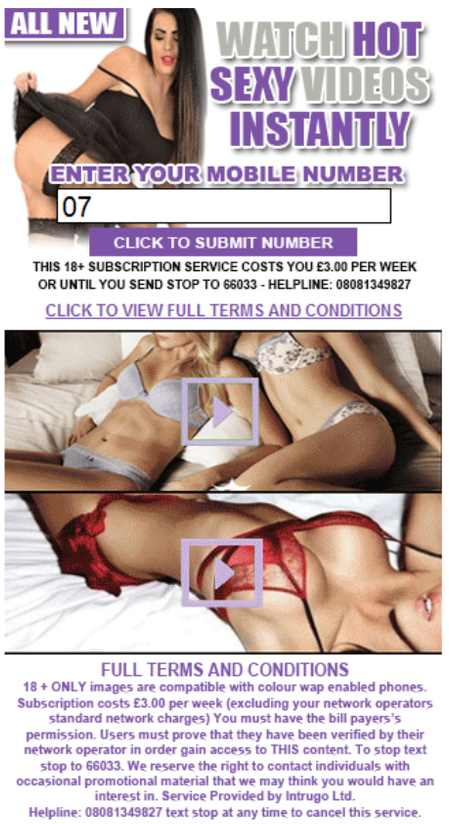
The Level 2 provider supplied the following summary of the promotion and operation of the Service:

- "MARKETING DEVICE – ONLINE BANNER

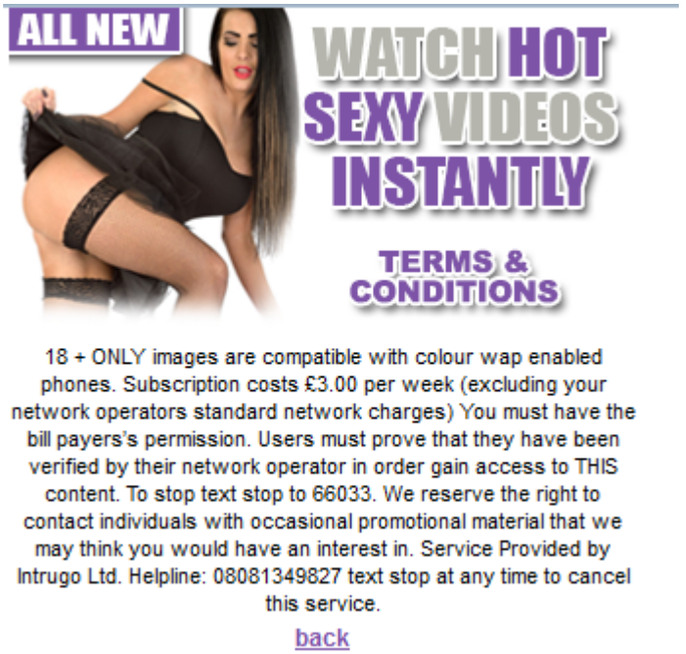
[Screen Shot One]

- MOBILE NUMBER VERIFICATION DEVICE – ONLINE FORM INTEGRATED WITH GOVEFIRY *[sic]* SYSTEM. BELOW PAGE IS RENDERED VIA SECURE PROTOCOL AND TIME STAMPED.

[Screen Shot Two]



[Screen Shot Three]



- SECOND STEP OF OPT IN FLOW – PIN VERIFICATION. 4 DIGIT PIN IS GENERATED BY GOVERIFY AND INSTANTLY DELIVERED TO HANDSET. BELOW PAGE IS ALSO RENDERED AND TIME STAMPED BY GOVERIFY

[Screen Shot Four]

- OPT IN PROCESS COMPLETES WHEN MOBILE NUMBER AND PIN ARE RECEIPTED, VERIFIED AND ACCEPTED BY CROSS CHECK GOVERIFY TOOL. EVIDENCE, I.E. CONTRACT BETWEEN INTRUGO AND GOVERIFY METHOD PROVIDER IS AVAILABLE ON REQUEST.

- SERVICE MESSAGE IS SENT BY INTRUGO TO CONFIRM SUBSCRIPTION START:

FreeMsg: You subscribed to Hot Mobi Babes for £3 per week until you text STOP To 66033 to opt out. Helpline: 08081349827 SP: Intrugo Ltd

- PREMIUM MESSAGE IS SENT BY INTRUGO – IT INCLUDES UNIQUE WAP LINK WITH PREMIUM MOBILE CONTENT, OPT OUT AND HELP GUIDE
- SERVICE MESSAGE IS SENT BY INTRUGO TO REMIND ABOUT ONGOING PREMIUM SUBSCRIPTION:

FreeMsg: You are subscribed to Hot Mobi Babes unlimited sexy videos for £3.00 Per week. Helpline: 08081349827 SP: Intrugo Ltd text STOP To 66033 to stop

- AVAILABLE OPT OUT METHODS – TEXT STOP OR STOP ALL TO 66033. OPTIONAL – CUSTOMER CARE TEAM ON 08081349827.
- SERVICE MESSAGE IS SENT BY INTRUGO UPON RECEIPT OF STOP REQUEST"

Summary of complaints

The Executive received 329 complaints concerning the Service in the period from 19 March 2015 to 20 January 2016. Complainants variously alleged that the Service charges were unsolicited. A sample of complainant accounts is provided below:

> "Hi I suddenly started getting unsolicited messages from New Sexybabe videos uploaded. I did not subscribe and it asks me to text 80252 to get out of it. I daren't text as I think it will make it worse!
>
> I did not subscribe to this service, I do not want adult videos. I don't know the website"

> "This company have been sending me Texts which I put a block on. I have never opened any of their texts nor responded to them in any way. Today I discovered that I have been charged £100 over the last 12 months for such texts. I use GiffGaff which isn't on your list. I have never had any communication from this company other than the SMS messages. I have never agreed to subscribe to anything by this company. I do not know where they got my number I need this to stop and to be refunded for the theft"

> "Not sure what service the above number is but it seems to text me and charge me and subscribe me when i did not subscribe to their services
>
> Did not subscribe or get any pop up just got message which i deleted and entered as spam on my phone but got charged for it, need full refund or sue company."

> "I have never request texts or subscription to this number or service at any time! The nature of the messages are as follows: FreeMsg: UR subscribe to Hot Mobi Babes unlimited sexy videos for £3.00 Per week. Helpline: 08081349827 SP: Intrugo Ltd text STOP To 66033 to stop I think I am being charged. I want the messages to stop and a refund of charges from this company."

