

Tribunal meeting number 186 / Case 1

Case reference: 77717
Level 2 provider: Crowtel Ltd. (UK)
Type of service: "Saucy-Babes" glamour video subscription service
Level 1 provider: Zamano Solutions 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 operating on shortcode 84508 (the "Service").

The Level 2 provider for the Service was Crowtel Ltd (the "Level 2 provider"). The Level 2 provider has been registered with PhonepayPlus since 5 January 2015.

The Level 1 provider for Service shortcode 84508 was Zamano Solutions Ltd. ("Zamano"). Zamano has been registered with PhonepayPlus since 3 June 2011.

The Service

The Service was stated to be a glamour video subscription service charged at £4.50 per week. Consumers entered the Service via a Wireless Application Protocol ("WAP") opt-in. The Level 2 provider confirmed that the Service commenced operation on 21 May 2015 and was currently operational. Zamano stated that the Service commenced operation on shortcode 84508 on 20 May 2015. The Level 2 provider registered the Service with PhonepayPlus on 14 January 2016.

The Level 2 provider supplied the following description and promotional material for the Service:

"We operate a weekly subscription service were our customers can subscribe to receive unlimited access to our unique glamour content for £4.50 per week. Our service is promoted through banner adverts which are strategically placed on websites similar to the content we provide to get the most out of our marketing budget. Once the banner is placed on these websites, customers have the option to click on the banner if our service interests them or simply ignore the banner if this is not something they wish to participate in. If the banner catches the customer's eye and they decide to click on it for more details they are forwarded to our call to action page which lets the customer know all the relevant details they would need to know prior to subscribing to our service, this includes the following:

- *The name of our service*

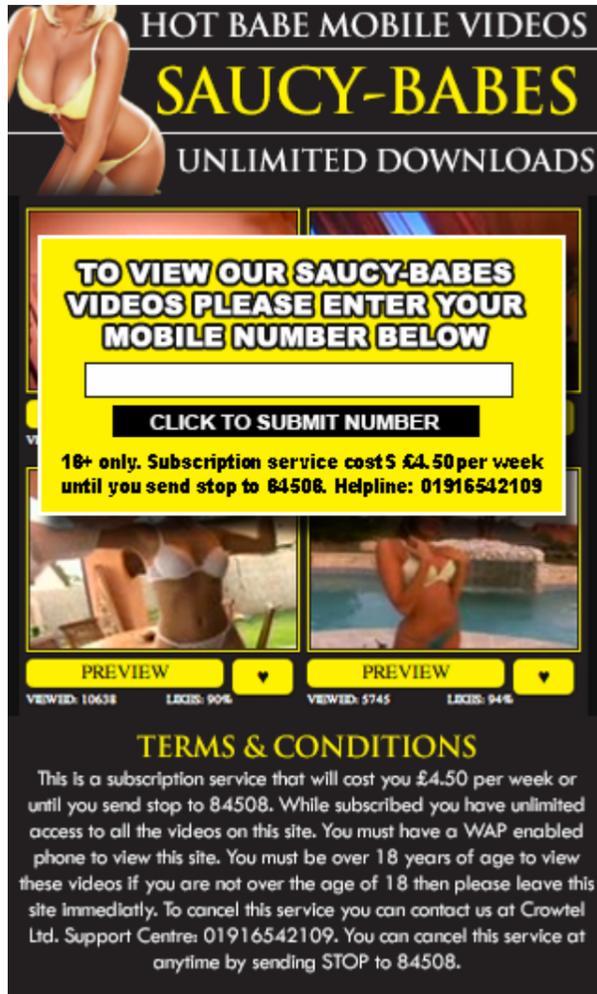


- *Our company name*
- *The cost of our service and the frequency of the billing.*
- *Opt in information*
- *Opt out information*
- *Our customer support details*

Now that the customer is up to speed with how our service operates and costs they can decide, at this stage, if they wish to follow the steps to subscribe to the service and receive unlimited access to our unique glamour content or not. If the customer decides to continue with the subscription process they simply enter their mobile number onto our call to action page as requested and if they do not wish to subscribe to the service they can simply leave our call to action page. When the customer enters their mobile number into our call to action page they are sent a free message from ourselves which contains a URL. The customer then opens the URL and is now on our subscription confirmation page that again displays all the relevant details they would need to know prior to subscribing to the service. The customer is then asked to click to subscribe to the service to get access to our unique glamour content and subscribe to the service. At this point the customer is now subscribed and given direct access to our content, a free join message is also automatically sent through to the customer which confirms that the customer is subscribed.

