Tribunal meeting number 170 / Case 1

Case reference:	**29396**
Level 2 provider:	**New SMS Media Ltd (UK)**
Type of service:	**Adult/glamour video subscription services**
Level 1 provider:	**GSO MMBU (Private Company) Limited (formerly Velti DR Limited) (UK) and Veoo Limited (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 13 June 2013 and 2 September 2014, PhonepayPlus received 46 complaints from consumers in relation to adult and glamour video subscription services (the **"Service(s)"**) operated by the Level 2 provider, New SMS Media Ltd (the **"Level 2 provider"**) until January 2014 when the Services were novated to another Level 2 provider, Venture247 Limited (**"Venture247"**). The Services were operated under the names "Mobteenxx", "F**ckMeHard24", and "GlamourBabesxxx" on the premium rate shortcodes 89320 and 88150. Consumers were charged £3 or £4.50 per week depending on the Service they engaged with. The Services commenced at different times; the earliest date was in March 2012 and some continue to be operated by Venture247.

The Services were promoted online via banner advertisements or a wireless application protocol (**"WAP"**) push message which was sent to consumers. Consumers subscribed to the Services, using mobile originating (**"MO"**) opt-in or a WAP link. Consumers could also engage with the Services using an Android application (the **"Application"**) which utilised a MO opt-in.

Concerns regarding the Application were uncovered as a result of a blog article by the anti-virus vendor Kaspersky Labs ("**Kaspersky**"). The article outlined its detection of over 300 adult Android applications, deemed as "SMS Trojans", from consumers' handsets. Kaspersky provided the samples to the PhonepayPlus Research and Market Intelligence team (the "**RMIT**"), which identified concerns regarding the operation of the Application which was malicious as it suppressed the receipt of Service messages.

The investigation

During the investigation, the Level 2 provider responded to a direction for information from the Executive, but in May 2014, the Executive was advised by the Level 2 provider that it was no longer trading and all correspondence should be referred to Venture247. Novation agreements between the Level 2 provider and Venture247 confirmed that the Services had been novated on 3 January 2014. Subsequent correspondence was directed to Venture247, which responded to directions for information on behalf of the Level 2 provider. The Executive sought to obtain a direct response to its enquiries from the Level 2 provider, but it did not receive a response. For the purposes of this decision, the Tribunal noted the responses from Venture247 but also noted that Venture247 was not a party to the proceedings.

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 26 June 2015. Within the breach letter the Executive raised the following breaches of the Code:

- Rule 2.3.1 - Fair and equitable treatment
- Rule 2.3.3 - Consent to charge
- Rule 2.4.2 - Consent to market

The Level 2 provider did not respond to the breaches raised by the Executive. The Tribunal was satisfied that the breach letter had been served on the Level 2 provider and that it had received an opportunity to provide a response. On 23 July 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 between 5 November 2013 and 7 December 2013, 3 March 2014 and the associated message logs;
- Correspondence between the Executive and the Level 2 provider/ Venture247 (including directions for information and the Level 2 provider/ Venture247's responses including supporting documentation);
- A sample of complainant message logs;
- Correspondence between the Executive and the Level 2 provider regarding previous enforcement action;
- Correspondence between the Executive and a third party verifier;
- The novation agreements between the Level 2 provider and Venture247;
- PhonepayPlus Guidance on "Privacy and Consent to Charge" and "Promotions and promotional material";
- Documents relating to the service of the breach letter; and
- The breach letter of 26 June 2015.

Complaints

The majority of the complainants stated that they had received unsolicited, reverse-billed text messages but that they had not engaged with the Services. The Executive noted that 41 of the 46 complaints related to the WAP method of entry to the Services rather than the Application. Therefore, such complaints were not relevant to the breaches of the Code raised in relation to the Application. The Executive asserted that it was unlikely that consumers who had engaged with the Application would complain to PhonepayPlus as many would be unaware that they had subscribed to the Service due to the suppression of Service messages.