> "I have been billed £3 weekly by 66033. I have never agreed to the charges. I have not received anything for the charges other than unwanted text messages. I have been charged £18 to date. I have no idea how they have subscribed me to their service without my permission. I have contacted them to stop the charges but they have failed to do so."

Complainant text message logs

As part of the standard request for information process, the Level 2 provider supplied text message logs for 312 out of the 329 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.

The Executive noted that 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. An example log can be seen at **Appendix A.**

Complainant responses to Executive questionnaire

In light of the high number of failed messages identified by the Executive in the complainants' text message logs provided by the Level 2 provider, which the Executive had noted were not generally shown in logs provided by the Level 1 provider, and the possible explanations offered by the parties in the value chain for the failed messages, on 19 November 2015 the Executive contacted 270 complainants (the total number of complaints received by PhonepayPlus about the Service as at that date) with the following series of questions:

> "Is the mobile phone that received the chargeable text messages on contract or pay-as-you-go?
>
> If the mobile phone that was charged is pay-as-you-go, please advise whether you regularly / always had more than £3 credit on your mobile phone?
>
> Please advise whether the mobile phone that received the chargeable messages was regularly switched off and/or had no mobile signal for long periods of time (i.e. for more than several days)?
>
> Please advise whether you transferred your mobile number between mobile telephone companies in the six months before your received the chargeable text messages? If yes, please confirm if you experienced long periods with no signal and/or difficulty in sending and receiving text messages."

In addition the complainants were sent a copy of Screen Shots One to Three (as shown as above) and asked whether they recalled viewing and/or interacting with it or a similar service promotion.

As at 19 February 2016, the Executive had received responses to the questionnaire from 69 complainants. Below is a breakdown of the complainant responses:

Question	*Response*	*Comments*
Is the mobile phone that received the chargeable text messages on contract or pay-as-you-go?	64 respondents confirmed they were on contract 2 respondents confirmed they were on Pay as You Go	3 consumers did not answer the question
If the mobile phone that was charged is pay-as-you-go, please advise whether you regularly / always had more than £3 credit on your mobile phone?	64 respondents stated that this question did not apply to them (contract plans) 2 respondents confirmed that they always had more than £3 credit on their phone	3 consumers did not answer the question
Please advise whether the mobile phone that received the chargeable messages was regularly switched off and/or had no mobile signal for long periods of time (i.e. for more than several days)?	61 respondents advised their mobile phone was not regularly switched off and/or had no mobile phone signal	2 respondents stated that they left their phones on all the time except for overnight 1 respondent stated that the phone was left on Monday to Friday/off evenings and weekends 1 respondent highlighted having signal issues, but stated that the phone did manage to send/receive messages eventually (within hours) 1 respondent stated that the phone was switched off during the day 3 consumers did not answer the question
Please advise whether you transferred your mobile number between mobile telephone companies in the six months before you received the chargeable text messages? If yes, please confirm if you experienced long periods with no signal and/or difficulty in sending and receiving text messages	62 respondents advised they had not transferred between mobile companies 1 respondent advised that they had transferred their plan to another provider in the last 12 months	1 respondent transferred their number over 12 months ago 1 respondent transferred in January 2015 4 did not answer the question

Please advise if you recall viewing and interacting with the attached, or a similar, promotion?	62 respondents advised that they did not view / interact with the Service promotion	2 respondents stated they saw the promotional material after receiving a text message 5 did not answer the question

Previous complaint resolution procedure

The Level 2 provider has had a prior informal dealing with PhonepayPlus. On 10 December 2014, 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 12 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 the Track 1 procedure was finalised.

The investigation

The Executive conducted this matter as a Track 2 investigation in accordance with paragraph 4.4 of the PhonepayPlus Code of Practice (13th Edition).

The Executive sent a breach letter to the Level 2 provider on 19 February 2016. Within the breach letter the Executive raised the following breaches of the PhonepayPlus Code of Practice (the "**Code**"):

- Paragraph 4.2.4 – Provision of false information to PhonepayPlus
- Rule 2.3.3 – Consent to charge

The Level 2 provider responded on 14 March 2016. On 31 March 2016, the Tribunal, having heard informal representations made on behalf of the Level 2 provider, 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 the Level 1 providers;
- Correspondence between the Executive and the Verifier;
- Correspondence between the Executive and a third party verifier;

- Complainant message logs from the Level 2 provider;
- The breach letter of 19 February 2016 and the Level 2 provider's response of 14 March 2016 including annexes;
- Correspondence between the Level 2 provider and Executive dated 18 March 2016 including annexes;
- Correspondence from the Level 2 provider and their representative to the Executive dated 29 March 2016, including attachments;
- Correspondence from the Executive to the Level 2 provider dated 29 March 2016 and 30 March 2016, including attachments; and
- A document referring to a list of ten MSISDNs supplied by the Level 2 provider.

PRELIMINARY ISSUE

The Level 2 provider made an oral application to the Tribunal for permission to rely on the material it had served on the Executive on 29 March 2016.

Upon questioning from the Tribunal as to why the material was not served with the response to the breach letter, the Level 2 provider stated that the issues had only recently been discovered over the course of the last week when the information was re-read. The Tribunal noted that the information had been available since the breach letter had been served. The Level 2 provider acknowledged this but, since its view was that the material had a major impact on the case, it was of the view that it was important to submit it even at this late stage.

Upon questioning from the Tribunal, the Executive confirmed it did not object to the late submission of this further material in this case, provided that it was permitted to submit its own material in response to the Level 2 providers' material.

The Tribunal found that the evidence was relevant and in principle could be admissible. Although the Tribunal found that the material had been served late and should properly have been served with the response to the breach letter, in the circumstances of this case, and in light of the Executive not raising any objection, the Tribunal considered that it was in the interests of justice for it to exercise its discretion to admit the material. The Tribunal therefore permitted the Level 2 provider to rely on the material.

In light of the Level 2 provider's application, the Executive made an application to rely on further material which it had obtained since the breach letter had been served. The Executive confirmed that this material had been served on the Level 2 provider prior to the date of the hearing. The Executive submitted that this material was relevant to matters now before the Tribunal, including matters raised by the further material which the Level 2 provider had been permitted to rely upon.

Upon questioning from the Tribunal, the Level 2 provider confirmed it did not object to the submission of this further material.

The Tribunal found that the evidence was relevant and in principle could be admissible. In the circumstances of this case, and noting that the Level 2 provider had not raised any objection, the

Tribunal considered that it was in the interests of justice for it to exercise its discretion to admit the material. The Tribunal therefore permitted the Executive to rely on the material.

SUBMISSIONS AND CONCLUSIONS

ALLEGED BREACH 1

Paragraph 4.2.4 – Provision of false information to PhonepayPlus

"A party must not knowingly or recklessly conceal or falsify information, or provide false or misleading information to PhonepayPlus (either by inclusion or omission)."

1. The Executive asserted that the Level 2 provider had breached paragraph 4.2.4 of the Code because message logs supplied by the Level 2 provider were false or misleading. 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, the Level 1 providers, complainant accounts (which are referenced in the 'Background' section above), complainant questionnaire responses and text message logs.

   The Executive noted that the complaints received by PhonepayPlus following the Track 1 procedure spanned the period between March 2015 and January 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 unbilled 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 ********931

   The Executive noted that the provided log showed that the initial opt-in to the Service occurred on 16 August 2014. The subscription confirmation message stated:

   "FreeMsg U have joined hot-mobi-babes Vids and pics club for £3 per week until you send STOP to 66033 Help? 08081349827"

   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', 'BILLED' or 'SENT'. The Level 2 provider however clarified that messages listed as 'SENT' were pending, as a positive

message delivery receipt had not been received from its aggregator, meaning that the messages had not been received by consumers.

The Executive noted that following the above entry in the message log, the status of all chargeable Service messages on shortcode 66033 was listed as either 'FAILED' or 'SENT'. The first Service message listed as 'BILLED' on shortcode 82999 was delivered on 15 March 2015, more than seven months after the purported opt-in date.

Level 2 provider message log for mobile number *********670

The Executive noted that the provided log showed that initial opt-in to the Service occurred on 2 August 2014. The subscription confirmation message stated:

"FreeMsg U have joined hot-mobi-babes Vids and pics club for £3 per week until you send STOP to 66033 Help? 08081349827"

The Executive noted that following the above entry in the message log, the status of all chargeable Service messages on shortcode 66033 was listed as either 'FAILED' or 'SENT'. The first message listed as 'BILLED' was on shortcode 82999 (after the Service had migrated to Veoo) and was delivered on 15 March 2015, almost seven months after the purported opt-in date.

Level 2 provider message log for mobile number ********029

The Executive noted that the provided log showed that initial opt-in to the Service occurred on 15 August 2014. The subscription confirmation message stated:

"FreeMsg U have joined hot-mobi-babes Vids and pics club for £3 per week until you send STOP to 66033 Help? 08081349827

The Executive noted that following the above entry in the message log, the status of all chargeable Service messages on shortcode 66033 was listed as either 'FAILED' or 'SENT'. The first message listed as 'BILLED' was on shortcode 80252 (after the Service had migrated to IMIMobile) and was delivered on 24 January 2015, almost six months after the purported opt-in date.

The Executive also produced 15 further examples of message logs supplied by the Level 2 provider which contained 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.

The Executive had contacted the Level 1 providers for a sample of complainant message logs. The Executive noted that although the logs provided by the Level 2 provider revealed a purported opt-in on Service shortcodes followed by a series of failed messages, the messages logs received from the Level 1 providers did not mirror those supplied by the Level 2 provider.

The Executive noted that, of the 15 messages logs provided by IMImobile, only one log showed an opt-in date matching that provided in the Level 2 provider's log, which in that case was prior to August 2014.

The Executive noted that, of the 34 message logs requested from Zamano, only 25 message logs were received showing there had been interaction with the Service. In relation to the remaining nine message logs, Zamano confirmed that the MSISDNs did not appear on its system. The Executive noted that none of the logs provided by Zamano showed an opt-in matching that shown in the Level 2 provider's log.

The Executive noted that the logs supplied by Veoo confirmed that the first chargeable Service message on the Level 2 provider logs generally occurred after the Service had migrated to Veoo.

In order to obtain further clarification on the message failure issue, the Executive had 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 41 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 that, from the 41 message logs supplied by the Verifier, 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, and that no failed messages were shown in the period after the purported opt-in. For example the Verifier log for ********931 listed the first Service message on 15 March 2015, and the Verifier log for ********670 listed the first Service charge on 15 March 2015.

The Executive submitted that the Verifier had previously confirmed that all messages sent from the Service shortcode that charge or attempt to charge the consumer would appear in its text message logs. Similarly, IMImobile had confirmed that all chargeable messages (attempted and successful) would appear in its text message logs. In light of this, the Executive asserted that the failed attempts to send the chargeable Service messages (which included the messages recorded as "sent") (as shown on the Level 2 provider's message logs) did not occur.
Furthermore, the Executive directed the Level 2 provider to provide an explanation for the high failure rate of chargeable Service messages. On 3 December 2015 the following response was received from the Level 2 provider:

"This matter also raised our concerns and our conclusion is that although Intrugo would send out premium messages on correct pattern to enlisted subscribers, reverse premium SMS might have not reach their destination, i.e. subscriber handsets. This was judged upon delivery rate ratio.

The reasons for failed status may vary between - insufficient airtime credit, network outages, power blackouts, server downtimes, network carrier blockages and users being blocked at Level 1 end as a result of previous opt out requests as it happens commonly in the case of premium/ shared short codes. Level 2 Provider's role in this communication chain is to initiate the premium message however the rest of chain links are in hands of Level 1 Providers and Network Carriers.

In order to correctly perceive above last note, we gathered a factual sheet presenting just a small cut of a major UK Network Outage Map. Report lists example network downtime logs submitted by genuine users from all across UK territory. It took 4 pages of small print for November 2015 alone, and it related only to users who were privileged to have alternative online access and who were frustrated enough to submit online complaint. We wish to present the Report to Executive to assist in understanding how common it is for mobile user to be outside of network coverage without ability to receive text messages, make calls or access internet for extended amount of time. Attached Summary presenting just sample outage map is only a micro-piece of the puzzle as network issues are in fact a permanent aspect of our everyday routine, our lives and surrounding reality."

The Executive also made enquiries to IMImobile and Zamano regarding the high failure rate of chargeable Service messages. Although Veoo provided a response, most of the failed messages occurred on the IMImobile and Zamano shortcodes, and therefore it was not able to provide a comprehensive response on the issue. Responses from IMImobile and Zamano are located below.

IMImobile response

"There are a number of reasons that the messages may be routinely failing such as:

- *Insufficient Credit;*
- *Failure at Network Level;*
- *Subscriber blocked from Network or Level 1 provider level.*
- *Message expired at Operator.*
- *Messages that have failed because they have been sent to the incorrect mobile network for that MSISDN ('Unknown Subscriber').*

Intrugo Limited would have received the Delivery Receipts for the messages that were failing. These receipts specify the reasons.