Now that the customer is an active subscriber of ours the billing mechanism is activated and the customer is sent a billing message 15 seconds after the join messages has been sent, the billing will then continue every week. The customer will also receive a monthly reminder message confirming that they are an active subscriber to our service and details of how to opt out if they choose to do so. If at any point the customer wishes to cancel their subscription at anytime all they need to do is either text in stop to our shortcode or contact our customer support team, all these details on how to do so are explained in the billing messages the customer receives every week as well as the reminder message the customer receives every month. Once the customer is unsubscribed they are sent a free confirmation message of this and then made inactive on our system to prevent any billing messages going out to the customer until they active another subscription with us.”

Examples of advertised banners:



HOT BABE MOBILE VIDEOS
SAUCY-BABES
UNLIMITED DOWNLOADS

TO VIEW OUR SAUCY-BABES VIDEOS PLEASE ENTER YOUR MOBILE NUMBER BELOW

CLICK TO SUBMIT NUMBER

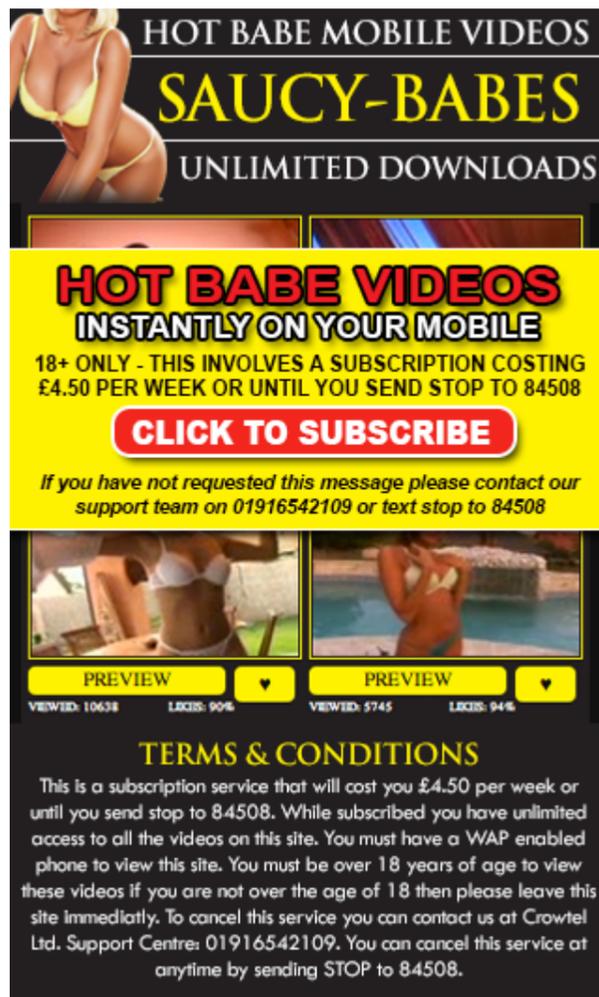
18+ only. Subscription service cost \$ £4.50 per week until you send stop to 84508. Helpline: 01916542109

PREVIEW  **PREVIEW** 

VIEWED: 10638 LIKES: 906 VIEWED: 5745 LIKES: 946

TERMS & CONDITIONS

This is a subscription service that will cost you £4.50 per week or until you send stop to 84508. While subscribed you have unlimited access to all the videos on this site. You must have a WAP enabled phone to view this site. You must be over 18 years of age to view these videos if you are not over the age of 18 then please leave this site immediately. To cancel this service you can contact us at Crowtel Ltd. Support Centre: 01916542109. You can cancel this service at anytime by sending STOP to 84508.



HOT BABE MOBILE VIDEOS
SAUCY-BABES
 UNLIMITED DOWNLOADS

HOT BABE VIDEOS
INSTANTLY ON YOUR MOBILE

18+ ONLY - THIS INVOLVES A SUBSCRIPTION COSTING
 £4.50 PER WEEK OR UNTIL YOU SEND STOP TO 84508

CLICK TO SUBSCRIBE

*If you have not requested this message please contact our
 support team on 01916542109 or text stop to 84508*

PREVIEW VIEWED: 10638 LIKES: 90%

PREVIEW VIEWED: 5745 LIKES: 94%

TERMS & CONDITIONS

This is a subscription service that will cost you £4.50 per week or until you send stop to 84508. While subscribed you have unlimited access to all the videos on this site. You must have a WAP enabled phone to view this site. You must be over 18 years of age to view these videos if you are not over the age of 18 then please leave this site immediately. To cancel this service you can contact us at Crowtel Ltd. Support Centre: 01916542109. You can cancel this service at anytime by sending STOP to 84508.

Summary of complaints

The Executive received 181 complaints concerning the Service between 29 May 2015 and 15 May 2016.

Complainants variously alleged that the Service charges were unsolicited. A sample of complainant accounts is provided below:

"I have been receiving text messages in the format above from 84508 to which I have text STOP as it mentions in the text message. I have received my bill and queried why it was so high, Vodafone confirmed I had been charged £18 for 4 premium text messages from 84508."

"I have no idea who this company is yet they have billed me twice for £4.50 per time. This £9 charge appeared on my last bill and I am unhappy with the outcome from phoning what I believe the company to be."



"I was receiving texts from saucy babes. I did not authorise payments to be taken from my phone account."

"I have never signed up to this and when I received the first text I replied STOP as instructed as I had no interest in its content."

"I received a link via text and there was no short code no "free msg" just the letter "e" i did not click the link as did not know what it was. Just kept the message on my phone incase I was charged checked my phone bill everyday since and had no charges. Received a link again but this time asking me to text back saying stop to unsubscribe so I text back stop then checked my bill today and charged for receiving the text and also for texting back to end the subscription when i never requested it in the first place! Tried to contact provider via email - no response... called 0191 help number and it just plays music constant - email again - no response." [sic]

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 7 June 2016. Within the breach letter the Executive raised the following breaches of the PhonepayPlus Code of Practice (the "Code"):

- Rule 2.3.3 – Consent to charge (12th Edition)
- Rule 3.4.14(a) – Failure to register a number (13th Edition)

The Level 2 provider responded on 21 June 2016. On 7 July 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 provider;
- Complainant message logs from the Level 2 provider;
- Guidance on "Privacy and Consent to Charge" (12th Code edition) and on "Consent to Charge" (13th Code edition);
- Screenshots from the PhonepayPlus registration database; and

- The breach letter of 7 June 2016 and the Level 2 provider's response of 21 June 2016 including the attached refund spreadsheet.

SUBMISSIONS AND CONCLUSIONS

ALLEGED BREACH 1

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 because consumers had been charged without their consent and the Level 2 provider had been unable to provide evidence which established that consent. The Executive relied on the content of PhonepayPlus Guidance on 'Privacy and consent to charge' (12th Code edition) and Guidance on "Consent to Charge (13th Code edition) (the "**Guidance**"), correspondence exchanged with the Level 2 provider and complainant accounts (which are referenced in the "Background" section above). The Executive asserted 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 Executive submitted that the Level 2 provider was required to hold robust consent to charge evidence for WAP opt-ins. The Executive asserted that the Guidance made it clear that all charges must be robustly verifiable. Although the Guidance was not binding on providers, the Executive submitted that where a provider fails to follow Guidance there was an expectation that it will take equivalent alternative steps to ensure that it fulfils PhonepayPlus' expectations (and complies with the Code).

On 6 July 2015, the Executive had written to the Level 2 provider requesting general Service specific information, including the opt-in information for a sample of MSISDNs. On 13 July 2015, the Executive received the Level 2 provider's response, but noted that no evidence of consent to charge had been provided.

As a result, the Executive had written to the Level 2 provider on 23 July 2015 seeking clarification on how it robustly verified WAP opt-ins to the Service. On 29 July 2015, the following response had been received:

"Our service are verified internally, customers must follow the steps outlined in question 1 and 2 of the initial assessment document prior to subscribing to the service. Once the customer has confirmed subscription the date and time is stored on our system along with the pin they used to activate the service."

On 28 April 2016, the Executive wrote to the Level 2 provider seeking further clarification on how opt-ins to the Service were stored, and stored so that they categorically could not have been interfered with. The Executive attached a spreadsheet of MSISDNs and requested that the Level 2 provider supply evidence of how it was able to robustly verify consent to charge for all the MSISDNs.

On 10 May 2016 the following response was received:

“The data is stored locally on our secured database with no external access to the data. The database is not accessible externally and as result cannot categorically be interfered with.”