Extracts from a sample of complainants' accounts included:

"I started receiving messages from this number about xxxsex stuff which I have no idea who they are or where there from and I hav'nt [sic] agreed to receive them and they charge me £1:50 each msge [sic] and they send 2 together every week. I have to confess I don't look through my bills thoroughly but having now spotted this charge have. The oldest bill I can lay my hands on is from March and the messages start on 08/03/13 and from then to my current bill I have received a total of 28 messages at 1:50 each, £42 in total which I never asked for, signed up to or agreed to. I have spoken to Orange who are my provider who say they can do nothing about it, which is also ridiculous. I've read online this is a scam and if I text "stop" to the number I will get charged £10 pounds and still receive messages. Can you please help me with how to stop these messages and try to re-coup the money they have effectively stolen from me."

"My reason for my complaint is that I have not subscribed to this "Sexual Entertainment Service" premium rate service as falsely claimed by New SMS Media Ltd. New SMS Media Ltd. are

generating unsolicited and unsubscribed premium rate service texts to my private mobile number, where all messages received have been unauthorised messages to me, as the mobile phone contract holder. In recklessly, knowingly and unlawfully obtaining monies from me by deception, New SMS Media Services Ltd. have as the Communications Provider broken statutory law on at least two counts, namely: A. Breach of Condition contrary to Section 120 of the Communications Act 2003 regulating Premium Rate Services and PhonePayPlus Associated Code of practice by unlawfully subscribing me to their service when I had not subscribed B. Fraud by False Representation contrary to Section 2 of the Fraud Act 2006 by billing Virgin Media Telecoms Limited, my mobile phone Network Provider and taking payment under the pretense that I was an authorised subscriber to their Premium Rate Service when I had not subscribed to their service I would therefore respectfully request that PhonePayPlus investigates my complain about New SMS Media Ltd. premium rate services. Because PhonepayPlus Code of Practice rules have been broken, PhonepayPlus should exercise its delegated powers from Ofcom to fine New SMS Media Ltd., to bar access to their services and to bar the individuals behind this company from running."

"Sending explicit texts weekly at a charge of £1.50 each. I've never signed up for this service and I want it to stop! This month alone I've been charged £18 for this service. It's been happening for the last 3/4 months. I have online bills as proof."

The Executive received complaints from consumers that had interacted with the Services via an MO opt-in and reported receiving unsolicited charges but had not received any text messages from the Services:

"Just want to know why this company has charged me even though I have not received any messages on my phone."

"Chose service type as customer service but had no idea what to put as did not receive any texts so don't know what type of company it is.no text received, just premium text received and charges on my account online in my call history. This number has charged me many times at £1.50 a time in groups of 3 at a time for texts not prescribed to or even received. If I had not checked my account online I would still be unaware they are charging me. I have not subscribed for anything and my mobile provider said I would have to sort it out myself, they could not stop them."

Monitoring

Following the discovery of the blog article by Kaspersky, the RMIT contacted Kaspersky to request samples of the Applications it had detected and on 30 October 2013 Kaspersky provided 335 samples to the RMIT for testing. Upon analysis of the samples, 236 samples were found to target UK consumers and of these 236 applications, six were identified as relating to the Services. The RMIT conducted testing of these Applications (for the GlamourBabesxxx service) between 5 November 2013 and 7 December 2013.

The Applications were transferred to a monitoring phone (HTC Desire handset running an Android 2.2 operating system) and installed through a file manager. The RMIT followed the default Android installation process, which involved viewing the permissions before selecting "install" (**Appendix A**).

The RMIT opened the Applications and was presented with the Application landing page, on which the RMIT clicked the top right hand corner of the screen (away from the options displayed on the menus) (**Appendix B**). The RMIT noted that the whole screen was an active link which meant that

clicking any part of the screen would initiate a subscription to the Service and accordingly, the RMIT was automatically subscribed to the Service. The RMIT was subsequently charged for three mobile terminating ("**MT**") subscription messages but it did not receive any messages to the inbox of the monitoring handset, because they were suppressed by the Application. The RMIT was able to detect and intercept the suppressed messages through a debugging tool on its monitoring computer. This detected all message activity experienced by the handset and enabled the RMIT to compile a log of all incoming and outgoing messages on the handset, which it had not seen on the handset.

In addition to the monitoring of the Kaspersky samples, the RMIT monitored an Application for the F**kMeHard24 and GlamourBabesxxx Services, having obtained it by browsing the internet. The Executive noted that the monitoring evidence of 3 March 2014 did not relate to the Level 2 provider as the Service was operated by Venture247 at the time of the monitoring. Therefore, the Executive included the monitoring only as background information and did not rely on this monitoring evidence in the breaches raised.

On 3 March 2014, the RMIT searched "porn" on the Google search engine, and followed a link in the search results to the website hardsextube.com (a third party website). Whilst viewing content and selecting a thumbnail image on the website, a new browser page loaded behind the page that the RMIT was viewing. The RMIT noted that selecting a thumbnail on hardsextube.com and/or the loading of a new browser webpage triggered an automatic download of the Application in the background. The new browser webpage had the appearance of a Google Play screen and included an "install" button. However, the RMIT did not select "install" to instigate the download process but instead it visited the handset's notification area, where any new downloads would appear. The RMIT noticed that there was a file entitled "234fmh8833g.apk", which had been downloaded to the handset. Accordingly, the RMIT followed the default Android installation process, which involved confirming installation of the Application by viewing the permissions before selecting "install".

The RMIT opened the Application and was presented with an Application landing page for the F**ckMeHard24 Service. In a similar manner to the RMIT's monitoring of the Kaspersky samples, the RMIT clicked the top right hand corner of the screen (away from the menu options) and noted that the menus shown were fake as the whole screen was an active link. Therefore, by clicking any part of the Application screen an MO message was sent to the Service and a subscription was initiated. The RMIT was charged for three subscription messages which were suppressed by the Application. The RMIT repeated the monitoring session and also found an Application for the GlamourBabesxxx services which it found behaved in the same way.

SUBMISSIONS AND CONCLUSIONS

ALLEGED BREACH 1
Rule 2.3.1
"Consumers of premium rate services must be treated fairly and equitably."

1. The Executive asserted that the Level 2 provider had acted in breach of rule 2.3.1 of the Code, as the Application for the Service suppressed messages.

   The Executive relied on the complainant accounts, where the complainant had entered the Services through an MO opt-in and reported not having received any text messages to their handset. In addition, the Executive relied on the RMIT monitoring conducted on the Kaspersky samples between 5 November 2013 and 7 December 2013, detailed above in the "Background" section above.

The Executive noted that during the monitoring session of the Application, the RMIT did not receive any text messages to the monitoring phone's message inbox, but it was charged for a number of mobile terminating ("MT") messages. The RMIT was able to intercept suppressed messages using a debugging tool on its monitoring computer. This revealed that following the RMIT's instigation of the Service on 5 November 2013, four Service messages (of which three were chargeable messages) were sent to the handset but suppressed. They stated:

Message 1
"FreeMsg:U have subscribed to Glamour Babes for £4.50 per week until you send STOP to 88150 Help:01138272094. SP NewSMSM 16+ New Videos available every week"

Message 2
""http://glamour-babesxxx.com/?secret=fe3193f03";

Message 3
"Glamour Babes has the hottest Videos Available anywhere";

Message 4
"so here at http://glamour-babesxxx.com/?secret=fe3193f03 we have uploaded new babe videos for you to view whenever you like."

The Executive submitted that the suppression of messages resulted in consumers who engaged with the Application not being aware that they had been subscribed to the Service or that they were incurring weekly charges.

During the investigation the Executive disclosed the findings of its monitoring sessions to the Level 2 provider. A response was received from Venture247 and it stated that it understood the Application had been obtained from a third party advertising network and it had not been designed to suppress any messages. Further, that there had an automatic update of the Application on 16 February 2014 directly to its server which it believed contained the malware infection. The Executive did not accept the explanation given by Venture247, as a result of the following:

- The monitoring of the samples provided by Kaspersky pre-dated the date Venture247 stated that the server was compromised;
- Applications are digitally signed by a developer to prevent the injection of malicious code occurring after the application has been packaged. The Executive noted that the Application from Kaspersky had been signed on 26 April 2013. The Executive submitted that for a significant alteration to be made to the coding of the application (such as adding coding that suppressed chargeable text messages) it would need to be re-signed and repackaged. However, the monitored Application was not signed at the time of the alleged malware injection;
- The Executive noted that the shortcode in the Application had not been altered to a third party's shortcode and accordingly consumers would be subscribed to the Level 2 provider's Service The Executive submitted that there was no financial motive for a third party to "inject" the malware into the Application, as the malware only generated revenue for the Level 2 provider; and
- During the investigation, Venture247 provided an application, which it stated was the application promoted to consumers. The RMIT analysed this application and noted that the coding of this application included the word "compliant" a number of times and additional text that would have inserted a further stage into the opt-in process

requiring the consumer to confirm that it agreed to the terms and conditions, including the cost of the Service. The Executive also noted that the application supplied by Venture247 had been compiled and signed on 30 May 2014 which was the same date that Venture247 responded to the Executive's direction for information. The Executive asserted that this application was different to the Application provided by Kaspersky.

The Executive submitted that the Service was in breach of rule 2.3.1 of the Code as once the Application was installed, it suppressed all Service messages including subscription reminder messages and accordingly, the Service did not treat consumers fairly or equitably.

2. During the investigation, the Level 2 provider and Venture247 had provided responses to the Executive's directions for information issued to the Level 2 provider but the Level 2 provider had not provided a response to the breach letter.

3. The Tribunal considered the Code and all the evidence before it. The Tribunal noted that the Application provided by Kaspersky had been found on consumers' handsets as early as April 2013. Further, it noted that RMIT had analysed the sample relating to the Services in November 2013. The Tribunal was satisfied that the Application that promoted and enabled consumers to access the Services was available in 2013. The Tribunal accepted the RMIT monitoring evidence of the Kaspersky sample and found that it was clear that the Application, used to promote and access the Services, suppressed service messages. Consequently, the Tribunal found that this did not treat consumers fairly and equitably, as it prevented them from understanding that they were subscribed to a Service and were being charged, and from exiting the Services.

   Consequently, the Tribunal was satisfied that the suppression of Service messages did not treat consumers fairly and equitably and it upheld a breach of rule 2.3.1 of the Code.

Decision: UPHELD

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

1. The Executive asserted that the Level 2 provider acted in breach of rule 2.3.3 of the Code for the following reasons:

   1) Consumers did not give valid consent to being charged as clicking any part of the screen on the Application automatically initiated a subscription; and

   2) The Level 2 provider had not provided evidence to establish that complainants who had entered the Services through the WAP opt-in had consented to be charged. Accordingly, consumers had been charged without their consent.

   The Executive relied on the content of PhonepayPlus Guidance on "Privacy and Consent to Charge" (the "**Guidance**") The Guidance at the relevant time stated:

   "Premium rate services allow a charge to be generated to a consumer's pre-paid credit or communications (telephone) bill directly and remotely. A major concern in recent years is the delivery of reverse-billed messages to consumers' phones, without them having requested a charge (unsolicited, reverse-billed texts).

Paragraph 1.4

"…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…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...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.

Paragraph 2.13

"Some charges, or opt-ins to marketing, are generated once consumers click on a mobile internet site – often to view an image or a page. Consent to receive a charge, or opt in to marketing, must be subject to robust verification, as set out above...".

Reason 1 - Consumers did not give valid consent to being charged as clicking any part of the screen on the Application automatically initiated a subscription.

During monitoring of the Services on 5 November 2013 detailed above in the "Background" section, RMIT was automatically subscribed to the Service after it clicked on the top right hand corner of the Application landing page (**Appendix B**).

The Executive noted that pricing information was provided at the bottom of the screen. However, it was not made clear to consumers what action needed to be taken to enter the Service and thereby incur premium rate charges.

Further, the Executive noted that the pricing information was included in a small dense block of text at the bottom of the landing page in a font size which was difficult to read. Therefore it asserted that consumers were unlikely to take note of it.

In the absence of any information to the contrary, the Executive asserted that it would be reasonable for consumers to assume that by selecting one of the categories listed it may instigate a subscription to the Service. However, it was unlikely that consumers would foresee that clicking anywhere on the screen would initiate a subscription.

The Executive submitted that clicking on any part of the Application landing page did not signify that consumers had given their informed consent to be charged.