Our Technical Support Group team have looked in detail at the Intrugo Limited's traffic that went across the IMImobile platform [a graph showing messages statuses based on the Level 2 provider's days when over 1000 PSMS MT were sent was provided]"

The Executive put forward the Level 2 provider's reasons for message failures to IMImobile and Zamano and asked the Level 1 providers to confirm if failed messages would appear on the message logs that they provided. IMImobile confirmed that:

"If the messages were initiated by the Level 2 provider and did fail before hitting our platform then they would not show on our message logs.

If the messages were successfully delivered to our platform for processing and then failed due to one of the many reasons that we and the Level 2 provider have given, then the answer is yes they would appear on our call logs with the failure reason.

I have highlighted within the email below the reasons (within the L2s response) that we would expect to see trigger on our logs [insufficient airtime credit, network outages, network carrier blockages and users being blocked at Level 1]. The other two:

- *Power blackouts – I am not sure what the L2 is referring to here.*

- *Server downtimes – If it was a server issue at the L2 level, that could cause it to not hit our platform. Other than that, any other failures at L1 or MNO level, we would expect to see."*

Zamano provided the following response:

"Should a message be sent by Level 2 Provider… it is technically reasonable to register it on Level 2 system, whereas at the same time it might not be present on the Zamano log. Correspondingly, when a message is transmitted by Intrugo and does not encounter any technical flaw on its way, it is clear that such message would show on Zamano's log. In the event of the following issues, technical interference, connectivity outage, error in Level 2 internal specification, these text messages would not reach Zamano gateway, as a result there will be no positive delivery receipts. As a consequence of this such messages would routinely fail."

In its breach letter dated 19 February 2016, the Executive had noted that the Level 2 provider had not stated that there was a technical fault that caused chargeable service messages to fail before arriving on the Level 1 providers' platforms, nor provided any evidence of such a fault. Moreover the Executive noted that the Level 2 provider's logs for the complainants showed message failures occurring over lengthy periods.
In response to questioning by the Tribunal following the Level 2 provider's submission of evidence regarding a technical fault, the Executive submitted as follows. Firstly, the Executive doubted the credibility of the evidence since it had not been submitted as the explanation for why messages appeared to be consistently failing when the Executive had asked this question on 18 November 2015. Secondly, referring to the dates when the Host had reported hacks to the Level 2 provider, the Executive noted that four of these incidents pre-dated the primary opt-in period, and so would not explain the discrepancies. The last hack in November 2014 did not explain the vast majority of message failures, given when it was remedied. The Executive accepted that the hacks may have occurred but submitted that they did not explain the pattern of consistent message failure shown, and did not explain failures after November 2014 (the date of the last reported hack) at all. The

Executive also referred to two instances of pairs of logs (********670 and ********485, and ********567 and ********378) which showed successful messages sent to one consumer's MSISDN shortly after failed messages to another MSISDN.

In response to questioning by the Tribunal following the Level 2 provider's submissions about the Verifier's evidence, the Executive stated that the Verifier was a third party who works with Vodafone and provides analytics. The Verifier had direct access to the platform. The Executive submitted that there was no reason for them to provide inaccurate evidence. The Executive submitted that the Level 2 provider's claim that the Verifier log was inaccurate was not well founded, and referred to evidence it had supplied in response to this submission which showed that one consumer MSISDN had in fact been charged by two different providers' services on the same shared shortcode, rather than showing double charging by the Service. In relation to the Verifier's evidence that failed messages would appear on its logs, the Executive accepted that this evidence had first been gathered in relation to an investigation into another service. The Executive accepted that the evidence was not specific to the Level 2 provider but submitted that the response which had been provided was a generic description of how the Verifier's systems operated. In any event, the Executive had produced further evidence in response to the Level 2 provider's submission which confirmed, specifically in relation to the Service shortcodes, that if attempts had been made to bill by the Service which had failed, the failed messages would appear on the Verifier logs.

In response to questioning by the Tribunal following the Level 2 provider's submission regarding shortcodes being inaccurately described as "dedicated" in the breach letter, the Executive admitted this was an error, which it had corrected prior to the Tribunal.

For the reasons stated above, the Executive submitted that the possible explanations for the failed messages provided by the Level 2 provider did not explain the discrepancies between the logs for the complainants.

Further, the Executive referred to the complainant accounts, and the complainant responses to the Executive's questionnaire (referenced in the 'Background' section above). The Executive submitted that it was highly unlikely that the complainant accounts, and those complainants who responded to the complainant questionnaire stating that they never interacted with the Service website, were unfounded.

The Executive noted from the previous Track 1 procedure that the Level 2 provider had asserted that it did not have robust verification prior to 12 January 2015. The Track 1 procedure was created in part to address an issue with 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 IMImobile, Zamano and the Verifier, the Executive considered that the message logs supplied by the Level 2 provider were incorrect, and the Executive had been provided with false information. Accordingly, the Executive submitted that the Level 2 provider had acted in breach of paragraph 4.2.4 of the Code.

2. The Level 2 provider denied the alleged breach. The Level 2 provider submitted that the case was not based on material evidence.

Firstly, the Level 2 provider submitted that it had actually sent all chargeable messages that were marked as 'failed', 'sent' or 'accepted'. The Level 2 provider submitted that these messages had however failed to reach the Level 1 provider, network and subsequently users' handset due to technical obstacles resulting from dedicated server abuse incidents.

The Level 2 provider noted that IMImobile had clearly confirmed that Level 2 provider server issues could cause messages to not hit the Level 1 provider technical platform, and that Zamano had clearly confirmed that technical flaws may cause messages to not show on Level 1 provider logs. The Level 2 provider submitted that this was material undermining the Executive's allegations and proved its statements.

The Level 2 provider stated that the server abuse issue had been reported to it by its hosting company **("the Host").** The Level 2 provider stated that it had continuously cooperated with the Host to solve the matter completely. The Level 2 provider stated that this technical obstacle resulted in blocking of certain ports (transmitters) which prevented particular messages being delivered to the Level 1 provider system. The Level 2 provider stated that it had implemented precautions to remedy the issue and the activity for these technical ports was restored gradually upon system scanning and maintenance. The Level 2 provider submitted that there had been no case of altering call logs on any part of message strings and stated that it considered this allegation was not based on any facts or evidence.

The Level 2 provider supplied evidence that such issues had been reported on 3 March 2014, 1 April 2014, 8 May 2014, 30 June 2014 and 17 November 2014, including extracts from correspondence with the Host. The evidence included details of whether in each case a port was blocked as a result of the incident, and when (save for in respect of the 1 April 2014 issue) each such incident was resolved (being 4 March 2014, 13 May 2014, 30 June 2014, and 17 November 2014 respectively).

During informal representations, the Level 2 provider supplied further explanation of this issue. The Level 2 provider referred to the correspondence between it and the Host which it had supplied (noting that the date of this correspondence had been incorrectly recorded as 2015, instead of 2014). The Level 2 provider explained that on 3 March 2014 it was notified that its server had tried to hack other services, and that its servers had been compromised.

It was reported to them that the Host had found some suspicious traffic, and had asked them to investigate. The Head of IT investigated and discovered some scripts on its servers which allowed scams / hacking of other services. The hack allowed other parties to remotely control the Level 2 provider's server and perform scamming attacks to other services and disrupt their traffic. The Level 2 provider stated that it had passed this information to both the Level 1 providers and they had confirmed that this would result in the Level 1 provider reporting the message status as "failed" at their end. The Level 2 provider asserted that this correspondence had been submitted as part of its original response.

The Level 2 provider had looked to see if this attack was targetted at their own messaging system but had concluded that it was instead some "script kiddies" looking to use their server to launch attacks in the future (such as a distributed denial of service attack) on other services of other organisations. However the attack had still caused the Level 2 provider's process to "die" because they had run out of RAM as a result of the hack. The Level 2 provider explained that it was on a 100MB connection and if the third parties used the server for an attack, this occupied their whole network card. The Level 2 provider explained that, when their server was being used for such an attack, this would affect all their traffic (noting that it only used one server for messaging, and only used HTP Port 80) for the time period of the attack. The Level 2 provider did not have monitoring tools from the Host which would be needed to specify when the card reached capacity, and did not normally monitor this. Some of their outbound traffic would reach its destination, but when the network connection reached its limit, messages would stop being sent.

The Level 2 provider was asked if the messages would simply be delayed rather than fail. The Level 2 provider stated that there was no retry option on the messages being sent to the Level 1 provider.

The Level 2 provider stated that it did not know when the attacks were occurring – they would be of short duration and intermittent. It did not prevent them receiving the emails from the Host. It was not aware at the time that this was affecting their outbound traffic. It only found out about the hacks when notified by its Host. When notified, the Head of IT had looked for the hidden files on its system. The Level 2 provider confirmed that the list of hacks it had supplied were all the hacks it was aware of.

The Level 2 provider stated that in one incident (somewhere between April and November 2014) it had asked the Host to whitelist the IP address of their backup server so it could send messages. The evidence of this had been lost as it was on a colleague's PC which had since been formatted.

The Tribunal noted that complainant MSISDNs showed consistent message failure over a period of several months and queried how the "hacks" would cause consistent message failure in this way. The Level 2 provider stated that it did not know if it was re-hacked throughout this period – it only knew about the "hacks" which the Host had highlighted to it. The Level 2 provider stated that if the security flaw through which the hack was occurring

was not identified, then it could keep happening. The Level 2 provider stated that the "hacks" were as a result of a bug which kept coming back onto their server, but Ubuntu fixed this in November 2014.

The Tribunal noted that complainant MSISDNs showed consistent message failure after November 2014 and queried how the hacks would cause consistent message failure in this way. The Level 2 provider's Head of IT was not aware that there had been message failures after 2014 and stated that the hacks did not explain these failures, as their servers were clean by that time. The Level 2 provider stated these failures could be for different reasons.

Secondly, the Level 2 provider submitted that use of the Consumer Questionnaire as evidence was outside of the expected standards that Industry would expect from the Investigations Team.

The Level 2 provider submitted that the methodology for the questionnaire was faulty. The Level 2 provider submitted that mail surveys suffered from very low response rates, and were exposed to response bias. The Level 2 provider submitted that the minimum sample size should have been 149 respondents, not 69. The Level 2 provider stated that the most important aspect that influences internet questionnaires was an unwillingness to provide honest answers (social desirability bias). The Level 2 provider stated that an obvious example would be any question concerning a person's relationship with the law, and that this social desirability bias was further intensified if the organisation conducting the survey was a government body or authority in the community. The Level 2 provider submitted that other normal instances of social desirability stemmed from conforming to social norms, including sexual behaviour.

The Level 2 provider submitted that to collect the most accurate data from respondents, the questionnaire must be unbiased, otherwise unanticipated communication barriers between the investigator and respondents would yield inaccurate results. The Level 2 provider submitted that bias may arise from the way individual questions were designed, the way the questionnaire as a whole was designed (for instance, the use of vague or complex wording, and the need to include a preliminary screening question), and how the questionnaire was administered or completed.

The Level 2 provider supplied a critical analysis of each of the questionnaire questions, which further highlighted its criticisms of the design of the survey and the quality of the responses, and suggested further questions which could have been asked.

The Level 2 provider challenged its validity and suggested it should be evaluated by professional academic consultants. The Level 2 provider submitted that it was in breach of the 'Privacy' rule specified in the Code. The Level 2 provider submitted that the questionnaire was not credible, professional or factual, and requested a statement that it was composed and interpreted without knowledge of how to conduct an email survey.

Thirdly, the Level 2 provider submitted that the Executive's investigation material did not meet the standards of material evidence and was itself in breach of para. 4.2.4 of the Code. The Level 2 provider referred to the fact that the Executive had in the original breach letter stated that some of the Service shortcodes were dedicated, when they were in fact shared. The Level 2 provider submitted that the Executive did not give due care and attention to its response provided in June 2015 (in which it had confirmed the nature of its Service shortcodes) when compiling the breach letter. The Level 2 provider submitted that this was contrary to PhonepayPlus' statement that they were "*effective and accountable. We project manage our work effectively to deliver results."* The Level 2 provider submitted that as a result of this, on a balance of probabilities, the rest of material enclosed in the breach letter was also incorrect or untrustworthy.

In informal representations, the Level 2 provider referred to the evidence supplied by the Executive which the Executive had stated supported the assertion that failed messages would appear on the Verifier's logs. The Level 2 provider supplied evidence that the same response from the Verifier had been used in two other cases brought by the Executive. The Level 2 provider noted that the response featured some redactions. The Level 2 provider stated that it was puzzled as to why the Executive had submitted evidence which didn't relate to the Service shortcode and duplicated evidence from other cases, and queried why the evidence had been redacted. The Level 2 provider submitted that this response should therefore not be admitted as evidence. The Level 2 provider submitted that this called into question the credibility of the Verifier evidence. The Level 2 provider also submitted that the Verifier evidence was faulty because one log appeared to show double charging, whereas it had obtained confirmation from its Level 1 provider that there had been no double charging of that MSISDN.

The Level 2 provider also referred to ten examples of complainants in respect of whom it had taken the Executive six to eight weeks to request logs from the Level 2 provider after the complaint was first made. The Level 2 provider submitted that if there was consumer harm, this had been exacerbated by the Executive's delay.
The Level 2 provider submitted that the Executive's evidence was weak, inaccurate and wrong.

Finally, the Level 2 provider disputed that it 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 is confined to a lack of independent third party verification."* The Level 2 provider submitted that if it was found to have breached the Code, it had not done so deliberately. The Level 2 provider stated that it had strictly adhered to the Track 1 remedy plan and implemented full online verification for online services, which could be verified with the GoVerifyIt system providers. The Level 2 provider asserted that verification of this information was apparently never even attempted with GoVerifyIt.

The Level 2 provider asserted that all evidence certified that no breach of the Code occurred.

3. The Tribunal considered the Code, the submissions made before and during informal representations and all the evidence before it. The Tribunal first considered the points raised by the Level 2 provider in relation to the quality of the Executive's evidence.

The Tribunal considered the Level 2 provider's submission that none of the Executive's evidence was reliable because they had made an error when describing whether the Service shortcodes were shared or dedicated. The Tribunal found that upon this error being made known to the Executive, the Executive had corrected their position. The Tribunal did not consider that such an error of this type was capable of rendering the entirety of the evidence as unreliable or undermining any of the Executive's other evidence, and rejected this submission.

The Tribunal considered the Level 2 provider's submission that none of the Verifier evidence was reliable because a Verifier log appeared to show double charging, despite a Level 1 provider confirming that no double charging had occurred. The Tribunal considered the Executive's explanation that the apparent double charging was caused by billing for a third party's service on the shared shortcode, and accepted that the evidence supported this explanation. The Tribunal therefore rejected this submission.

The Tribunal considered the email dated 16 July 2015 provided by the Verifier which had in part been redacted and which had been received in the course of the Executive's investigation into another provider, a fact which the Level 2 provider alleged had been concealed by the redaction. The Tribunal considered it would have assisted if the Executive had explained the circumstances in which the email had been received and the reason for the redactions to the Level 2 provider at the outset. However the Level 2 provider was entitled to challenge and question the redaction, which it had done. The Executive had in response obtained further evidence from the Verifier in an email dated 29 March 2016 which confirmed that if billing messages from the Level 2 provider had failed, then they would still appear on the Verifier's logs. Accordingly it was unnecessary for the Tribunal to place any weight on the redacted original email and the reasons for the redaction, in light of the more recent specific evidence on this issue which was both relevant and admissible.

The Tribunal considered the Level 2 provider's submissions regarding the Consumer Questionnaire evidence. The Tribunal considered that there was some force in some of the arguments submitted by the Level 2 provider about the Consumer Questionnaire, which could reduce the weight which the Tribunal would give to the evidence. However, in light of the evidence from the Level 1 providers that if billing messages from the Level 2 provider had failed between the Level 1 provider and the consumer for the possible reasons given by the Level 2 provider, then they would still appear on the Level 1 provider's logs, it was unnecessary for the Tribunal to place any weight on the Consumer Questionnaire evidence in any event.

Having considered the Executive's evidence, including in particular the nature of the complaints, the discrepancies between the Level 2 provider's logs and the Level 1 provider and Verifier logs, and the relevant correspondence (including statements from the Level 1

providers about what types of failed messages would appear in their logs), the Tribunal found that the there was a compelling body of cogent evidence to show, on a balance of probabilities, that the Level 2 provider had produced inaccurate message logs which it had submitted to the Executive. Further, the Tribunal considered that the Level 2 provider knew that the existence of the entries shown in their logs (and not the Level 1 provider or Verifier logs) was in their interest. Any doubt that there may have been about the cause or reason for errors in the logs, such as the technical interference by "hacking" into the Level 2 provider's server, was removed by the absence of any evidence of such interference after November 2014 and the Level 2 provider's admission that the effect of any hacking had been resolved in November 2014. There was no evidence before the Tribunal that there was or could have been any "hacking" of the server post November 2014.

The Tribunal then considered whether the material submitted by the Level 2 provider explained the discrepancies between the logs produced by the Level 1 providers and the Level 2 provider, and undermined the case which had been advanced by the Executive.

The Tribunal gave consideration to the potential technical reason for message failure which had been put forward by the Level 2 provider. The Tribunal considered that the pattern of consistent message failure for specific consumers was not credibly explained by a possibility of server abuse on an intermittent basis for short periods. Moreover the Tribunal noted that, since the Level 2 provider's evidence was that the server abuse issue had been resolved in November 2014, this did not explain why the pattern of consistent message failure for specific consumers continued after November 2014, for six months in some cases. The Tribunal considered that the Level 2 provider had been given ample opportunity to provide sufficient evidence to substantiate its submission that the discrepancies were due to a technical reason, but it had not done so. In the course of the informal representations, the Level 2 provider's Head of IT was specifically asked by the Tribunal to comment on the period post November 2014 and invited to make submissions on whether there were any further reported incidents of "hacking" which the Level 2 provider had been alerted to by internal messaging or external third parties (such as the Host) but the answer given was there were none. Further, there was no documentary material of the kind which was relied on for the period before November 2014, such as correspondence with the Host. Absent this kind of evidence and a coherent explanation from the Level 2 provider, the inevitable conclusion the Tribunal was drawn to was that there was in fact no answer to the Executive's case on this point.

Whilst the Tribunal recognised that the complainants represented only a small percentage of the Level 2 provider's customer base, the Tribunal would expect a provider to have identified a pattern of consistent message failure for specific consumers rather than allowing it to carry on for a lengthy period. The Tribunal understood that the successful delivery of chargeable messages was fundamental to the Level 2 provider's business model and to the successful operation of its systems, and it appeared implausible to the Tribunal that the Level 2 provider would not have sought to robustly investigate the extent of any such problem once it had become aware of it or any technical or 'hacking' issues that it believed may have arisen.

The Tribunal did not consider that the Level 2 provider had supplied any evidence or credible supposition which was sufficient to show that the issue in relation to hacking set out above (or any other technical issue) had caused the discrepancies between the Level 2 provider's logs and the Level 1 provider (and Verifier) logs in respect of the complainants.

Therefore, having had regard to the facts of the case, the Tribunal did not consider that the Executive's case that the reason for the inaccuracy of the logs provided by the Level 2 provider was that they had been falsified (the burden of proving such remaining on the Executive on the balance of probabilities) was undermined by the material submitted by the Level 2 provider.

Consequently, the Tribunal was satisfied, on the balance of probabilities, for the reasons advanced by the Executive, that the Level 2 provider had knowingly falsified information, and 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 – Consent to Charge
"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 alleged breach of paragraph 4.2.4 and noted 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 noted that the Verifier had provided 41 message logs to it. Correspondence with the Verifier indicated that attempts to deliver chargeable Service messages which failed would appear in its message logs, and the Executive noted that, in respect of some logs, failed messages did appear within the message logs provided by the Verifier. Examples of such failed messages could be found in the following message logs:

<u>Verifier message log for mobile number ********339</u>

The Verifier log for MSISDN ********339 showed that chargeable messages failed to be delivered between 12 April 2015 and 10 May 2015. The Executive noted that the purported

opt-in date within the Level 2 provider's message log was 16 August 2014. However, the first message to appear on the Verifier message log was recorded on 15 March 2015.

Verifier message log for mobile number ********494

The Verifier log for MSISDN ********494 showed that three out of six chargeable messages failed to be delivered between 25 April 2015 and 30 May 2015. The Executive noted that the purported opt-in date within the Level 2 provider's message log was 8 August 2014. However, the first message to appear on the Verifier message log, albeit a failed message, was recorded on 25 April 2015.

The Executive asserted that this evidence supported its contention that entries in the Level 2 provider's complainant message logs which showed failed messages, but which were not reflected in the Level 1 provider or Verifier's logs, must therefore be false.

As noted in the alleged breach of paragraph 4.2.4, the Executive had requested that IMImobile provide message logs for 15 complainants. IMImobile had provided message logs that did not correspond with those which were supplied by the Level 2 provider. Further to this, the Executive had requested that Zamano provide message logs for 34 complainants. Zamano had provided message logs that did not correspond with those which were supplied by the Level 2 provider. In the case of nine complainants Zamano confirmed that the MSISDNs did not appear on its system.

As referenced earlier in the alleged breach of paragraph 4.2.4, the Level 2 provider had supplied six reasons why the Service messages may be routinely failing. However, taking into account the responses received from IMImobile, Zamano and the responses to the complainant questionnaire, the Executive asserted that no explanation had been provided as to why the Level 2 provider logs for complainants showed almost all Service messages failing, but the Level 1 provider and Verifier logs did not reflect such failed messages.

In addition the Executive noted that the Level 2 provider had not stated that an issue had occurred on its system nor provided evidence of such an issue. The Executive therefore concluded that there had not been a message failure issue and that Service messages listed in the Level 2 provider message logs were not sent (or attempted to be sent) to complainants. 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.

As noted in 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.

Further, in any event the Level 2 provider had charged consumers in the period after 10 December 2014 whilst knowing that it did not have the required robust third party verification of consent to charge in respect of those consumers. 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.

In response to questioning by the Tribunal following the Level 2 provider's submission regarding Veoo logs showing an entry which stated "GVIOPT", the Executive understood this showed the opt-in date of which Veoo had been advised when the Service migrated to their shortcode. The Executive's positon was that the log did not evidence a message sent via Veoo's platform. The Executive understood that the source of the entry could be the Level 2 provider. The Executive noted that the purported opt-in dates shown were before the Level 2 provider had stated that GoVerifyIt was in full use.

In response to questioning by the Tribunal following the Level 2 provider's submission regarding delay in requesting message logs from it, the Executive accepted this had occurred. The Executive could not establish the reason for this without further internal enquiries. The Executive accepted the delay shown was a learning point. The Executive submitted that the Level 2 provider had also delayed in its responses to queries from the Executive.

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 alleged breach. The Level 2 provider referred to the submissions it had made in response to the alleged breach of paragraph 4.2.4 of the Code.

The Level 2 provider stated that each and every single log record provided to PhonepayPlus was genuine. The Level 2 provider stated that technical reasons explained why certain premium messages would not show on Level 1 provider or Verifier logs. The Level 2 provider noted that both Level 1 providers had confirmed that technical interferences including server issues would indeed lead to messages not hitting their technical platforms.

The Level 2 provider submitted that the paperwork was gathered by the Executive without due care for standards, good practice or attention to details, and also submitted that the burden of proof had been reversed and shifted to it. Nevertheless, the Level 2 provider stated that it (and not the Executive) was able to present material evidence that was professional (unlike the questionnaire or short code synopsis, for example).

The Level 2 provider stated that it used robust independent verification for its online services and the Track 1 Action Plan had been fully implemented.

In informal representations, the Level 2 provider noted that Veoo's logs for opt-ins prior to November 2014 stated "GVIOPT" which could show that there had been robust evidence of consent to charge.

The Level 2 provider submitted that the alleged breach of Code rule 2.3.3 had no factual basis, and stemmed from the Executive's claim that its logs were incorrect. The Level 2 provider stated that its logs were correct and true and this was based on facts, not assumptions. The Level 2 provider stated that technical interferences were caused by server abuse incidents. The Level 2 provider stated that its entire reasoning was based on verifiable material unlike the Executive's paperwork. The Level 2 provider submitted that the case should be fully dismissed if PhonepayPlus wished to protect its accountability and its credible role within the industry as a regulator with a core goal being to protect consumers.

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

The Tribunal referred to its previous findings regarding breach of para. 4.2.4. 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. Accordingly the breach of charging without consumer consent had occurred after the Track 1 procedure had been concluded.

The Tribunal noted the Level 2 provider's detailed response and submissions, however the Tribunal did not consider that they provided a defence or an adequate explanation for why it had charged consumers without holding robust evidence of their consent. The Tribunal noted that the information on the Veoo logs related to migrated opt-in information and did not constitute such evidence, and moreover the opt-in dates pre-dated when the Level 2 provider stated it had put GoVerifyIt into full use.

The Tribunal considered the Level 2 provider's submission that the Executive had unduly delayed before asking the Level 2 provider for log evidence relating to at least ten complaints. The Tribunal considered that it was the Level 2 provider's responsibility to ensure that it held evidence of consent to charge for consumers, and it was not the Executive's responsibility to bring this to their attention, and so this delay did not mitigate the Level 2 provider's actions. For the purpose of fact finding and deciding whether there had been a breach of Code rule 2.3.3, the Tribunal did not find any delay to have been a determinative feature.

Consequently, for the reasons advanced by the Executive, on the balance of probabilities, 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

Initial overall assessment

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

Paragraph 4.2.4 - Provision of false information to PhonepayPlus

The initial assessment 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 deliberately supplied false and misleading information to PhonepayPlus.

Rule 2.3.3 – Consent to charge

The initial assessment 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; and
- The case had a clear and highly detrimental impact on consumers.

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

Final overall assessment

In determining the final overall assessment for the case, the Tribunal found the following aggravating factor:

- The Level 2 provider had previously been subject to a Track 1 procedure, which had included requirements regarding consent to charge.

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

- There was evidence that some complainants had been refunded by the Level 2 provider.

The Level 2 provider's evidenced revenue in relation to the Service in the period from December 2014 to December 2015 was in the range of Band 1 (over £1,000,000).

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 and having considered the proportionality of the sanction and the risk of consumers suffering further harm as a result of a breach of the Code, the Tribunal decided to impose the following sanctions:

- a formal reprimand;
- a fine of £250,000;
- 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 PhonepayPlus that such refunds have been made.

Administrative charge recommendation: **100%**

APPENDIX A

[redacted]

OPTIN	URL	TIME
16/08/2014	http://enter.hot-mobi-babes.com/?c=4edb11a2a	13:47:33

FREE/PREMIUM	MESSAGES	LANDED	TIME
FREE	http://enter.hot-mobi-babes.com/?c=4edb11a2a	SENT	16/08/2014 13:44
FREE	FreeMsg U have joined hot-mobi-babes Vids and pics club for £3 per week until you send STOP to 66033 Help? 08081349827	SENT	16/08/2014 13:47
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	FAILED	17/08/2014 13:36
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	FAILED	24/08/2014 14:22
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	SENT	31/08/2014 16:51
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	FAILED	07/09/2014 12:34
FREE	FreeMsg: UR subscribe to Hot Mobi Babes unlimited sexy videos for £3.00 Per week. Helpline: 08081349827 SP: Intrugo Ltd text STOP To 66033 to stop	SENT	13/09/2014 18:59
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	FAILED	14/09/2014 12:06
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	FAILED	21/09/2014 18:20
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	FAILED	28/09/2014 14:44
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	FAILED	05/10/2014 18:10
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	SENT	12/10/2014 14:56
FREE	FreeMsg: UR subscribe to Hot Mobi Babes unlimited sexy videos for £3.00 Per week. Helpline: 08081349827 SP: Intrugo Ltd text STOP To 66033 to stop	SENT	13/10/2014 19:54
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	SENT	19/10/2014 13:54
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	FAILED	26/10/2014 17:43
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	SENT	02/11/2014 16:22
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	FAILED	09/11/2014 14:21
FREE	FreeMsg: UR subscribe to Hot Mobi Babes unlimited sexy videos for £3.00 Per week. Helpline: 08081349827 SP: Intrugo Ltd text STOP To 66033 to stop	SENT	13/11/2014 20:25
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	FAILED	16/11/2014 17:58
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	FAILED	23/11/2014 13:02
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	FAILED	30/11/2014 12:56
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	FAILED	07/12/2014 13:58
FREE	FreeMsg: UR subscribe to Hot Mobi Babes unlimited sexy videos for £3.00 Per week. Helpline: 08081349827 SP: Intrugo Ltd text STOP To 66033 to stop	SENT	13/12/2014 18:03
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	SENT	14/12/2014 12:13
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	SENT	21/12/2014 14:10
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	FAILED	28/12/2014 17:03
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	FAILED	04/01/2015 19:24
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	FAILED	11/01/2015 16:17
FREE	FreeMsg: UR subscribe to Hot Mobi Babes unlimited sexy videos for £3.00 Per week. Helpline: 08081349827 SP: Intrugo Ltd text STOP To 66033 to stop	SENT	13/01/2015 18:33
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	FAILED	18/01/2015 12:29
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	FAILED	25/01/2015 13:55
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	FAILED	01/02/2015 15:11
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	SENT	08/02/2015 19:19
FREE	FreeMsg: UR subscribe to Hot Mobi Babes unlimited sexy videos for £3.00 Per week. Helpline: 08081349827 SP: Intrugo Ltd text STOP To 66033 to stop	SENT	13/02/2015 19:29
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	FAILED	15/02/2015 12:54
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	SENT	22/02/2015 18:31
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	SENT	01/03/2015 14:25
PREMIUM	http://enter.hot-mobi-babes.com/?c=430947d80 TEXT STOP TO 66033 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	FAILED	08/03/2015 12:19
FREE	FreeMsg: UR subscribe to Hot Mobi Babes unlimited sexy videos for £3.00 Per week. Helpline: 08081349827 SP: Intrugo Ltd text STOP To 66033 to stop	SENT	13/03/2015 20:16
FREE	FreeMsg: Your subscription is changing shortcode to 82999 costing £3 per week. SP Intrugo Help? 08081349827 text stop to 82999 to stop.	SENT	14/03/2015 13:05
PREMIUM	http://hot-new-babes.com/?c=430947d80 TEXT STOP TO 88150 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	BILLED	15/03/2015 12:51
PREMIUM	http://hot-new-babes.com/?c=430947d80 TEXT STOP TO 82999 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	BILLED	22/03/2015 13:23
PREMIUM	http://hot-new-babes.com/?c=430947d80 TEXT STOP TO 82999 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	BILLED	29/03/2015 13:21
PREMIUM	http://hot-new-babes.com/?c=430947d80 TEXT STOP TO 82999 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	BILLED	05/04/2015 13:20
PREMIUM	http://hot-new-babes.com/?c=430947d80 TEXT STOP TO 82999 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	BILLED	12/04/2015 13:20
FREE	FreeMsg: UR subscribe to Hot New Babes unlimited sexy videos for £3 Per week. Helpline: 08081349827 SP: Intrugo Ltd text STOP To 82999 to stop	SENT	13/04/2015 18:34
PREMIUM	http://hot-new-babes.com/?c=430947d80 TEXT STOP TO 82999 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	BILLED	19/04/2015 13:19
PREMIUM	http://hot-new-babes.com/?c=430947d80 TEXT STOP TO 82999 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	BILLED	26/04/2015 19:00
PREMIUM	http://hot-new-babes.com/?c=430947d80 TEXT STOP TO 82999 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	BILLED	03/05/2015 19:10
PREMIUM	http://hot-new-babes.com/?c=430947d80 TEXT STOP TO 82999 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	BILLED	10/05/2015 19:10
PREMIUM	http://hot-new-babes.com/?c=430947d80 TEXT STOP TO 82999 TO STOP ALL MESSAGES, FOR HELP 24HOURS CALL 08081349827	BILLED	17/05/2015 19:11
FREE	FreeMsg: UR subscribe to Hot New Babes unlimited sexy videos for £3 Per week. Helpline: 08081349827 SP: Intrugo Ltd text STOP To 82999 to stop	SENT	18/05/2015 19:36