“All of our subscribers go through a 2-step authentication process on our database to become a subscriber of any of our services. When a customer requests one of our services by entering their mobile number into our landing page, they are issued with a provisional pin which allows the customer to continue the subscription request. Once the free message is sent to the customer with the provisional pin, we store this information in our database. As this is a unique provisional pin allocated to a specific customer we can record if/when the url link has been opened and if/when the subscription process has been completed when the customer clicks ‘CLICK TO ENTER’. When the customer completes the subscription process we then record this information on our database and generate a unique subscriber pin for the customer. Before a join message is sent to a customer we have a script in place that does one final check and only when there is an entry in the database which matches the prerequisites, will the system allow a join message to be sent to a customer and the billing process begin.

This is a process that continues throughout the lifespan of the customer’s subscription. When we are processing the number for billing, the database is first interrogated to make sure the number has completely opted-in and is not blocked.”

Examples of the ‘provisional and subscriber PIN numbers’ which were supplied by the Level 2 provider as evidence of consent to charge are attached at **Appendix A**.

The Executive asserted that although the Level 2 provider made reference to ‘provisional and subscriber PIN numbers’ being used, the Service did not use the PIN-protected opt-in route referred to within the Guidance. The Executive submitted that data relating to the complainants’ opt-ins was not held by a third party, nor was it held in a way which meant it categorically could not have been tampered with since its creation, as the Level 2 provider held the data internally.

In response to questioning by the Tribunal in relation to complainant MSISDN *****805, the Executive noted that the Level 2 provider had stated in response to a preliminary enquiry that this number had not been charged by the Service, but referred to the complainant’s description of events which clearly identified the Level 2 provider as the organisation which had charged them without their consent.

For the reasons set out above the Executive asserted that the information supplied by the Level 2 provider to verify that the complainants opted into the Service via WAP was not sufficiently robust. As the Level 2 provider relied upon this information as evidence of complainants’ opt-ins, the Executive submitted that there was no evidence that consumers opted into the Service. Accordingly, the Executive asserted that the Level 2 provider had acted in breach of rule 2.3.3 of the Code.



2. The Level 2 provider admitted the breach in part. The Level 2 provider highlighted its willingness to co-operate with the Executive and stated that it wished to explain its point of view on the Guidance and Rules, which it accepted might have been incorrect, to some extent. The Level 2 provider submitted that it had attempted to follow PhonepayPlus' regulations on premium services with good will and a positive approach. It had wished to offer a high quality mobile service to consumers and it had never been its intention to infringe PhonepayPlus' directions. The Level 2 provider submitted that its belief was that this matter could have been dealt with as a Track 1 matter. It referred to Paragraph 4.2.9 of the Code which states:

"If further relevant information comes to light during the course of an investigation, and the case has not yet been placed before a Tribunal, PhonepayPlus may change the investigation procedure used, or withdraw an allegation of any or all breaches, at its discretion. If the investigation procedure is so changed PhonepayPlus shall allow adequate time to the party concerned to deal with the matter."

The Level 2 provider submitted that it had never been the subject of a Track 1 procedure, or any other compliance review or procedure. It considered this to be a positive point, bearing in mind the alleged breach and the case history.

The Level 2 provider submitted that it had provided the Executive with a service description and an opt in flow method review in July 2015, and had trusted that this was accepted as no further correspondence had been received by it until April 2016. The Level 2 provider stated that it had also provided the Executive with explanatory notes in its May 2016 response and it had hoped that, should any issues arise, these could be worked out together with PhonepayPlus in order to achieve a mutual goal of consumer protection.

The Level 2 provider accepted that it might have committed an oversight when it came to its interpretation of the Code and the Guidance and, should this be the case, it apologised for this and it could provide an assurance that, if it was directed by the Executive to implement a third party opt in flow, it would be willing to implement this immediately. It submitted that a Track 1 Action Plan would be likely to be implemented by it much more promptly, rather than it having to proceed through a time consuming Tribunal process. The Level 2 provider therefore asked the Executive to proceed via a Track 1 Action Plan, referring to PhonepayPlus's mission statement, which outlined an intention to work with providers and industry as a whole in order to build a healthy market. The Level 2 provider submitted that it would comply with any necessary set of actions in order to remedy the alleged breach and to prevent any repetition and it would work to meet any deadline set.

The Level 2 provider stated that it wished to explain the background to its misinterpretation of the Code and Guidance in relation to the issue of consent to charge. It referred to section 1.3 of the Guidance which deals with the need for transparency in pricing information and to paragraph 2.2.4 of the Code which read:

“All written information which is material to the consumer’s decision to purchase a service must be easily accessible, clearly legible and presented in a way which does not make understanding difficult. Spoken information must be easily audible and discernible”.

The Level 2 provider asserted that it had adhered to paragraph 2.2.4 in full. It stated that the promotional material it had provided to the Executive indicated both pricing information and billing frequency, together with Customer Support contact details and STOP guidance. The Level 2 provider indicated that should the Executive recommend any changes to the material, it would be happy to implement these changes straight away.

The Level 2 provider referred to paragraph 2.1 of the Guidance which read:

“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 initiated by anything else other than a consumer legitimately consenting, and cannot have been interfered with since the record was created.”

The Level 2 provider confirmed that its view was that the consent to charge for every single subscriber was properly verifiable in that the subscription could not have been initiated by anything other than the consumer interacting with the advertisement and willingly to enjoying the service content at an affordable weekly fee. The Level 2 provider submitted that records of such consent could not be interfered with, simply because they were stored locally on its secured database with no external access to the data. The Level 2 provider submitted that the secured database was not accessible externally and, as a result, categorically could not be interfered with. The Level 2 provider stated that, should the Executive find its secured database inefficient or not sufficient, it would immediately change the way that consent was recorded and stored.

The Level 2 provider stated that it noted the risks associated with the entering of a mobile number on a website, as described at section 2.6 of the Guidance, which read:

“Some services are initiated by a consumer entering a mobile number on a website, or a mobile website (i.e. a website browsed on the mobile handset). This is most frequently where the consumer browses the site on a laptop or tablet, or where they browse via wi-fi – and not their mobile network’s internet provision – on their phone. Consumers do not always appreciate that entering their number can result in a charge being generated to their mobile device, or that the entry of their number can be understood as being consent to future marketing by the provider concerned.”

The Level 2 provider submitted that it had developed a safeguard to avoid the risk. It had not advertised the service for desktop users. The Level 2 provider stated that the advertisements were only targeted at mobile phone users and, therefore, there could be no confusion about the service price or billing frequency. A consumer could not access the promotional material



from a laptop or a tablet, unless they were using a mobile emulator, which the Level 2 provider stated with 100% certainty was not likely in the case of a common consumer. The Level 2 provider asserted that, with all honesty it could not have been more prominent with the pricing information, let alone with other parts of the terms and conditions which made the consumer aware that this was a chargeable subscription service.

The Level 2 provider referred to paragraph 2.7 of the Guidance which read:

“The risk of harm is increased where a consumer enters a mobile number belonging to someone else (either by mistake or deliberately) and generates a charge to a second – unwitting – consumer. Even if there are no chargeable messages, just free marketing messages, the second consumer often feels that their privacy has been invaded”

The Level 2 provider stated that it agreed with the risk described in paragraph 2.7. However, it submitted that it had overcome this potential harm by extending the opt-in flow to a two-step process in order to avoid any infringement of consumer privacy in the event that someone decided to fraudulently abuse a mobile phone belonging to another person. The Level 2 provider stated that its opt in flow required MSISDN input but, as a second step safeguard, the subscription commenced only once a unique PIN was identified and verified by its system. The Level 2 provider stated that the PIN structure was twofold – consisting of allocated provisional and subscriber PINs, both securely stored.

The Level 2 provider referred to paragraph 2.12 of the Guidance which read:

“Any MT message sent in these circumstances should not act as a promotion for the service itself (e.g. use its name). They should be designed and drafted as a functional tool to enable the completion of the verification process.”

The Level 2 provider submitted that the requirements of paragraph 2.12 had been met because the PIN embedded in the second step of the verification process was the actual tool to enable subscription completion. The Level 2 provider submitted that this facilitated the end user to enter the second step of the opt in process, which was shown in the second screenshot that it had provided to the Executive (above).

The Level 2 provider proposed a remedy plan in respect of the points noted above because it valued the Executive’s comment. The Level 2 provider submitted that there was still time (for a remedy plan), in order to save the Code Compliance Panel valuable time and hassle with administrative procedures. The Level 2 provider stated that it was ready and more than willing to comply with any suggestion and official direction that the Executive proposed. The Level 2 provider stated that, should the current internal verification and opt in recording system in place be insufficient to satisfy the expectations of a Level 2 provider, it would implement any necessary changes as soon as possible upon confirmation of such a requirement by the Executive.



The Level 2 provider submitted that the procedure of a preliminary investigation was not straightforward to it because it had never been the a subject of such a procedure before and it had never been its intention to break the rules. The Level 2 provider submitted that the impression it had formed was that there might be an insufficient degree of guidance from PhonepayPlus, but it also put a percentage of guilt upon itself because it should have taken the initiative to ask if the information it provided to the Executive alongside preliminary correspondence, was satisfactory or not. The Level 2 provider stated that it did not realise that this matter would turn into an allegation that the Code had been broken due to the operation of the Service. The Level 2 provider proposed a closer co-operation plan and the shifting of the procedure from the Tribunal procedure to an Action Plan. The Level 2 provider stated that it was looking forward to receiving the Executive's feedback on this matter and that it hoped for decent degree of cooperation too. The Level 2 provider stated that its reasoning behind its suggestion of an Action Plan was based upon its submission that it had followed the rules to its best available capacity, trusting that it had adhered to the Guidance because it had offered consumers the following:

- Information on the nature of the service and pricing (together with all supporting details) prior to subscription commencement
- Two-step opt in process as a true safeguard and consumer protection factor
- High standard of customer support
- High level of technical development for twofold PIN allocations
- Secure storage of consent to charge for all subscribers

The Level 2 provider also enclosed a report on consumer refunds, which it submitted should be viewed as a major mitigating factor. It had disclosed the report, even though the Executive did not ask for the report, in order to show its full will to closely cooperate to achieve consumer satisfaction.

In informal representations, the Level 2 provider repeated its previously submitted written response.

The Level 2 provider described the method of opt-in to the Service. All service subscribers joined through a two-step process. When a customer enters their MSISDN on its landing page, they are issued with a preliminary PIN which allows them to continue with their subscription request. When a free message was sent to them with the provisional PIN that was recorded on the Level 2 provider's system database. The provisional PIN was unique to each specific customer, and the Level 2 provider could record when the URL was opened. When the subscription process was completed by the consumer clicking "click to enter", the Level 2 provider recorded this information on its database and generated a unique subscriber PIN for the customer. The Level 2 provider stated that before it issues a chargeable message to the consumer it had a script which checks the PIN. Once a customer subscribed, the date and time was stored to their system with the PIN. The database was securely stored locally, with no external access, so categorically could not be interfered with.



The Level 2 provider stated that its Service promotional materials, as supplied, complied with rule 2.2.4 of the Code, and indicated the billing frequency, costs, STOP guidance and customer support details. The Level 2 provider submitted that this was sufficient to make it clear to consumers that they were entering a chargeable subscription service.

The Level 2 provider acknowledged the feedback from the Executive regarding the guidance for the 12th Code and the current (13th) Code, and agreed that the merits and outcomes expected by these pieces of Guidance were similar. The Level 2 provider admitted, in part, that one could interpret the situation as unfortunate, and submitted that if there had been a breach of the Code, this was unintentional. The Level 2 provider submitted that it may have committed an oversight but if the Executive directed that it is required to have an outside party verify consumer opt-ins it would be implemented promptly.

In response to questioning from the Tribunal, the Level 2 provider confirmed it had not to date changed its process of consumer verification since its interaction with the Executive.

The Level 2 provider was asked about the purposes of the two PINs it had described. The Tribunal noted that the opt-in flow provided by the Level 2 provider did not appear to involve any step where a consumer entered a PIN which they had been sent. The Level 2 provider explained that the URL sent to every consumer was specific to them. The unique PINs for each customer enabled the Level 2 provider to see that the subscription came from that person, so they could say it was the actual use of the phone. It could therefore keep track that it was that person and that phone that had signed up. The Level 2 provider was unable to explain whether or not the subscriber PIN was also sent to the consumer, as it did not have all the information to hand.

The Level 2 provider referred to the spreadsheet of consumer refunds it had supplied as evidence that it had refunded consumers.

3. The Tribunal considered the Code and all the evidence before it. The Tribunal considered the Guidance on Privacy and Consent to Charge (12th Code edition). The Tribunal noted that the Guidance stated that *"...it is essential that providers can provide robust evidence for each and every premium rate charge. 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...was created."* The Tribunal noted that the Guidance set out factors which could contribute to robustness which included *"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);"* *"Records are taken and maintained by a third-party company which does not derive income from any PRS... 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;"* and *"any other evidence which demonstrates that the opt-in cannot be interfered with."*



The Tribunal also considered the Guidance on Consent to Charge (13th Code edition), which came into force on 1 July 2015. The Tribunal noted that the relevant sections of this Guidance were similar to the previous Guidance. The Tribunal noted at para. 2.10 the example given of a way to robustly verify consent to charge where charges were generated by entering a mobile number on a website. This example would normally involve (as one part of the system) records being taken and maintained by a third-party company which did not derive income from a service. The Tribunal considered that this Guidance was also explicit that robust verification involved the creation of a clear audit trail that could not have been interfered with since the record was created.

The Tribunal considered the submissions of the Level 2 provider. Whilst the Level 2 provider had stated that its records were secure against external interference, what the Level 2 provider should have ruled out was the possibility of tampering with the records by the Level 2 provider itself. The Tribunal considered that a system in which consumers could click on a unique URL and then click to enter on the web page which then appeared, was not by itself sufficient to robustly verify consent to charge for all those charged by the Service. It was not clear how the two PIN system alone created a clear audit trail that categorically could not have been interfered with since records were created, since the consumer did not enter the provisional PIN into the website, there was no evidence that the second subscription PIN was sent outside the Level 2 provider's own systems, and there was no involvement of a sufficiently independent third party company in this process.

Accordingly the Tribunal did not view the Level 2 provider's records of opt-ins as sufficient to establish that the complainants had consented to be charged.

The Tribunal noted that the Level 2 provider had admitted the breach in part, and had submitted that it was willing to make changes if directed to do so by the Executive. In respect of this submission, the Tribunal commented that providers were required to pro-actively take steps to comply with the Code and were themselves responsible for compliance with the Code. The Executive was not required to direct Level 2 providers individually on what steps they should take. The Tribunal noted that the Level 2 provider could have consulted the Guidance, and taken compliance advice if it was unsure of what it had to do to comply with the Code.

The Tribunal examined the preliminary enquiry in respect of MSISDN *****805 and noted that there appeared to have been a typographical error when the digits were transferred from the complaint to the enquiry, which might explain the Level 2 provider stating that this number had not been charged by the Service. Nevertheless, there was sufficient evidence in respect of other complainants to uphold the alleged breach.

Consequently, for the reasons advanced by the Executive, the Tribunal was satisfied that the Level 2 provider had not provided evidence which established consumers' consent to be charged for the Service. Accordingly, the Tribunal upheld a breach of rule 2.3.3 of the Code.

Decision: UPHELD

ALLEGED BREACH 2

Para. 3.4.14(a)– Failure to register a number

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

1. The Executive submitted that the Level 2 provider had acted in breach of paragraph 3.4.14(a) of the Code as it had failed to provide PhonepayPlus with relevant details to identify the Service operating on shortcode 84508 to consumers for a period of time when the Service was operational. Furthermore, the Level 2 provider had failed to provide PhonepayPlus with the identity of the Level 1 providers concerned with the provision of the Service.

The Executive stated that the Code required that Level 2 providers supplied relevant details to identify services to consumers. The PhonepayPlus Registration Scheme was in place to facilitate providers to supply relevant details to identify their services to consumers. Once a provider had supplied details of its services, including which premium rate numbers it operated on, the details appeared on the ‘Number Checker’ section of the PhonepayPlus website, www.phonepayplus.org.uk. The Number Checker allowed consumers to enter a phone number they may not recognise on their phone bill, and find out information regarding that number.

The Executive submitted that the information supplied by the Level 2 provider showed that the Service had commenced operation on 21 May 2015. However, the shortcode 84508 had not been registered with PhonepayPlus until 14 January 2016. The Executive further submitted that, although the Service had been registered on 14 January 2016, the Level 2 provider had still not provided the identity of the Level 1 providers concerned with the provision of the Service.

In response to questioning by the Tribunal, the Executive confirmed that it had the ability to search shortcode facilities and could therefore establish who the Level 1 provider was without this information being provided by the Level 2 provider, but noted that it was nevertheless a requirement that Level 2 providers supply this information upon registration.

The Executive submitted that the information on the PhonepayPlus registration system indicated that the PRN was not registered with PhonepayPlus for more than seven months. The Executive asserted that, where services are not registered, consumers do not have the ability to access information relating to the Service, which impairs PhonepayPlus’ regulatory function. The Executive submitted that the failure to provide the requisite information to PhonepayPlus by registering the Service number was a breach of paragraph 3.4.14(a) of the Code.



2. The Level 2 provider admitted the breach in part. It apologised for an oversight at its end, which resulted from the fact that, despite its attempts to keep all administrative aspects under control, it somehow had not managed to register the short code on time. The Level 2 provider stated that its team felt very uncomfortable with the situation and that at the time of the commencement of the Service, there had been a true learning curve and pressure on them. The Level 2 provider submitted that, after the launch of the Service, most probably by error of oversight, the relevant item on the checklist had been ticked as completed. The Level 2 provider submitted that it had never been notified by PhonepayPlus that this was an issue, and it would have expected such an indication to appear on call logs received by its team. It submitted that because it had not been notified about this issue, it had trusted that everything was in order. The Level 2 provider admitted that the burden of duty was probably on its side and it apologised and confirmed that this was a lesson very well learned and remembered for the future.

In informal representations, the Level 2 provider repeated its previously submitted written response.

3. The Tribunal considered the Code and all the evidence before it, including the Level 2 provider's partial admission. For the reasons advanced by the Executive, the Tribunal was satisfied that the Level 2 provider had failed to provide all the information to PhonepayPlus required upon registration by paragraph 3.4.14(a) of the Code. Accordingly, the Tribunal upheld a breach of paragraph 3.4.14(a) 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 criteria:

- The Level 2 provider charged consumers without having reliable evidence of consent to charge;
- The nature of the breach was likely to severely damage consumer confidence in premium rate services; and
- The case had a clear and highly detrimental impact on consumers.

Rule 3.4.14(a) – Failure to register a number



The initial assessment of rule 3.4.14(a) of the Code was **serious**. In determining the initial assessment for this breach of the Code the Tribunal applied the following criteria:

- The Level 2 provider had continually failed to comply with a PhonepayPlus requirement (registration of the service number);
- The service was operated in such a way that demonstrates a degree of recklessness over compliance with the Code; and
- The nature of breach meant the service would have damaged consumer confidence in premium rate services

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 factors:

- 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 May 2015 to March 2016 was in the range of Band 2 (£500,000 - £999,999).

Having taken into account the circumstances of the case, the Tribunal concluded that the seriousness of the case should be regarded overall as **very serious**. The Tribunal did not find the mitigating factor was sufficient to make the case less serious overall, but the mitigating factor would be reflected in the sanctions imposed, which would otherwise have been more severe.

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 £150,000;
- 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 consumers, including any existing subscribers to the Service;
- a requirement that the Level 2 provider seek compliance advice on its mechanism for obtaining robust verification of consent to charge, such advice to be implemented before charging any new or existing customers for whom there is no adequate existing evidence of consent to charge, and in any event within 28 days of publication of this decision (subject to any extension of time agreed with PhonepayPlus) to the satisfaction of PhonepayPlus; 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

	A	B	C	D
1	msisdn	provisional_pin	subscriber_pin	subscriber_date
2		6e80f5450	f47fea29c	13/06/2015 12:25
3		bb3275558	29252f688	23/10/2015 14:05
4		3e5f8ce7f	cad432555	30/10/2015 14:06
5		f26a5d7ff	e214ebd09	20/06/2015 12:40
6		f8128a458	098c15f75	20/06/2015 12:40
7		f2518722f	9925ae78e	13/06/2015 12:25
8		7d91e7747	db2458401	20/11/2015 14:03
9		4f98f98be	1ea55a7fa	06/11/2015 14:03
10		379125493	b47af8c71	06/11/2015 14:04
11		0d236b6fa	dea7bafa5	25/12/2015 17:35
12		2831a8ae5	8b2e1864f	13/06/2015 12:26
13		9ec915e1b	dbd577814	31/07/2015 19:30
14		70893ee00	cc662d736	18/12/2015 14:00
15		3d08202e4	1d9fec6f9	13/06/2015 12:25
16		f3bd5e937	f10b123ec	20/11/2015 14:00
17		059fc6938	c50dc44d0	27/11/2015 14:03
18		f94e6bc1a	c4b574d1f	13/02/2016 19:45
19		6fbc2eeaa	d62b99a97	18/12/2015 14:22
20		0465b4c34	8f1f9020d	13/06/2015 12:25
21		28253424a	28253424a	20/06/2015 12:41
22		24f8e2aa0	54f53adea	26/02/2016 14:15
23		90389ab4c	4536b6170	20/06/2015 12:40
24		38da6383e	b7310ead3	01/01/2016 17:34
25		38da6383e	b7310ead3	01/01/2016 17:34
26		7c645d169	4a4dca627	05/12/2015 14:07