Reason 2 - The Level 2 provider had not provided evidence to establish that complainants who had entered the Services through the WAP opt-in had consented to be charged. Accordingly, consumers had been charged without their consent

The Executive relied on the content of all the complainants' accounts in relation to the WAP opt-in detailed in the "Background" section above. The Executive noted that the majority of complaints received by PhonepayPlus were from complainants who had interacted with the Services via a WAP opt-in and these complainants routinely stated that they did not consent to charges.

In addition, the Executive relied on the Guidance, which it stated makes it clear that all charges must be robustly verifiable. The Executive stated that although the 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 compliance with the Code).

During the investigation the Level 2 provider was directed to provide information in relation to consumers' consent to be charged. The Level 2 provider stated that it had third party verification in place from 22 July 2013. The Executive contacted the named third party to ascertain whether any verification data was available for a sample of the complainants MSISDNs that had opted in to the Services post 22 July 2013. The third party verifier stated that it held no data on the sample of the complainants MSISDNs.

The Executive submitted that the Level 2 provider had been unable to provide robustly verifiable evidence or any evidence at all, that consent to be charged had been obtained from some consumers. The Executive noted the complainants' accounts which stated that they had not consented to be charged. Consequently, the Executive submitted that the Level 2 provider did not have sufficiently robust systems in place to provide evidence of consent to charge and further, on the balance of probabilities some consumers did not consent to be charged. For both the reasons detailed, the Executive submitted that a breach of rule 2.3.3 of the Code had occurred.

2. During the investigation, the Level 2 provider and Venture247 had provided responses to the Executive's directions for information issued to the Level 2 provider but the Level 2 provider had not provided a response to the breach letter.

3. The Tribunal considered the Code, Guidance and all the evidence before it. In relation to the first reason raised by the Executive, the Tribunal noted that the Application obtained from Kaspersky contained a landing page which was an active link. The Tribunal accepted that whilst consumers were provided with some pricing information, the design of the Application landing page meant that it would be easy for consumers to inadvertently subscribe to the Service and incur a premium rate charge. The Tribunal noted that the pricing information was small and not sufficiently prominent, and if a consumer attempted to zoom in on the pricing information, as the screen was an active link, consumers would have activated a subscription to the Service. The Tribunal found that clicking any part of the screen did not constitute valid consent and accordingly, consumers had not given valid consent to be charged.

   In relation to the second reason raised by the Executive, the Tribunal noted that the Level 2 provider had stated that it had robust and properly verifiable evidence of consent to charge in relation to the consumers who had accessed the Service through a WAP opt-in as it had engaged a third party verifier from 22 July 2013. Having considered the evidence from the third party verifier, the Tribunal was not satisfied that the Level 2 provider had robust evidence of consent to charge for the WAP opt-in complaints.

   The Tribunal considered the number of consistent complaints that routinely stated that they had been charged without their consent. Accordingly, the Tribunal concluded that the Level 2 provider had not provided sufficient evidence to establish consumers' consent and further on the balance of probabilities, consumers had been charged for the Services without their consent. For both reasons presented by the Executive, the Tribunal found that the Level 2 provider had charged consumers without their consent and upheld a breach of rule 2.3.3 of the Code.

Decision: UPHELD

ALLEGED BREACH 3
Rule 2.4.2
"Consumers must not be contacted without their consent and whenever a consumer is contacted the consumer must be provided with an opportunity to withdraw consent. If consent is withdrawn the consumer must not be contacted thereafter. Where contact with consumers is made as a result of information collected from a premium rate service, the Level 2 provider of that service must be able to provide evidence which establishes that consent."

1. The Executive asserted that the Level 2 provider had acted in breach of the Code as it purchased marketing lists from third parties who had not obtained consumers' hard opt-in to be contacted. Accordingly, the Level 2 provider had contacted consumers by sending a WAP marketing text message without their consent.

   The Executive relied on the content of PhonepayPlus Guidance on "Privacy and Consent to Charge". The Guidance at the relevant time stated:

   Paragraph 4.2
   "Consumers have a fundamental right to privacy – enshrined in law, through the Privacy and Electronic Communications Regulations 2003 ('PECR'). In the UK, the Information Commissioner's Office ('ICO') is the body charged directly with enforcing PECR. We work closely with the ICO in order to define what constitutes acceptable and auditable consent to marketing. We may refer cases to the ICO, when appropriate, but will also treat invasions of consumers' privacy through paragraph 2.4 of the PhonepayPlus Code of Practice.

Paragraph 4.3
"PECR's provisions on consent (which apply to all marketing relating to a premium rate service by virtue of rule 2.1 of the Code) in summary are that:

- Where there is no explicit consent, the marketer must have obtained the individual's details through a sale, or negotiations for a sale, and the individual must have been given the opportunity to refuse such marketing, when their details were collected (a practice known as 'soft' opt-in);
- Soft opt-in marketing materials must relate to that marketer's products or services and only concern similar products to the individual's initial purchase, or area of interest (e.g. it would not be appropriate to promote adult services to someone who had only previously purchased ringtones);
- Soft opt-in consumers must be given a simple means of opting out at the time of initial purchase, and in each subsequent promotion; and
- Where soft opt-in conditions are not met a positive action signifying consent must be obtained from consumers after clear information about the intended activity has been provided. For example, where the individual's details are to be passed to third parties, they must be clearly informed of this, and positively confirm their acceptance (a practice known as 'hard' opt-in).

Paragraph 5.4
"In order to reach a greater number of consumers, some providers trade or purchase consumers' personal data. In these circumstances, further protection is necessary because the connection between the consumer and the business they first interacted with, and subsequently with the provider who is now marketing to them, is remote and indirect.

Paragraph 5.12
"Providers using marketing lists should ensure that each number marketed to has a valid opt-in, gathered no more than six calendar months ago. Providers should ensure that they can robustly verify (see the whole of section 5 of this General Guidance Note) each and every consumer's opt-in, and ensure that none are currently suppressed. Please note that, where a hard opt-in is used to market to consumers who have not previously purchased from a provider, or been in 'negotiations for a sale', then we will expect opt-in to be robustly verifiable in the event of any complaints, no matter how small or large the scale; this is in contrast to the approach to soft opt-in set out at paragraphs 5.1-5.3 of this General Guidance Note."

The Executive relied on the content of the complainants' accounts relating to the WAP opt-in. Specifically the Executive noted the following complaints:

"I recieved [sic] spam messages from them that I deleted however became concerned when I recieved [sic] a txt [sic] stating that I am signed up to there service and needed to text back to cancel."

"…around 3 or 4 texts received a day, always deleted and ignored. Not idea how they got mu [sic] number. explicit messages on how to get teenage sex pictures."

In its response to a direction to supply information, the Level 2 provider stated that it had purchased marketing lists from a third party. The Level 2 provider stated:

"The MSISDNs that have been passed onto us that originate from voices services are promoted on television. Our clients strictly adhere to guidelines set out by PhonepayPlus and Ofcom/BCAP. Attached is an example of the terms and conditions promoted on television that detail their marketing policy"

The attached terms referred to by the Level 2 provider stated:

"By connecting with any of our services you agree that we and selected third parties may send you promotional messages. If you do not wish to receive these messages text STOP to [SHORTCODE of show]"

The Level 2 provider also submitted details of how certain consumers consent was obtained, which stated:

"The customer has opted-in to receive direct marketing when calling our third party client's IVR Platform. Please see attached terms and conditions promoted on television which indicates that clients may be sent further marketing by third parties"

"The customer has opted-in to receive direct marketing on the following site: http://superstarmobuk.com"

The Executive submitted that the statement provided by the Level 2 provider indicated that only a soft opt-in was obtained by the third party, which did not meet the obligations set out in the Guidance. The Guidance clearly sets out that where individuals' data is shared with third parties a hard opt-in is required. Therefore when the Level 2 provider purchased marketing lists it should have requested and obtained robust evidence that each consumer had positively confirmed their acceptance to have their details passed onto third parties. The consent should have involved a positive step beyond mere purchase of the service by the consumer to be valid.

The Executive noted that the Level 2 provider had not provided any evidence that a hard opt-in had been obtained when it purchased the marketing lists. Accordingly the Executive submitted that the Level 2 provider had breached rule 2.4.2 of the Code as it had failed to provide robustly verifiable evidence of valid consumer opt-ins and consumers had been contacted without their consent.

2. During the investigation, the Level 2 provider and Venture247 had provided responses to the Executive's directions for information issued to the Level 2 provider but the Level 2 provider had not provided a response to the breach letter.

3. The Tribunal considered the Code and Guidance and all the evidence before it. The Tribunal noted the evidence from the complainants who reported receipt of unsolicited messages from the Level 2 provider. Further, it noted that the Level 2 provider had accepted that it had obtained consumers' details via a third party. The Tribunal concluded that the evidence provided by the Level 2 provider was not evidence of a hard opt-in, which was required. The Tribunal found that consumers had not provided valid consent to be contacted by the Level 2 provider. Accordingly, the Tribunal upheld a breach of rule 2.4.2 of the Code.

Decision: UPHELD

SANCTIONS

Initial overall assessment

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

Rule 2.3.1 - Fair and equitable treatment

The initial assessment of rule 2.3.1 of the Code was **very serious**. In determining the initial assessment for this breach of the Code the Tribunal applied the following criteria:

- The breach had a clear and highly detrimental impact or potential impact, directly or indirectly on consumers;
- The nature of the breach was likely to severely damage consumer confidence in premium rate services; and
- Consumers had incurred an unnecessary cost and the Services had the potential to cause other consumers to incur such costs.

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 breach had a clear and highly detrimental impact or potential impact, directly or indirectly on consumers;
- The nature of the breach was likely to severely damage consumer confidence in premium rate services; and
- The Level 2 provider had charged consumers without obtaining valid consent to charge.

Rule 2.4.2 - Consent to market

The initial assessment of rule 2.4.2 of the Code was **serious**. In determining the initial assessment for this breach of the Code the Tribunal applied the following criteria:

- The Services had been operated in such a way that demonstrated a degree of recklessness or intentional non-compliance with the Code; and
- The Level 2 provider had contacted consumers without their consent and was unable to provide satisfactory evidence establishing consent.

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

Final overall assessment

In determining the final overall assessment for the case, the Tribunal found no aggravating or mitigating factors. The Tribunal commented that the cumulative effect of the breaches of the Code relating to the Application, where consumers initiated a subscription by clicking anywhere on the Application landing page and were then not afforded the opportunity of viewing Service messages meant that the impact on consumers was more significant.

The Level 2 provider's revenue in relation to the Services was in Band 3 (£250,000 - £499,999). The Tribunal relied on the evidenced revenue figures provided by the Level 1 provider.

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

Sanctions imposed

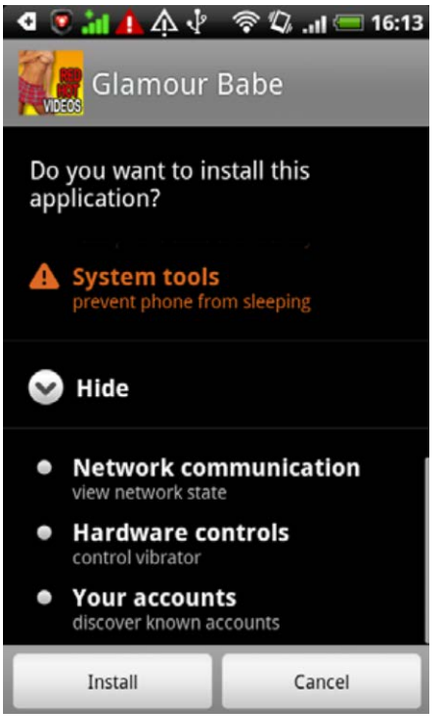
Having regard to all the circumstances of the case, the Tribunal decided to impose the following sanctions:

- a formal reprimand;
- a warning that if the Level 2 provider fails to demonstrate that it has robust verifiable evidence of consumer's consent to charge in the future it should expect to receive a significant penalty;
- a fine of £200,000;
- a requirement that, within three months of the Level 2 provider re-commencing trading, the Level 2 provider submit to a compliance audit of its procedures for ensuring consumers provide valid consent to be charged and that it has robust verifiable evidence of that consent, the recommendations of the audit must be implemented within a period defined by PhonepayPlus, the audit must be conducted by a third party approved by PhonepayPlus and the costs of such audit must be paid by the Level 2 provider; 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%**

Appendices

Appendix A – A screenshot of the Application installation process:



Appendix B – A screenshot of the Application landing page for the GlamourBabesxxx Service: