

Tribunal meeting number 174 / Case 1

Case reference: 56005
Level 2 provider: Rhydel Ltd (UK)
Type of service: NewBabes - Glamour video subscription service
Level 1 provider: Zamano Solutions Limited (Ireland) and 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

Between 5 November 2014 and 22 July 2015, PhonepayPlus received 143 complaints from consumers in relation to a glamour video subscription service called NewBabes (the “**Service**”), which operated on the dedicated shortcode 78018 and on the shared shortcodes 82999 and 88150 at a cost of £3 per week. The Level 2 provider for the Service was Rhydel Ltd (the “**Level 2 provider**”) and the Level 1 providers were Zamano Solutions Limited (“**Zamano**”) with respect to shortcode 78018 and Veoo Ltd (“**Veoo**”) with respect to shortcodes 82999 and 88150 (the “**Level 1 providers**”). The Service commenced operation (i) on 23 September 2014 on shortcode 78018; (ii) on 1 November 2014 on shortcode 88150; and (iii) on 11 February 2015 on shortcode 82999. The Service continues to operate on shortcodes 82999 and 88150 but the Service was voluntarily suspended by Zamano Solutions Limited on 10 September 2015, following correspondence with PhonepayPlus.

The Level 2 provider stated that the Service was promoted on banners within the mobile web platform. To interact with the Service, consumers could click on the banners which redirected them to the Level 2 provider’s landing page. Consumers initiated the Service by responding to receipt of a wireless application protocol (“**WAP**”) message to their handset or by sending a mobile originating (“**MO**”) text message containing a keyword to one of the Service shortcodes.

Complaints

Concerns regarding the Service were raised by complainants who variously alleged that the Service charges they incurred were unsolicited and/or that the STOP command failed to cancel the Service.

The Executive relied on the content of all the complaints received, examples of which include:

“I have not subscribed to any additional services, so I cannot understand why I am being charged. Not once or twice, but on multiple occasions.”

“Consumer received link to an adult website every time he tops up. Consumer has never subscribed to this service. Consumer has sent a STOP message which has not worked.”

“I have been charged for a service I have never signed up for. This service appears to be an adult service called BABES I have no idea of the website I seem to be getting charged £2.50 per text so far charged £2.50 October £10 Nov £20 Dec £20 Jan total £52.50 according to your checker the company is called Rydel Ltd [sic].”

“Seems to be some sort of adult site. I incurred a £5 charge (2x £2.50 weekly charges). I contacted O2 and they advised me to text the word STOP to the following number: 78018 After texting STOP, I then received a reply from the number to notify me the following: "FreeMsg: Your number has been removed and unsubscribed [sic] from our service, there will be no more messages sent to you from us." However, I have NEVER subscribed [sic] to their service or any other service so this is obviously a big scam...”

“Text message received unsolicited containing link to internet URL. Message deleted immediately but have been charged £3 for receiving this. The SMS was completely unsolicited and yet I’ve been charged £3 for receiving.”

During the investigation, the Executive requested text message logs for the complainants from the Level 2 provider and the Level 1 providers. After analysing the Level 2 provider’s message logs, the Executive noted that i) there was a high failure rate of chargeable Service messages following the purported consumer opt-ins and (ii) the delivery status for Service messages was unclear. The Executive noted that the complaints could broadly be divided into three categories:

Category one: Message logs for complainants in category one showed an opt-in followed by successfully delivered chargeable messages. These logs did not contain failed messages and tended to be for complainants that complained during the early part of the complaint period.

Category two: Message logs for complainants in category two often showed two successfully delivered chargeable messages on the same day. These logs tended to include both billed and failed messages which mainly occurred among the early complaints to PhonepayPlus.

Category three: Message logs for complainants in category three (the largest category) showed numerous failed messages from the date of the complainants’ purported opt-in, followed by successfully delivered chargeable messages. These logs tended to include both billed and failed messages and mainly occurred among the later complaints to PhonepayPlus.

In light of the large number of failed messages identified by the Executive in the complainants’ text message logs, and the possible explanations offered by the parties in the value chain (referred to under the alleged breach of rule 2.3.3 of the Code), the Executive contacted 131 complainants (the total number of complainants who had contacted PhonepayPlus about the Service as at that date) with the following series of questions:

- “1) Is the mobile phone that received the chargeable text messages on contract or pay-as-you-go?
- 2) 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?
- 3) 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)?
- 4) 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 a screenshot of the Service subscription site and asked whether they recalled viewing and/or interacting with it or a similar service promotion. In total, 35 of the complainants responded. In relation to question one, 31 complainants confirmed that they had a contract phone. For the two complainants that were on pay-as-you-go, one complainant advised that they always kept their credit on or around £5 to £10. In relation to question three, 27 of the complainants advised that their mobile phone was not regularly switched off or had no mobile signal. In relation to question four, 30 complainants advised that they had not transferred their MSISDN between mobile telephone companies in the six months before receipt of the chargeable text messages.

The investigation

The Executive conducted this matter as a Track 2 investigation in accordance with paragraph 4.4 of the PhonepayPlus Code of Practice (12th Edition) (the "**Code**").

The Executive sent a breach letter to the Level 2 provider on 7 August 2015. Within the breach letter the Executive raised the following breaches of the Code:

- Rule 2.3.3 – Consent to Charge
- Paragraph 4.2.4 – Provision of false/misleading information to PhonepayPlus
- Rule 2.3.12 – Subscription Spend Reminders

The Level 2 provider responded to the breach letter on 21 August 2015. In response to the Level 2 provider's comments on the breach letter, on 24 August 2015 the Executive sent a follow-up direction for information to the Level 1 providers. The Level 1 providers responded on 28 August 2015 and 1 September 2015.

The Level 2 provider had initially indicated that it wished to provide informal representations to the Tribunal but it was unavailable to attend the date of the scheduled Tribunal. The Tribunal date was rescheduled to a new date but the Level 2 provider did not respond to emails from the Executive to confirm whether it wished to attend and provide informal representations. The Tribunal considered the correspondence regarding this matter and was satisfied that the Level 2 provider had been notified of the new Tribunal date and that it had been given an opportunity to provide informal representations but had chosen not to do so. On 17 September 2015, the Tribunal reached a decision on the breaches raised by the Executive.

The Tribunal considered the following evidence in full:

- The complainants' accounts;
- The Executive's monitoring of the Services conducted on 10 and 13 July 2015;
- 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 a Mobile Network operator's verifier;
- Correspondence between the Executive and a Third Party Verifier;
- Complainant message logs from the Level 2 provider, Level 1 provider and Mobile Network operator's verifier;
- Complainant questionnaires and responses;
- Complainants' mobile telephone bills;
- PhonepayPlus Guidance on "Privacy and Consent to Charge" and "Promotions and promotional material"; and
- The breach letter of 7 August 2015 and the Level 2 provider's response.

SUBMISSIONS AND CONCLUSIONS

ALLEGED BREACH 1

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 this consent."

1. The Executive submitted that the Level 2 provider had breached rule 2.3.3 of the Code as consumers had been charged without their consent for the following reasons:
 - i. Robust evidence of consent to charge was not held for complainants;

- ii. Category three complainant message logs supplied by the Level 2 provider that purported to show consumers opt-in to the Service were false;
- iii. Itemised telephone bills and evidence supplied by Mobile Network operators demonstrated that category two complainants were charged more than the advertised price; and
- iv. There were discrepancies between the date of the Service commencement and the dates of purported Service opt-ins.

The Executive relied on the content of PhonepayPlus Guidance on 'Privacy and consent to charge' (the "**Guidance**"), correspondence exchanged with the Level 2 provider, complainant accounts (example of which are referenced in the 'Background' section above), complainant questionnaire responses (also referenced in the 'Background' section above) and complainant text message logs. The Guidance states:

Paragraph 1.4

"For this reason, it is essential that providers can provide robust evidence for each and every premium rate charge...."

Paragraph 2.1

"Robust verification of consent to charge means that the right of the provider to generate a charge to the consumer's communication bill is properly verifiable. By 'properly verifiable', we mean a clear audit trail that categorically cannot have been interfered with since the record, either of consent to purchase or simply of consent to future marketing... was created...."

Paragraph 2.9

"It is more difficult to verify where a charge is generated by a consumer browsing the mobile web, or by using software downloaded to their device. In these circumstances, where the consumer may only have to click on an icon to accept a charge, the MNO has no record of an agreement to purchase, and so robust verification is not possible through an MNO record alone."

Paragraph 2.10

"In both of the instances set out above, we would expect providers to be able to robustly verify consent to charge (or to marketing, see Part Two of this General Guidance Note). Factors which can contribute to robustness are:

- An opt-in is PIN-protected (e.g. the consumer must enter their number to receive a unique PIN to their phone, which is then re-entered into a website);
- A record is taken of the opt-in, and data is time-stamped in an appropriately secure web format (e.g. https or VPN);
- Records are taken and maintained by a third-party company which does not derive income from any PRS. We may consider representations that allow a third-party company which receives no direct share of PRS revenue from the transaction, but does make revenue from other PRS, to take and maintain records. It will have to be proven to PhonepayPlus' satisfaction that these records cannot be created without consumer involvement, or tampered with in any way, once created;
- PhonepayPlus is provided with raw opt-in data (i.e. access to records, not an Excel sheet of records which have been transcribed), and real-time access to this opt-in

data upon request. This may take the form of giving PhonepayPlus password-protected access to a system of opt-in records;

- Any other evidence which demonstrates that the opt-in cannot be interfered with.”

Reason one - Robust evidence of consent to charge was not held for complainants

The Executive noted that the message logs supplied by the Level 2 provider showed that all complainants, for which the Executive had been supplied a message log, had opted-in to the Service via the WAP route.

The Level 2 provider was required to hold robust consent to charge evidence for the WAP opt-ins. The Executive noted that the Guidance makes it clear that all charges must be robustly verifiable. Although Guidance is not binding on providers, where a provider fails to follow Guidance there is an expectation that it will take equivalent alternative steps to ensure that it fulfils PhonepayPlus’ expectations (and complies with the Code).

In response to a direction from the Executive, the Level 2 provider confirmed on 26 January 2015 the following:

“Up until the 25th of November 2014 we were using a [sic] offline version of robust verification where the 3rd party verification company would take daily mark ups of our landing pages this was also backed up by our own in house system where users were assigned a unique identification. We can confirm that all our services now use online versions of robust verification.”

The Executive noted from the complainant message logs that all complainants appeared to have purportedly opted-in to the Service before 25 November 2014 and therefore fell into the period where the Level 2 provider had admitted it had no robust evidence of consent to charge.

The Executive sought clarification from the Level 2 provider regarding the third party verification company it used to robustly verify opt-ins to the Service. On 11 February 2015 the Level 2 provider confirmed the name of this company (the “**Third Party Verifier**”).

The Executive understood that the Third Party Verifier offers two types of services; one where they take a secure tamper proof record of the PIN that is entered into a provider’s website (the “**Full version**”) and another where they take a screenshot of the landing page on a particular day to show what a consumer may have seen (the “**Offline version**”). It is clear that for the purposes of robust evidence of consumers’ consent to be charged only the Full version is sufficient evidence, as the offline version does not provide any evidence that a consumer consented to charges; it only shows what a consumer would have seen on a provider’s website on a particular day. The Executive understood from the Level 2 provider’s response that it was stating that prior to 25 November 2014, it had only engaged the Third Party Verifier to provide the Offline version.

During the investigation, the Executive wrote to the Third Party Verifier to request robust opt-in verification for a sample of eighteen complainant MSISDNs which had opted in to, and been charged by the Service. The Third Party Verifier advised that, whilst it took a daily snapshot of the Service website, it was unable to provide robust verification of an opt-in for those MSISDNs.

In addition to making enquiries with the Third Party Verifier, the Executive made enquires of Veoo; the Executive noted that the Third Party Verifier had provided to Veoo evidence of robust opt-in for ten consumers’ MSISDNs, all of which opted in to the Service on 29 October

or 30 October 2014. This was in apparent contradiction to the Level 2 provider's statement that robust verification of the WAP Service opt-in route had not been activated until 25 November 2014. In light of this, the Executive submitted that the Level 2 provider may have had the Full version of the Third Party Verifier's service in place before 25 November 2014 but it would have no record of opt-ins if the Level 2 provider had chosen not to use the Full version despite it being available.

Notwithstanding the information received from Veoo, the Executive submitted that the Level 2 provider had not provided evidence, as required under rule 2.3.3 of the Code, which established that it had obtained consent to charge for complainants who it stated had opted in, and were charged by, the Service.

Reason two – Category three complainant message logs supplied by the Level 2 provider that purported to show consumers' opt-in to the Service were false;

The Executive noted that the complaints received by PhonepayPlus spanned the period between November 2014 and July 2015. Further, it noted from complainant text message logs supplied by the Level 2 provider that the apparent opt-in dates were consistently shown in all complainant message logs as occurring between August 2014 and November 2014 regardless of when the complaint was received. Yet in the category three complainant message logs, the date of the first successfully charged Service message was, in the majority of the message logs, significantly later than the purported date of the Service opt-in.

Further, in the case of complaints later in the complaint period 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 highlighted two example message logs which demonstrated this pattern:

The Level 2 provider message log for MSISDN ending 973:

The Executive noted that the provided log showed that the initial opt-in to the Service occurred on 23 August 2014. The Executive also noted from the message log supplied by the Level 2 provider that the status of the chargeable Service messages were variously described as 'FAILED', 'BILLED', or 'SENT'. During correspondence exchanged in the investigation, the Level 2 provider clarified that messages listed as 'SENT' should in fact be listed as 'FAILED' within the message logs. The Executive noted that the above entry in the message log and numerous subsequent messages' status were listed as either 'FAILED' or 'SENT'. The first Service message listed as 'BILLED' was delivered to this MSISDN on 31 January 2015, 23 weeks after the purported opt-in date.

The Level 2 provider message log for MSISDN ending 524:

The Executive noted that the provided log showed that the initial opt-in to the Service occurred on 30 August 2014. The Executive also noted that the above entry in the message log and numerous subsequent message status of all chargeable Service messages were listed as either 'FAILED' or 'SENT'. The first message listed as 'BILLED' was delivered on 7 March 2015, 27 weeks after the purported opt-in date.

During the investigation, the Executive directed the Level 2 provider to provide an explanation for the high failure rate of chargeable Service messages and the following response was received:

"We have submitted the messages from our system via our aggregator who in turn submits them to the networks. Once we submit the messages they are out of our control until we

receive a delivery status receipt which states the result of the sent messages, we have no way of knowing where in the line the messages have failed and these could be at aggregator or network level. There could be a number of reasons why these fail including technical errors within the line.”

The Executive sought further clarification from the Level 2 provider and requested that it supply a complete list of all the solutions implemented in an attempt to eradicate the high message failure rate and confirm the outcome of its investigation. The Level 2 provider stated:

“We regularly cleaned up our database by removing MSISDN’s that had continuously status “Failed” messages for a period of time this was recognised during some of the migration process that incorrect network codes could be causing the failures. *[The Executive noted that, despite this assertion, the failed Service messages continued for 23 and 27 weeks respectively in the above example message logs].* We also did network look ups where the correct code for a particular network is tied up to the MSISDN’s on our system to ensure that the correct network code was being reported and entered on to our system prior to any messages sent to MSISDN’s that were not delivering positive receipts.

We can confirm that our system has been altered to only recognise only positive receipts as billed, all other status messages are recognised as failed and a regular system clean up now removes consistently failed messages...

As mentioned in the last response, there can be many reasons for messages to fail and some of the reasons not limited to but include network errors, Level 1 delivering issues, time outs, phones handsets off, credit fails, incorrect network code, no network on the phone. In all probability the high rate of failures can only be answered by the Level 1 provider.”

The Executive also made enquiries of the Level 1 providers regarding the high failure rate of chargeable Service messages. The Executive received the following response from Zamano:

“Once a text message has left Zamano’s message gateway its delivery to the customer’s mobile phone is out of our control. Primary causes of failed message delivery include:
The customer’s phone has gone out of range or has ran out of power
The customer is out of mobile credit
If routing information stored against a certain mobile number is incorrect for some reason (e.g. following a botched port between operators) the message may not be routed to the correct mobile operator”

The Executive also received the following response from Veoo:

“In the case of the MSISDNs provided [MSISDNs redacted] Veoo have not received a delivery receipt confirming a status of the messages from the mobile network operator therefore after period of 3 days the Veoo platform has placed the messages into an “error” status as this is the length of validity of the messages. Status’ on messages sent through each Mobile Network are passed back to L1’s and are reflected in the logs accordingly.”

In addition to the above explanations provided by Zamano and Veoo, the Executive considered that the complainant message logs provided by the Level 1 providers did not assist in understanding the regularity with which failed messages appeared in the logs.

Given the unclear explanation regarding the high failure rate of the chargeable Service messages from the Level 2 provider and the Level 1 providers, the Executive contacted a verifier which had access to mobile data held by one of the Mobile Network operators (the “**Verifier**”). The Verifier was sent a sample of 27 complainant mobile numbers and was

requested to supply message logs showing the interaction between the Service and the complainants' mobile numbers.

Notwithstanding seven mobile numbers for which the Verifier was unable to provide information, the Executive noted from the remaining 20 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 on 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 MSISDN ending 973 listed the first Service message on 31 January 2015, and the Verifier log for MSISDN ending 524 listed the first Service charge on 7 March 2015.

In response to enquiries from the Executive, the Verifier confirmed that failed attempts to charge consumers from the Service shortcode would appear in its text message logs. In light of this, the Executive asserted that the logs showing failed chargeable Service messages were not correct, nor were the purported opt-in dates listed in the Level 2 provider's message logs.

Further, the Executive referred to the complainant accounts, and the complainant responses to the Executive's questionnaire, both of which are referenced in the 'Background' section above. The Executive considered, on a balance of probabilities, 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. Rather, the Executive submitted that the message logs supplied by the Level 2 provider which listed opt-ins to the Service were, on a balance of probabilities, incorrect.

In light of the above confirmation from the Verifier, the complainant accounts and the complainant responses to the Executive's questionnaire, the Executive asserted that the logs did not show valid opt-ins to the Service and the Level 2 provider did not have consent to charge consumers.

Reason three - Itemised telephone bills and evidence supplied by Mobile Network operators demonstrated that category two complainants were charged more than the advertised price

The Executive asserted that complainants were charged more than the advertised price for the following two reasons:

- 1) Two Service charges were issued on the same date; and
- 2) The price point of Service shortcode 88150 increased, however the frequency on which Service messages were issued from Service shortcode was not decreased.

Two Service charges were issued on the same date

The Executive noted that the Level 2 provider had confirmed that the price point for the Service was £3 per week, that the Service cost was also stated as £3 per week in promotional material, and that Service messages provided by the Level 2 provider stated the cost of the Service was £3 per week.

The Executive noted that within some message logs supplied by the Level 2 provider for complainants falling into category two, there were multiple chargeable entries on the same dates. By way of example, the Executive highlighted the following message logs:

The Level 2 provider message log for MSISDN ending 769

The Executive noted that the message log stated that the complainant opted-in and was successfully charged on 26 October 2014. The Executive further noted that 'FAILED' chargeable Service messages were issued on 2 November, 9 November and 16 November 2014. On 23 November 2014, one 'FAILED' Service message and one 'BILLED' Service message were issued. On 30 November, 7 December and 14 December 2014 two 'BILLED' Service messages were issued to the complainant on each date.

On initial consideration of the message log, the Executive's view was that it appeared that two chargeable Service messages were issued on 30 November, 7 December and 14 December 2014 to recoup the 'FAILED' Service messages issued on 2 November, 9 November and 16 November 2014 and may therefore be valid charges.

However, after a complainant contacted PhonepayPlus to register his complaint, the complainant supplied two itemised telephone bills. The Executive noted from the telephone bills that successful £3 Service charges were delivered on 26 October, 2 November, 9 November and 16 November 2014. In addition, two successful £3 Service charges were delivered on 23 November, 30 November and 7 December 2014. The message log charges for the 14 December 2014 fell outside the time period covered by the itemised telephone bill. Accordingly, the Executive noted that the delivery status of the messages on the Level 2 provider's log were incorrect.

The Executive asserted that, given the promotional material and the Service messages' explicit promotion of a £3 per week service, and the clear evidence from itemised telephone bills, the above complainant had been overcharged and it was clear that the complainant would not have consented to being charged twice for the same subscription to the Service.

The Level 2 provider message log for MSISDN ending 661

The Executive noted that the message log stated that the complainant opted-in, and was successfully charged, on 18 October 2014. The Executive further noted that a 'FAILED' chargeable Service message was issued on 22 November 2014. On 29 November and 6 December 2014 one 'FAILED' Service message and one 'BILLED' Service message were issued. On 13 December 2014 two 'BILLED' Service messages were issued to the complainant. On 25 October, 1 November, 8 November, 15 November, 20 December, 27 December 2014 and 3 January 2015 one 'BILLED' Service message was issued on each date. On initial consideration of the message log, the Executive's view was that it appeared that two chargeable Service messages were issued on 13 December 2014 to recoup the 'FAILED' Service message issued on 22 November 2014 and may therefore be valid charges.

However, after the complainant contacted PhonepayPlus to register his complaint, the complainant supplied three itemised telephone bills. The Executive noted from the telephone bill covering the period 6 October 2014 to 5 November 2014 that three successfully charged Service messages were sent, that the telephone bill covering the period 5 November 2014 to 5 December 2014 showed five successfully charged Service messages were sent and the telephone bill covering 6 December 2014 to 5 January 2015 showed seven successfully charged. In comparing the number of Service charges in the itemised telephone bill, and the entries in the Level 2 provider message log, it was clear that the status of all entries in the message log listed as 'FAILED' were incorrect and should have been listed as 'BILLED'.

In addition to the itemised telephone bill supplied by the complainant, the Executive contacted the Mobile Network operator concerned and requested a message log for the MSISDN ending 661. The log supplied by the Mobile Network operator also demonstrated that no Service messages failed, contrary to the Level 2 provider message log for the same MSISDN, and that double charging occurred on 29 November, 6 December and 13 December 2014.

The Executive asserted that, given the promotional material and Service messages' explicit promotion of a £3 per week service, and the clear evidence in the itemised telephone bills and the Mobile Network operator log, the consumer was overcharged £6 on 29 November, 6 December and 13 December 2014, and the above complainant would not have consented to the Service charges incurred.

The price point of Service shortcode 88150 increased, however the frequency with which Service messages were issued from the Service shortcode was not decreased accordingly

The Executive noted from the message logs for complainants that migrated from the Service opt-in shortcode 78018 to Service shortcode 88150 that they were issued with two £1.50 chargeable Service messages per week to ensure the £3 per week Service charge was collected.

Further, the Executive noted when reviewing the Verifier's message logs that there were two examples which demonstrated that the price point for Service shortcode 88150 changed from £1.50 per message received to £3 per message received on or around 1 February 2015. The Executive also noted that the frequency at which the Service messages from shortcode 88150 were issued was not reduced accordingly to take into account the increased price point, resulting in complainants incurring a £6 per week charge instead of a £3 per week charge. Whilst the Executive relied on the two examples referenced above, the Executive considered it highly likely that all consumers who were charged by Service shortcode 88150 on or around 1 February 2015 were overcharged. Clearly for the reasons listed above, consumers would not have consented to charges of £6 per week, given the promotion of a £3 per week charge.

Reason four – Discrepancies between the date of Service commencement and the dates of purported Service opt-in

The Level 2 provider had confirmed that the Service commenced operation in September 2014. Zamano also confirmed to the Executive that the Service commenced operation on 23 September 2014.

The Executive noted when reviewing the Level 2 providers' message logs that several message logs show a Service opt-in date prior to 23 September 2014. As an example, the Executive referenced the message logs for the MSISDNs ending 973 and 899 which showed Service opt-in dates of 23 August 2014 and 6 September 2014 respectively.

The Executive asserted that the opt-ins to the Service shown in the Level 2 provider message logs that predated the 23 September 2014 could not have validly occurred, given that the Service had not even commenced operation at that time, and therefore any consent associated with the purported opt-ins pre-23 September 2014 did not exist.

For all the reasons set out above the Executive asserted that the Level 2 provider had not provided evidence of consent to charge consumers and further it did not have consent to charge consumers. Accordingly, the Executive submitted that the Level 2 provider had acted in breach of rule 2.3.3 of the Code.

In response to questions from the Tribunal, the Executive acknowledged that the Level 2 provider had raised the possibility of a network code error or problem on the line with the transmission of messages to the Network operator as a possible explanation for the numerous failed messages. However, the Executive highlighted that it had contacted the

Level 1 provider to seek comment on this and although it had raised general reasons as to why messages may fail, it had not stated that it was aware of a technical problem or that it had not transmitted the messages to the Network operator. Therefore, the Executive submitted that it was reasonable to infer that the Level 1 provider had transmitted the messages to the Network operator in which case, the Verifier would have had sight of any attempts to bill the consumer. The Executive confirmed that it was dependant on the information supplied by parties in the value chain to ascertain what had happened and in this case, it had requested evidence concerning the matters raised but none had been provided.

In response to questioning from the Tribunal regarding the Level 2 provider's migration from Zamano to Veoo, which the Level 2 provider had stated it had done because of the high rate of failed messages, the Executive highlighted that Level 2 provider appeared to have signed a contract with Veoo in October 2014 and revenue appeared to have been generated on the Veoo shortcodes from January 2015. Yet, the Executive noted that some complainants remained on the Zamano shortcode and encountered failed messages until March and April 2015.

The Executive stated that all complaints received by PhonepayPlus had had a purported opt-in before 25 November 2014, therefore it had not been able to test the Level 2 provider's assertion that it had third party verification in place after that date.

In relation to reason three regarding the increase in price point, the Executive acknowledged that Veoo had confirmed the version of events given by the Level 2 provider, that the increase in the price point of the Service shortcode had occurred earlier than the dates given by Veoo in its email to the Level 2 provider. The Executive submitted this matter was still a breach of rule 2.3.3, albeit it invited the Tribunal to consider the explanation given in determining the seriousness of the breach.

In relation to the failed messages, the Executive reiterated its case theory that the Level 2 provider had inserted a string of failed messages into some complainants' message logs, to make it appear that the consumers' opt-in had occurred at a time when the Level 2 provider had admitted that it did not have robust third party verification in place, thus limiting the extent of the breach.

The Executive clarified its written submissions regarding the message logs that showed an opt-in prior to Service commencement. The Executive stated that it did not accept the Level 2 provider's submission that this had occurred as a result of human error. The Executive noted that if the opt-ins were meant to have occurred at a later date, messages would have been sent out more frequently than the weekly subscription and consumers would have been charged more than the advertised cost of the Service.

In relation to the Level 2 provider's assertions that some complaints were not genuine. The Executive denied that was the case and stated that the Level 2 provider had been provided with a full list of all complaints concerning the Service during the investigation.

2. The Level 2 provider denied that it was in breach of rule 2.3.3 of the Code and addressed each of the reasons for the alleged breach raised by the Executive.

In relation to reason one, the Level 2 provider stated that whilst it understood that the guidance advised that charges should be robustly verifiable, it also understood that the guidance was not binding. The Level 2 provider submitted that it had taken equivalent steps to ensure that it had consent to charge by way of an offline verification system which took daily snapshots of consumers' opt ins and this was also backed up by its in-house tamper proof system. The Level 2 provider stated that it held a full audit trail of consumers who had

subscribed using this system and that it would be willing to provide the technical specifications to PhonepayPlus.

The Level 2 provider explained that it used the offline and in-house system, while the online version was still being implemented. It had marketed its Service using both the online and off line versions simultaneously, although more marketing campaigns had used the offline version. The Level 2 provider asserted that, as a fledgling company that was less than a year old, it had addressed the issue of full robust verification in the correct way. It had found a service which after a period of promotion appeared to be very popular with subscribers, with this in mind it was aware that it had to act quickly and provide a platform that would protect not only the Level 2 provider but also its subscribers.

In relation to the second reason raised by the Executive, the Level 2 provider stated that it was obvious that it would have gained more subscribers during August and December as it had advertised its services on a daily basis during these months. It categorically denied the accusation that the logs that it had supplied were false. By way of explanation, it stated that the only real basis for the failed messages was that the Network operators had not received the messages. The Level 2 provider stated that it had previously explained to the Executive that the failure of the messages was outside its control once the messages had left its platform and been sent to its Level 1 provider, who in turn submitted them to the Mobile Network operators.

The Level 2 provider stated that it was aware that both its Level 1 providers had submitted information to the Executive regarding the possible reasons for failed messages. The Level 2 provider highlighted that message failures were not limited to the reasons provided by them, as there could be many more reasons including technical issues and a communication breakdown between it sending out the message and the delivery point.

The Level 2 provider addressed the Executive's evidence from the Verifier and stated that the Verifier would not see any messages in its message logs if the messages had encountered an issue on the line before reaching the Network operator. The Level 2 provider noted that the Executive had supplied 27 MSISDNs to the Verifier, yet the Verifier had only been able to supply information for 20 of those MSISDNs, which demonstrated that the Verifier could not supply information for more than 25% of the numbers supplied. For these reasons, it submitted that the information from the Verifier could not be 100% accurate and should not be relied upon by the Executive. Further, the Level 2 provider stated that the MSISDNs provided to the Verifier were complainants so their message logs must have showed some activity since the complainants had made a complaint.

The Level 2 provider noted that the Executive had submitted that the message logs supplied by the Level 2 provider were incorrect on a balance of probabilities. The Level 2 provider expressed surprise that the case had simply been based on a balance of probabilities.

The Level 2 provider submitted that the complainant questionnaire evidence was flawed and in its view was an example of an unnecessary course of action which it believed did not amount to admissible evidence. The Level 2 provider explained that the questions on the questionnaire were misleading and it was surprised that the Executive had taken it upon itself to send out a leading questionnaire. In its experience, it had found that complainants were unlikely to readily admit to having viewed or interacted with adult material and emailing complainants screenshots of a service that led a complainant to answer "Yes" or "No" did not prove whether they had interacted with a service or not.

The Level 2 provider asserted that it believed that the Executive had an agenda against its company, when it had contacted the complainants. Of the 35 complainants contacted, the

Level 2 provider stated that it appeared that certain individuals were contacted although they had not made an official complaint to PhonepayPlus and it had not been followed up nor had the Level 2 provider been asked for information about those complainants. The Level 2 provider provided a list of those complaints (with their complaint reference numbers) and for each one questioned whether it was a genuine complaint. For one of the complaints, the Level 2 provider noticed that it did not have a complaint reference allocated to it and it queried why this MSISDN had been contacted by the Executive. The Level 2 provider stated that the Executive had either contacted these individuals with graphic screenshots that may embarrass and infringe their right to privacy, or it had simply not followed up on complaints made and was therefore not protecting the public in the way it should have done. In summary, the Level 2 provider stated that the Executive had created a dangerous precedent.

In relation to the third reason raised by the Executive, the Level 2 provider stated that it had not charged consumers more than the advertised price. It stated that it was clear from the message logs that some MSISDNs had a retried billed message where it had not received a positive billed status receipt. The Level 2 provider explained that once it sent a billed message, it was completely reliant on the Mobile Network operator and the relevant Level 1 provider to return a positive billed receipt, if it did not receive this then the billing messages were retried as its system would identify these messages as not billed.

The Level 2 provider understood that the Executive has received confirmation from the complainant and the Mobile Network operator that these messages were billed however it had not received a positive receipt and was therefore unaware that was the case. It stated that it was unfortunate but it could happen for a number of reasons which were beyond its control.

The Level 2 provider stated that when the price point of Service shortcode 88150 was due to be increased it had already made changes to decrease the number of messages to be sent on the relevant dates that had been provided to it by the Level 1 provider. However, the changes took place by some Network operators earlier than it had been told by the Level 1 provider, which was completely outside of its control. The Level 2 provider supplied an extract of an email that it had received from Veoo notifying it of the dates that changes to the price point would be made.

The Level 2 provider stated that it adhered to the information given by the Level 1 provider and it had no reason to doubt that this information was correct. In light of this, the Level 2 provider invited the Executive to withdraw this part of the breach. It expressed its disappointment that the Executive had not verified this information.

In relation to the fourth reason raised by the Executive, the Level 2 provider stated that the message logs containing opt-ins that pre-dated 23 September 2014 were due to a technical issue that it had encountered with its server, as data was being incorrectly reported as it was pulled from the system due to a "bad configuration". It stated that the system was not updated to the correct date and time or the correct stamp order. The system retrieves values for a given date or time type in a standard output format, but it would always attempt to interpret other formats that may have been supplied. Date parts must always be given in year-month-day order, rather than in the month-day-year or day-month-year orders commonly used elsewhere. Where dates had been provided in an unexpected format, the system would attempt to convert this into a valid date but in some cases it inserted the wrong dates. In an effort to rectify this, a member of the Level 2 provider's staff had incorrectly inserted the wrong dates when the message logs were pulled from the system.

3. The Tribunal considered the Code, Guidance and all the evidence before it, including the written submissions made by the Level 2 provider.

In respect of reason one raised by the Executive, the Tribunal noted that the Level 2 provider had stated that it was using the third party Offline Version in conjunction with its own in-house system to verify consent to charge. However, the Tribunal noted that the Level 2 provider had not provided any evidence of consent to charge. Notwithstanding this, evidence from these sources was unlikely to be sufficiently robust. The Tribunal commented that the Guidance and previous Tribunal adjudications had made it clear what amounted to robust verification. Accordingly, the Tribunal was satisfied that the Level 2 provider had not provided sufficient evidence to establish that complainants had consented to be charged. Further, due to the lack of consent to charge evidence and given the consistent complainants' accounts that stated that they had not consented to be charged, the Tribunal found that, on the balance of probabilities, consumers had been charged for the Service without their consent.

In respect of reasons two and four raised by the Executive, the Tribunal considered the issue of complainant message logs purporting to show consumer opt-in's that were said to be false. In relation to the complainant message logs that purported to show an opt-in pre-Service commencement, the Tribunal commented that if the Level 2 provider's explanation was correct, the correct opt-in dates would have had to be later than 23 September, but this would have increased the frequency of the subscription messages post-23 September 2014 resulting in consumers being charged more than they should have done. Consequently, in relation to the complainant message logs that purported to show an opt-in prior to Service commencement, the Tribunal did not accept the explanation given by the Level 2 provider and was satisfied that for those complainants the Level 2 provider's logs were incorrect, and there was not a valid opt-in or consent to charge.

In relation to the category three complainant message logs, the Tribunal noted that numerous complainant message logs provided by the Level 2 provider showed an unusual pattern of failed messages following the consumers' purported opt-in and this was not reflected in the Verifier's logs for the same complainants. However, the Tribunal also noted that the message logs provided by the Level 2 provider generally matched the logs supplied by the Level 1 provider and that it was likely that the Level 2 provider had obtained the information in its logs from the Level 1 provider. Consequently, the Tribunal concluded that it was not satisfied, on the balance of probabilities, that the logs supplied by the Level 2 provider were false and it did not find that there had been a breach of rule 2.3.3 in respect of the category three complainant message logs on the basis that those logs had been falsified.

In respect of reason three, after consideration of the itemised telephone bills from two complainants and a message log from a Mobile Network operator, it was satisfied that some consumers had been charged twice for the same subscription. The Tribunal found that those consumers would not have consented to two charges for the same subscription and accordingly had been charged without their consent.

The Tribunal noted the Level 2 provider's explanation regarding the change in price point of Service shortcode 88150 and that its explanation had been corroborated by Veoo. Accordingly, whilst it appeared some consumers may have been charged more than the advertised price, in the circumstances, it did not find it appropriate to uphold the breach for this reason.

Accordingly, for the reasons outlined above, the Tribunal found that the Level 2 provider had not provided evidence which established consumers' consent and that consumers had been charged without their consent. The Tribunal upheld a breach of rule 2.3.3 of the Code.

Decision: UPHELD

ALLEGED BREACH 2

Paragraph 4.2.4

“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 submitted that the Level 2 provider had breached paragraph 4.2.4 of the Code for the following reasons:
 - i. Message logs supplied by the Level 2 provider were false;
 - ii. The Level 2 provider provided misleading information relating to the date on which robust third party verification for the Service commenced; and
 - iii. The Level 2 provider provided false information on the number of user opt-ins via the WAP route.

The Executive relied on correspondence exchanged with the Level 2 provider, complainant accounts (which are referenced in the ‘Background’ section), complainant questionnaire responses and text message logs.

Reason one – Message logs supplied by the Level 2 provider were false

- i. The date of Service opt-in in some Level 2 provider message logs predated the commencement of the Service

As referenced in the alleged breach of rule 2.3.3 of the Code, the Executive highlighted that the Level 1 provider Zamano had confirmed that the Service commenced operation on 23 September 2014, and supplied an email exchange with the Level 2 provider confirming this. Further, as noted in the alleged breach of rule 2.3.3 of the Code, the Executive had been provided with message logs by the Level 2 provider which showed Service opt-ins occurring before 23 September 2014. Given the confirmation from Zamano, the Executive submitted that it would not be possible for a consumer to opt-in to the Service prior to the date that the Level 2 provider would have had access to the Service shortcode via Zamano’s technical platform. Accordingly, the Executive asserted that any Level 2 provider message log showing an opt-in prior to 23 September 2014 must be false.

- ii. Failed chargeable Service messages listed in some of the Level 2 provider message logs were not sent (or attempted to be sent) to complainants in category three

As referenced in the alleged breach of rule 2.3.3, the Verifier provided 22 message logs to the Executive, all of which did not contain failed chargeable Service messages. The Verifier confirmed that attempts to deliver chargeable Service messages which failed would appear in its message logs. Given the absence of failed chargeable Service messages in the Verifier’s message logs, the Executive asserted that the entries in the Level 2 provider’s category three complainant message logs must therefore be false.

The Executive noted that the Level 2 provider stated at an early stage in the investigation that it did not have robust verification for the period between August and November 2014. The Executive noted however that it continued to receive complaints about consent to charge into the second 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 24 November 2014, 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 as opposed to a wider allegation of unsolicited charges.

- iii. Failed chargeable Service messages listed in some of the Level 2 provider message logs for complainants in category two were incorrectly listed as 'FAILED'

As referenced in the alleged breach of rule 2.3.3, the Executive identified several examples of category two complainant message logs supplied by the Level 2 provider which stated that chargeable Service messages had failed. However, when reviewing the corresponding itemised telephone bill and/or the Mobile Network operator's message logs it was apparent that the Service messages listed as failed in the Level 2 provider's message logs had actually been successfully transmitted to, and charged to, consumers. Given the evidence that the failed Service messages had been successfully transmitted to the MSISDNs, the Executive asserted that the failed Service message entries in the Level 2 provider's message logs must therefore be false.

Reason 2 – The Level 2 provider provided misleading information relating to the date on which robust third party verification for the Service commenced

As referenced in the alleged breach of rule 2.3.3, in response to a direction from the Executive which required the Level 2 provider to provide evidence of how it robustly verified consent to charge, the Level 2 provider confirmed the following:

“Up until the 25th of November 2014 we were using a [sic] offline version of robust verification where the 3rd party verification company would take daily mark ups of our landing pages this was also backed up by our own in house system where users were assigned a unique identification. We can confirm that all our services now use online versions of robust verification.”

The Executive understood this response to mean that the Level 2 provider did not have third party robust verification prior to 25 November 2014. The Executive also made enquiries to Veoo who advised that, as part of its due diligence, risk assessment and risk control on the Level 2 provider, it had requested evidence of Service opt-ins from the Third Party Verifier on a sample of ten Service users' MSISDNs. The Executive noted that the Third Party Verifier had supplied evidence to Veoo of Service opt-ins for the ten MSISDNs in question. Further, the Executive noted that the Service opt-in dates for the ten MSISDNs were on 29 October 2014 or 30 October 2014.

The Executive contacted the Third Party Verifier to confirm that the evidence supplied to Veoo was evidence that the PINs issued by SMS had been entered on to the Service website (i.e. robust evidence of consent to charge) and the date on which the full version of its service with the Level 2 provider commenced. The Third Party Verifier confirmed that the PINs had been entered on its “PIN-entry” system and the start date of its contract with the Level 2 provider was 6 August 2014.

The Executive submitted that the evidence of users' opt-ins on 29 October 2014 and 30 October 2014, and subsequent confirmation from the Third Party Verifier, demonstrated that it was misleading for the Level 2 provider to suggest that it did not use the “online versions of robust verification” until 25 November 2014. The Executive asserted that the Level 2 provider had systems for robust verification in place by 29 October 2014 at the latest. Further, given the 6 August 2014 start date on the contract between the Level 2 provider and the Third Party Verifier, the Executive submitted that, on a balance of probabilities, robust verification was available to the Level 2 provider since the stated commencement date for the Service, contrary to statements made by the Level 2 provider during the course of the investigation.

The Executive stated that it viewed the Level 2 provider's lack of evidence of robust verification of the Service opt-in for the complainants as more serious than simply not having

third party robust verification in place, because the Level 2 provider was aware of the requirement and did indeed appear to have used it for a sample of consumers. However, the Level 2 provider had not used the third party verification available to it to robustly verify the Service opt-in of all consumers.

Reason three – The Level 2 provider provided false information on the number of user opt-ins via the WAP route

The Executive noted that the Level 2 provider had confirmed that there were two Service opt-in routes; a WAP opt-in route and an MO opt-in route. The Executive sought clarification from the Level 2 provider regarding the proportion of users who opted in via each method of entry.

On 5 June 2015 the Level 2 provider confirmed in relation to the WAP opt-in route, “From the launch of the service we have 9896 online and offline [Third Party Verifier] subscribers.” In relation to the MO route into the Service, the Level 2 provider stated, “We have 228 verifiable subscribers.”

Following this, the Executive directed the Level 2 provider to provide a monthly breakdown of opt-ins via the WAP and MO routes. On 23 June 2015 the Executive received the following information:

“Please see below wap opt in subscribers for Newbabes service, we do not have many MO subscribers as we did not promote an MO based service.

Month	WAP Subscribers
Sept	75
Oct	326
Nov	1409
Dec	2478
Jan	2216
Feb	34
Mar	24
Apr	43
May	30”

The Executive noted that the total number of WAP opt-in consumers was stated to be 6635. The Executive noted the discrepancy in the number of WAP opt-ins to the Service detailed in the Level 2 providers’ responses, and submitted that clearly one of the responses supplied by the Level 2 provider was wrong.

The Executive asserted that, for the reasons listed above the Level 2 provider has provided inaccurate, false or misleading information to PhonepayPlus 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.

In response to questioning from the Tribunal, the Executive confirmed that in relation to the number of WAP opt-ins to the Service, it was not aware of an advantage that the Level 2 provider would gain from providing different figures to the Executive.

Further, the Executive was asked to guide the Tribunal through several examples of message logs provided by the Level 1 and Level 2 providers. The Executive submitted that the logs provided by Zamano and the Level 2 provider were generally the same, albeit there were some entries in the logs that were different. For example, the Executive highlighted two examples where spend reminders were listed as “SENT” on the Level 2 provider’s log but on

the Zamano logs they were listed as “NOT DELIVERED”. The Executive also highlighted two examples where the Level 2 provider’s logs showed an opt-in before the Service commencement date but the Zamano logs had an opt-in date post Service commencement. In addition, the Executive noted that logs provided by Zamano prior to the service of the breach letter were largely the same at the Level 2 provider’s logs, and where the Level 2 provider’s logs showed a string of failed messages, Zamano’s log also did. However, the Executive confirmed that it had requested message logs from Zamano after service of the breach letter but those logs had not shown repeated failed messages and they differed substantially to the Level 2 provider’s logs for the same complainants.

The Executive was asked to confirm if Level 2 providers would generally compile its message logs from information provided by a party higher up the value chain, such as a Level 1 provider. The Executive confirmed that it believed that was the case.

2. The Level 2 provider did not accept that it had acted in breach of paragraph 4.2.4 of the Code and it addressed each of the reasons for the alleged breach in turn.

In relation to the first reason raised by the Executive, the Level 2 provider stated that the message logs that pre-dated 23 September 2014 were due to a technical issue that it had encountered on its server. As it had explained under the breach of rule 2.3.3, data was pulled from its server incorrectly due to an incorrect configuration. The Level 2 provider highlighted that this problem only existed on message logs for consumers that had subscribed in the early part of the server being commissioned.

The Level 2 provider reiterated that just because the Verifier could not see the messages sent in its logs, it did not mean that they were not sent by the Level 2 provider, as a breakdown in sent messages could occur anywhere between its platform and the Level 1 provider’s platform and the Level 1 provider’s platform and the Network operator’s platform. The Level 2 provider asserted that it had sent the messages and it had not attempted to persuade the Executive of anything other than the fact that this was a technical issue.

The Level 2 provider submitted that it had not incorrectly listed any messages that had failed. If it did not have a positive delivery receipt for the messages, they would be marked as failed. It stated that the Executive should be familiar with the fact that if a Network operator has not sent a positive delivery receipt then the message is flagged as failed, and this can be for a variety of reasons, as had previously been explained.

In relation to the second reason raised by the Executive, the Level 2 provider described this as a misunderstanding. It stated that it had contracts in place with the Third Party Verifier but the system was not fully operational until it fully marketed the Service after 25 November 2014. In the interim, the system had been live to do promotional testing.

In relation to the third reason raised by the Executive, the Level 2 provider acknowledged that the Executive had been provided with two different figures for the WAP opt-ins, but it could not see any reason why the Executive would think that it had so done so on purpose. The Level 2 provider stated that this was an error on its part and no more than that.

3. The Tribunal considered the Code, Guidance and all the evidence before it, including the Level 2 provider’s written submissions.

In respect of reason one, as outlined in the Tribunal’s reasoning for the breach of rule 2.3.3 of the Code, the Tribunal found that the Level 2 provider had provided false message logs for those complainants that had a purported opt-in before the Service commencement date. The Tribunal commented that, whatever the reason for the consumer’s opt-in appearing to

be before the Service commencement date, it was clear that this could not be accurate. Further, the Tribunal noted that there were several examples of failed chargeable messages being recorded as failed on the Level 2 provider's message logs, yet consumers' itemised telephone bills and a Mobile Network operators record indicated that the messages had been successfully sent and charged. Accordingly, the Tribunal was satisfied that the Level 2 provider had supplied inaccurate information to the Executive, and was satisfied that a breach of paragraph 4.2.4 of the Code had occurred for these reasons.

For the reasons outlined in the breach of rule 2.3.3 of the Code, the Tribunal was not satisfied, on the balance of probabilities, that the allegation in relation to falsification of log entries showing repeated failed chargeable Service messages had been made out.

In respect of reason two, the Tribunal noted the Level 2 provider's explanation regarding the provision of information concerning the date robust third party verification had commenced and that it had stated that its explanation had been misunderstood. Nonetheless, the Tribunal found that the information provided by the Level 2 provider had been misleading and therefore was satisfied that a breach of paragraph 4.2.4 of the Code had occurred for this reason.

In respect of reason three, the Tribunal noted the information supplied by the Level 2 provider in relation to the number of WAP opt-ins to the Service. It paid regard to the fact that there was unlikely to be any benefit to the Level 2 provider in providing false information in this regard. It was willing to accept that the discrepancy in the information provided by the Level 2 provider had been in error and in those circumstances, did not find it appropriate to uphold the breach for this reason.

Accordingly, for the reasons detailed above, the Tribunal upheld a breach of paragraph 4.2.4 of the Code.

Decision: UPHELD**ALLEGED BREACH 3****Rule 2.3.12(d)**

"For all subscription services, once a month, or every time a user has spent £17.04 plus VAT if that occurs in less than a month, the following information must be sent free to subscribers:

- (i) the name of the service;
- (ii) confirmation that the service is subscription-based;
- (iii) what the billing period is (e.g. per day, per week or per month) or, if there is no applicable billing period, the frequency of messages being sent;
- (iv) the charges for the service and how they will or can arise;
- (v) how to leave the service; and
- (vi) Level 2 provider contact details."

1. The Executive submitted that the Level 2 provider had breached rule 2.3.12(d) of the Code as subscription reminder messages had not been issued to some complainants.

The Executive relied on correspondence from the Level 2 provider and complainant accounts (which are referenced in the 'Background' section).

The Executive noted that some complainants stated that they recalled receiving Service text messages, however they did not realise they were incurring Service charges until they viewed their telephone bill. The Executive was concerned that a lack of awareness of the Service charges on the part of complainants may have indicated that Service spend reminders were not being issued as required by rule 2.3.12(d) of the Code.

The Executive directed the Level 2 provider to provide clarification on the issuance of spend reminder messages. On 5 June 2015 the Level 2 provider stated:

“We understand the point the executive has raised here, since we have not received a positive status of these messages, our system is designed to recognise these as ‘SENT’. Moving forward, our programmers are implementing the change to reflect these as failed rather than sent.”

The Executive submitted that, notwithstanding the attempt by the Level 2 provider to issue spend reminders to complainants, given that the Level 2 provider had not received a “positive status” for the spend reminder messages, and the apparent admission from the Level 2 provider that failing to receive a “positive status” amounted to confirmation that the spend reminder message had not been delivered to the complainant, the Level 2 provider was on notice that such spend reminder messages were failing to be delivered. In failing to deliver spend reminder messages to complainants when required by the Code, the Level 2 provider had acted in breach of rule 2.3.12(d) of the Code .

The Executive therefore asserted that, for the reason listed above, the Level 2 provider had failed to issue spend reminder messages to complainants when required.

In response to questioning from the Tribunal, the Executive confirmed that it had obtained message logs from the Level 1 providers to ascertain whether spend reminders had been sent. The Executive referred the Tribunal to the Zamano message logs for the complainants and clarified that generally spend reminders appeared to have been sent to the complainants in accordance with the Code, in contradiction with the logs supplied by the Level 2 provider, which appeared to show no spend reminder messages being sent. However, the Executive confirmed that there were some examples in Zamano’s logs where spend reminders were not sent as they should have been.

2. The Level 2 provider denied that it was in breach of rule 2.3.12(d) of the Code and stated that it had generally sent the spend reminder messages to consumers in accordance with the Code but it acknowledged that there will have been instances when errors occur in the line of messages sent and delivered. The Level 2 provider commented that it was surprised that the Executive had not verified with the Level 1 providers if spend reminder messages had been sent.
3. The Tribunal considered the Code, Guidance and all the evidence before it, including the Level 2 provider’s written submissions.

The Tribunal noted the Level 2 provider’s submission that it had generally sent spend reminders but there had been problems with messages being sent and delivered. The Tribunal noted that the message logs provided by the Level 2 provider and Zamano generally matched but in relation to spend reminder messages there were differences and Zamano’s logs indicated that spend reminders had been sent more frequently. That said, the Tribunal also noted from Zamano’s message logs that there were instances where spend reminders had not been sent in accordance with the Code. Accordingly, the Tribunal found that spend reminders had not been sent every month and it upheld a breach of rule 2.3.12(d) of the Code.

Decision: UPHELD

SANCTIONS

Initial overall assessment

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

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 criterion:

- The Level 2 provider charged consumers without their consent and did not provide satisfactory evidence establishing consent.

Paragraph 4.2.4 – Provision of 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 criterion:

- The Level 2 provider supplied inaccurate and misleading information in relation to a case that concerned a serious issue of consent to charge.

Rule 2.3.12(d) – Subscription spend reminders

The initial assessment of rule 2.3.12(d) of the Code was **serious**. In determining the initial assessment for this breach of the Code the Tribunal applied the following criteria:

- Serious cases have a clear detrimental impact, directly or indirectly, on consumers and this breach has a clear and damaging impact on consumers; and
- The costs incurred by consumers may have been higher, and the service had the potential to generate higher revenues, as a result of the breach.

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 did not find any aggravating factors.

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

- The Level 2 provider stated that it had ceased all advertising for the Service once it had received correspondence from the Executive regarding its concerns.

The Level 2 provider's evidenced revenue in relation to the Service was in the range of Band 3 (£250,000 - £499,999). The Tribunal noted that the majority of the WAP opt-ins and therefore a significant amount of the revenue was generated outside the period of the breach of rule 2.3.3 of the Code.

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 £120,000;
- 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%