**Tribunal meeting number 161 / Case 3**

**Case reference:** 29838
**Level 2 provider:** Circle Marketing Ltd
**Type of service:** Adult/glamour video subscription services
**Level 1 provider:** IMImobile Europe 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 14 December 2012 and 1 October 2014, PhonepayPlus received 68 complaints from consumers in relation to adult and glamour video subscription services (the "**Service(s)**") operated by the Level 2 provider, Circle Marketing Ltd (the "**Level 2 provider**") until January 2014 when the Services were novated to another Level 2 provider, Cloudspace Limited ("**Cloudspace**"). The Services were operated under the names "UrHottestBabes", "Fun-sexygirls", and "HornyHotBabes" on the premium rate shortcodes 89333, 85222, and 88150. Consumers were charged £3 or £4.50 per week depending on the Service they engaged with. The Services commenced operation in March 2012 and June 2013 and continue to be operated by Cloudspace.

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 an 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 that appeared to utilise a form of malware that 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 January 2014, the Executive was advised via an email notification to contact Cloudspace as the Services had been novated to Cloudspace. Subsequent correspondence was directed to Cloudspace, 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 or confirmation that it was content for Cloudspace to respond on its behalf but the Executive did not receive a response. 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 15 October 2014. 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 acknowledged receipt of the breach letter in writing and responded by stating that it was no longer trading. 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 27 November 2014, 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 31 October 2013 and 27 February 2014 and the associated message logs;
- Correspondence between the Executive and the Level 2 provider/ Cloudspace (including directions for information and the Level 2 provider/ Cloudspace's responses including supporting documentation);
- Correspondence between the Executive and a third party verifier;
- Correspondence between the Executive and the anti-virus company Kaspersky;
- The novation agreements between the Level 2 provider and Cloudspace;
- PhonepayPlus Guidance on "Privacy and Consent to Charge"; and
- The breach letter of 15 October 2014 and the Level 2 provider's response of 23 October 2014.

**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 63 of the 68 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. In relation to the Application method of entry to the Services, 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:

**"**Service Description: No Idea, I did not subscribe,
Transcript of Text: Download your content now.
Summary of Complaint: I did not subscribe to ANY text service. I am being billed by these thieves. Receiving text saying download your content, this is a subscription service. I am being billed £1.50 for each text received. I DID NOT SUBSCRIBE TO ANY SUCH SERVICE!"**";**

**"**We are paying a lot for the call from your company which we do not remember agreeing. I strongly demand my money back please and stop the sending me the texts. I believed I have been forced to pay for which I never agreed. It is completely wrong, I contacted the company they told us, someone is taking your money not us**";**

**"**I do not know where these messages are coming from as I have never signed up for anything like this. I am receiving 2 messages at a time advertising websites for adult content with girls and every text I receive I am being charged £1.25. Please make this stop it is driving me mad. The frequency is probably not every day but every couple of days. I think in total I have been billed £12.50."

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:

**"**Apparently I am subscribed to a service called newbabez.com although I have never signed up to this or received anything from the company.
Never received any texts from the company
I have been billed £18-£20 per month since I apparently signed up to this service although I have not received anything from them."

"Consumer didn't initially have the shortcode and was having trouble getting info from T-mobile. To help I had him search his phone. He eventually found the 'spam folder' which contained more than 100 messages - including the initiation message - from 88150. He genuinely hadn't seen any of these before. I asked him to check his 'other downloads' folder, there was nothing odd there, but he normally downloads from the Google play store".

**Monitoring**

Following the discovery of the blog article by Kaspersky, the RMIT contacted Kaspersky to request the 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, four were identified as relating to the Services. The RMIT conducted testing on three of these Applications (for the Service "Fun-sexygirls") on 31 October 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 Fun-sexygirls Service, having obtained it by browsing the internet. The Executive noted that the monitoring evidence of 27 February 2014 does not relate to the Level 2 provider as the Service was operated by Cloudspace at the time of the monitoring. The Executive therefore included the monitoring only as background information and did not rely on this monitoring evidence in the breaches raised.

On 27 February 2014, the RMIT searched "hard 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 "fsg1086ts.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 selecting "package installer" on the following screen and then viewing the permissions before selecting "install".

The RMIT opened the Application and was presented with an Application landing page for the Fun-sexygirls 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. RMIT was charged for three subscription messages which were suppressed by the Application. Further, the RMIT obtained the IP address of where the Application was hosted and noted that this pointed to other domains that were connected to the Level 2 provider.

**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 service messages.

   The Executive relied on the complaints and the monitoring conducted by the RMIT on the Kaspersky samples on 31 October 2013, detailed above in the "Background" section.

   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 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 31 October 2013, four Service messages (of which three were chargeable messages) were sent to the handset but suppressed. They stated:

   Message 1
   "FreeMsg:You joined fun-sexygirls videos for £4.50 per week. Support 01618840150, STOP to 88150 to unsubscribe. SP Circle Marketing. 16+";

   Message 2
   ""fun-sexygirls has videos of girls to download now! New videos are sent every week! Calls us on 01618840150 for help SP CircleM";

   Message 3
   "To Download the best video on your mobile click on the link sent to your phone";

   Message 4
   "http://fun-sexygirls.com/?pin=82a143353".

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, and Cloudspace responded and stated that it understood the Level 2 provider had received the Application from a third party advertising network in December 2013 and it had not been designed to suppress any messages. Further, that the third party advertising network had provided it with an email addressed to undisclosed recipients and dated 12 May 2014 which explained that its server had been compromised and an automatic update had been sent from its servers on 16 February 2014 to update the Application. The update contained a harmful piece of software which caused the Application to suppress messages and gather information from consumers without their knowledge. The Executive did not accept the explanation given by the Level 2 provider and the third party advertising network, as a result of the following:

- The monitoring of the samples provided by Kaspersky pre-dated the date the Level 2 provider 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 Applications were signed on 15 May 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 Applications were not signed at the time of the alleged malware injection;
- 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. 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 Service.

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. The Level 2 provider did not provide a response to the breach letter.

3. The Tribunal considered the Code and all the evidence before it. The Tribunal noted that it was clear under the Code and it had been clearly stated in previous Tribunal adjudications, that Level 2 providers are responsible for the operation of its services, which includes the promotion of those services. In this case the Level 2 provider had chosen to engage an advertising network to promote the Services through an Application. Consequently, the Tribunal concluded that the Level 2 provider was responsible for the Application that promoted and enabled consumers to access the Services.

The Tribunal found that whether the Application was designed to suppress messages from the outset or was subsequently hacked, it was clear that the Application used to promote and access the Services would hide messages and this did not treat consumer fairly and equitably. The Tribunal commented that the cumulative effect of an application automatically downloading, consumers initiating a subscription by clicking anywhere on the Application landing page and the suppression of the Service messages meant that the unfair treatment of consumers was more significant.

Consequently, the Tribunal was satisfied that the suppression of Service messages did not treat consumers fairly and equitably.

**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 evidence provided by the Level 2 provider to establish that complainants who had entered the Services through the WAP opt-in had consented to be charged was not verified by an independent third party, or in a way that meant that it could not be tampered with. Accordingly, the Level 2 provider had not provided sufficient evidence to establish consumers had consented to be charged.

   The Executive relied on the content of PhonepayPlus Guidance on "Privacy and Consent to Charge" (the "**Guidance**") The Guidance states:

   "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 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 videos under the heading "choose what video you want to watch first", this would 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 evidence provided by the Level 2 provider to establish that complainants who had entered the Services through the WAP opt-in had consented to be charged was not verified by an independent third party, or in a way that meant that it could not be tampered with. Accordingly, the Level 2 provider had not provided sufficient evidence to establish consumers had consented to be charged.**

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 were from complainants who had interacted with the Services via a WAP opt-in. 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. Cloudspace responded by stating that it had third party verification in place and provided a contract with a third party verifier which had been signed by the Level 2 provider on 17 December 2012. The Executive contacted the named third party to ascertain whether any verification data was available for a sample of the complainants MSISDNs. 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 that consent to be charged had been obtained from some consumers. The Executive noted the consistent 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. The Level 2 provider did not provide 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 version of 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. The Tribunal particularly noted that a consumer may attempt to zoom in on the pricing information presented in a small text but as the screen was an active link, zooming in on the page risked activating a subscription. The Tribunal noted that there was no particular acceptance page or button for a consumer to consent to be charged and consequently the Tribunal found that clicking any part of the screen did not constitute valid consent.

In relation to the second reason raised by the Executive, the Tribunal noted that the Level 2 provider had been requested to provide robust and properly verifiable evidence of consent to charge but it had not provided any evidence. The Tribunal was not satisfied that the third party verifier held robust verification of consumers' consent to charge. The Tribunal took into account the large 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 the 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 acted in breach of the Code as it purchased marketing lists from third parties which 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 states:

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

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. The Guidance clearly sets out that where individuals' data is shared with third parties a hard opt-in is required. The Executive submitted that 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 on to third parties.

Accordingly the Executive submitted that the Level 2 provider 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. The Level 2 provider did not provide 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 in the absence of any evidence of consent to market and in light of the complainant accounts, consumers had not consented 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 nature of the breach was likely to severely damage consumer confidence in premium rate services; and
- The Services sought to generate revenue through an Application that automatically downloaded onto consumers' handsets, and once it had been installed, through the use of message suppression.

**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 nature of the breaches and the scale of harm caused to consumers were likely to severely damage consumer confidence in premium rate services;
- The Services were promoted and accessed through an Application that had caused consumers to unknowingly subscribe to a Service to seek to generate revenue; and
- The Level 2 provider charged consumers without obtaining robustly verifiable evidence of consent to charge and although it had employed a third party verifier to retain such evidence, it had not consistently used the system provided.

**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 criterion:

- The Level 2 provider 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 took into account the following two aggravating factors:

- The Level 2 provider had failed to follow PhonepayPlus Guidance on consent to charge and consent to market and the numerous previous adjudications published concerning the requirement to have and produce, when requested robustly verifiable evidence of consent to charge and consent to market.
- The Level 2 provider had been subject to an adjudication in January 2013 in which sanctions including a fine of £60,000, had been imposed for breaches of the Code including breaches of rules 2.3.3 and 2.4.2 of the Code. The Tribunal noted that at the time of the previous adjudication, the Level 2 provider had made a number of assurances to the Tribunal that it had remedied the breach of rule 2.3.3 of the Code and it was clear that this had not been done.

In determining the final overall assessment for the case, the Tribunal determined that there were no mitigating factors.

The Level 2 provider's revenue in relation to the Services was in the range of Band 3 (£250,000 - £499,999).

Having taken into account the aggravating factors, and in particular the previous adjudication against the Level 2 provider, the Tribunal concluded that the seriousness of the case should be regarded overall as **very serious**.

**Sanctions imposed**

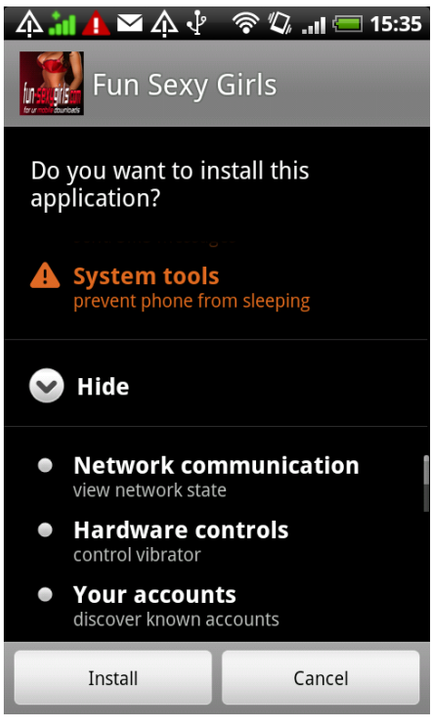
Having regard to all the circumstances of the case, the Tribunal decided to impose the following sanctions:

- 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 £130,000 (which includes a £20,000 uplift that was imposed as a result of the Level 2 provider's relevant breach history), ;
- 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 provider 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 Fun-sexygirls Service: