Tribunal meeting number 161 / Case 2

Case reference: **45018**
Level 2 provider: **Cloudspace Limited (UK)**
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 20 March 2014 and 12 August 2014 PhonepayPlus received 32 complaints from consumers in relation to adult and glamour video subscription services (the "**Service(s)**") operated by the Level 2 provider, Cloudspace Limited (the "**Level 2 provider**"). The Services 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 had engaged with. The Services commenced operation in March 2012 or June 2013 and were initially operated by another Level 2 provider, Circle Marketing Ltd ("**Circle**"). The Services were novated to the Level 2 provider in January 2014 and they continue to operate.

The Services were promoted by sending consumers a wireless application protocol ("**WAP**") push message which led them to a Service webpage to subscribe. Consumers could also engage with the Services using an Android application (the "**Application**") which utilised mobile originating ("**MO**") opt-in.

Concerns regarding the Application were uncovered as a result of a blog article by the antivirus 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**") for testing. In addition, the RMIT discovered Android applications on the internet and conducted monitoring which identified concerns regarding the operation of the Application for the Service as it appeared to utilise a form of malware that suppressed the receipt of Service messages.

The investigation

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

The Executive sent a breach letter to the Level 2 provider on 23 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
- Paragraph 3.9.2 - Appropriate use of a number range

The Level 2 provider responded on 13 November 2014. On 27 November 2014, after hearing informal representations from the Level 2 provider, 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 Service conducted on 31 October 2013 and 27 February 2014 and the associated message logs;
- 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 a third party verifier;
- Correspondence between the Executive and the anti-virus company Kaspersky;
- PhonepayPlus Guidance on "Privacy and Consent to Charge" and "The appropriate use of number ranges";
- Two novation agreements between Circle and the Level 2 provider dated 21/22 January 2014; and
- The breach letter of 23 October 2014 and the Level 2 provider's response of 13 November 2014 including supporting evidence.

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 31 of the 32 complaints related to the WAP opt-in method of entry to the Services rather than the Application. Such complaints therefore were not relevant to the breaches of the Code raised in relation to the Application method of entry to Service. 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 Services due to the suppression of Service messages.

Extracts from a sample of complainants' accounts included:

"Consumer saying she is getting adult messages and quiz messages Consumer saying she has changed her mobile number a few times because she keeps getting random messages which she has not requested. Consumer saying has not given her mobile phone to no one. Consumer has had the mobile number for over 7 months. Consumer has been receiving messages. Consumer has been deleting the messages. Consumer says he has not subscribed to anything. Consumer doesn't remember entering details in any kind of competition"

"My daughter has no idea where this company have got her mobile number from. My mobile provider has refunded the charges to my account, but is unable to stop this company sending texts. They advised me to text the words stop and stop all to this number, which I have done, however I am concerned that this company will continue to send inappropriate texts to my young teenage daughter"

"Give links to videos of 'hot babes' which I have not asked and don't want. I have not opened the links and trashed all texts before today not knowing I was getting charged I have started receiving texts from this number and found that I am being billed £1.50 for each text".

The Executive received one complaint from a complainant that opted in to the Service via an MO and stated that s/he had received messages but that they were unsolicited.

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. 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". The RMIT opened the Applications and was presented with an Application landing page, on which the RMIT clicked the top right hand corner of the screen (away from the options displayed on the menus). 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.

The Executive noted that the monitoring evidence of the Kaspersky samples did not relate to the Level 2 provider because at the time of the monitoring, the Services were operated by Circle and not the Level 2 provider. The Executive included the monitoring of the Kaspersky samples as background information but it did not rely on this monitoring evidence in the breaches of the Code raised.

In addition to the monitoring of the Kaspersky samples of the Application, on 27 February 2014, the RMIT monitored the Application for the Fun-sexygirls Service, having obtained it by browsing the internet.

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 viewing the permissions before selecting "install" (**Appendix A**).

The RMIT opened the Application and was presented with the Application landing page for the Fun-sexygirls Service (**Appendix B**). 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.

In addition to the monitoring detailed above, during the course of the investigation the Level 2 provider supplied the Executive with a sample of the Application. On 6 October 2014, the RMIT analysed the coding of the Application provided and noted that the coding contained the word "compliant" and had additional text that had been given the name "complientmsg" [sic], which had not been found in the coding of the Application captured on the internet on 27 February 2014 by the RMIT.

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 for the following reasons:

    1. The Application automatically downloaded without consumers' knowledge or consent; and
    2. The Application suppressed Service messages.

    Reason 1 - The Application automatically downloaded without consumers' knowledge or consent.

    The Executive relied on the monitoring conducted by the RMIT on 27 February 2014, detailed in the "Background" section above. The Executive noted that the Application downloaded automatically when a new browser webpage (fun-sexygirls.com) opened in the background while the RMIT was browsing on the website hardsextube.com and after it had selected a thumbnail.

    The Executive acknowledged that the RMIT was required to manually install the Application once it had downloaded by visiting the notifications area and following the default installation process. However, the Executive asserted that until the Application had been opened, it was not clear that the file that had been downloaded, contained a premium rate service. Accordingly, consumers would not have any information to make an informed decision as to whether or not to install the file. Furthermore, the Executive submitted that consumers were likely to have believed that they had pro-actively downloaded a connected file or an update, which related to an existing application.

    The Executive submitted that, by not giving consumers any information to enable them to exercise their discretion as to whether or not to download and/or install the Application, the Level 2 provider did not treat consumers fairly or equitably.

    Reason 2 - The Application suppressed Service messages.

    The Executive relied on the monitoring conducted by the RMIT on the Application found on the internet on 27 February 2014, detailed above in the "Background".

    The Executive noted that during the monitoring session, 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. For example, this revealed that following the RMIT's instigation of the

Service on 27 February 2014, four Service messages (of which three were chargeable messages) were sent to the handset but suppressed and they stated:

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

Message 2
"http://fun-sexygirls.com/?pin=207065751";

Message 3
""fun-sexygirls has videos of girls to download now! New videos are sent every week! Calls us on 01618840150 for help SP Cloudspace";

Message 4
"To Download the best video on your mobile click on the link sent to your phone".

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 it confirmed that the Application was supplied by a third party advertising network to Circle in December 2013. The Level 2 provider understood that the third party advertising network had tested the Application prior to providing it to Circle and it had no reason to believe that there were any problems with it. Further, it stated 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:

- 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 for the Fun-sexygirls Service were digitally signed on 6 February 2014. 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 on the date 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 Services.

The Executive submitted that the Services were in breach of rule 2.3.1 of the Code as, the Application automatically downloaded without consumers' knowledge or consent and once the Application was downloaded and installed, it suppressed all Service messages including subscription reminder messages. Accordingly, the Service did not treat consumers fairly or equitably.

2. The Level 2 provider denied that a breach of rule 2.3.1 of the Code had occurred as consumers were provided with all the information they required and when the Level 2 provider had tested the Application, it had not experienced the suppression of messages.

   Generally, the Level 2 provider stated that it believed that the RMIT's monitoring had been conducted on a handset that did not meet the standard required by the Application.

   The Level 2 provider stated that it entered into a novation agreement with Circle in January 2014 and upon novation of the Services, it was of the understanding that all Services, not limited to Application, were operated in accordance with the Code.

   The Level 2 provider stated that Circle had not provided the Level 2 provider with a full explanation in relation to the Application and therefore it could only answer limited questions. The Level 2 provider was unclear why a case had been brought against it, as it believed the Executive should have pursued a case against Circle rather than the Level 2 provider.

   Reason 1 - the Application automatically downloaded without consumers' knowledge or consent.

   The Level 2 provider stated that a consumer would have to download the Application manually and it believed that consumers had been provided with the all information they required to access the Services fairly. It stated that after downloading the Application but before opening it, there were a series of pop-ups and confirmation requests that highlighted that there were weekly costs associated with the Service. The Level 2 provider supplied copies of the warnings that it stated a consumer would have viewed (**Appendix C and D**).

   Reason 2 - the Application suppressed service messages.

   The Level 2 provider stated that it had tested the Application on 31 January 2014. It downloaded the Application and selected "I Agree" on its handset and it was satisfied that it had received all the Service messages that should have been received. The Level 2 provider asserted that the Application, which it understood had been designed by a third party advertising network, operated in the manner it should have and there was no message suppression.

   The Level 2 provider submitted that 147 consumers had subscribed to the Service through the Application but other than PhonepayPlus, it had not received any complaints. It highlighted that upon being notified of the potential issues with the Application, it ceased marketing for all application based Services. The Level 2 provider stated that it felt strongly that the Executive should have directed any questions regarding the Application to the third party advertising network that supplied the Application, as it was unable to answer any questions relating to it.

   During informal representations conducted on behalf of the Level 2 provider, it stated that it was concerned that there was no independent expert witness evidence to corroborate the RMIT's monitoring of the Kaspersky sample and accordingly it submitted that this evidence should not be relied on by the Tribunal.

   The Level 2 provider reiterated its written submissions and stated that it was concerned that the Android 2.2 operating system had been used by the RMIT during its monitoring session. It asserted that the HTC Desire handset running on an Android 2.2 operating system was not compatible with modern Android applications and was used by an insignificant number of

users. The Level 2 provider stated that its view was that updated handsets would not encounter the same difficulties with the Application.

The Level 2 provider stated that had it been made aware of the Executive's concerns as soon as the Executive had discovered the problems, it would have taken corrective action sooner and prevented any consumer harm. It questioned why this had not been done.

The Level 2 provider submitted that it was an established premium rate service provider that had no history of breaches of the Code. The Level 2 provider stated that it had co-operated and provided the Executive with full and accurate responses to every question that had been asked of it in a precise and timely manner.

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

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 did not accept the Level 2 provider's assertion that because the Executive had used a handset which did not reflect the most commonly used operating system, the monitoring did not support a breach of the Code. It was quite possible that that operating system was still being used by some consumers and the Application could be accessed with that equipment. The Tribunal noted from the RMIT's monitoring that the Application did not carry a warning that it was incompatible with the older operating system.

The Tribunal noted that the monitoring conducted by the RMIT in February 2014 demonstrated that the Application automatically downloaded. The Tribunal noted that following this, the Application had to be installed by a consumer before s/he could interact with the Service. Notwithstanding this, the Tribunal concluded that the automatic download of an Application without providing sufficient information and obtaining valid consent did not treat consumers fairly and equitably.

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 being able to initiate 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 found that for the reasons raised by the Executive, the Service had not treated 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 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 landing page of the Application **(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 from the menu, 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 screen 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 be charged.

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 used a third party verifier and supplied a copy of the contract with it. In addition to this, the Level 2 provider stated that it had its own in-house verification to provide a further layer of security, with unique PINs generated for each subscriber. It stated that this data is stored internally and was fully protected from any external access. It enclosed the PINs that related to the complainants.

On 16 October 2014, the Executive accessed the third party verification system to ascertain whether any verification data was available for a sample of the complainants' MSISDNs. The Executive was notified that the third party verifier did not hold any records for 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 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 denied that a breach of rule 2.3.3 of the Code had occurred and stated that consumers of the Application were provided with all the required information and had consented to be charged. In relation to the second reason raised by the Executive, it stated that it had experienced some difficulties with the third party verifier's system but in any event it held internal PINs which were a secure system of verification.

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.

The Level 2 provider submitted that the screenshots that it had provided demonstrated that a consumer would be fully aware that they are entering a subscription service **(Appendix C and D)**. The Level 2 provider asserted that the Executive had accepted that consumers were required to manually install the application once it had downloaded and therefore a consumer had agreed to send in a keyword that was attached to the Application prior to incurring charges.

The Level 2 provider stated that it had only ever received one consumer complaint since 22 January 2014 in relation to the Services that were initiated by an MO opt-in.

In addition, the Level 2 provider stated that the Application that it had submitted to the Executive had been provided by the third party advertising network and it was not set up to received updates from the auto-update platform. Accordingly, the Application submitted to the Executive contained the original coding of the Application prior to it being compromised. The Level 2 provider highlighted that it had removed the Application from its server as soon as it had been notified of the problem by the third party verifier.

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 Level 2 provider stated that it had provided the Executive with a contract with a third party verifier which, after novation, had been taken over by the Level 2 provider. The Level 2 provider asserted that it did not have up-to-date contact details for the third party verifier's system immediately post novation. It had recently been in correspondence with the third party verifier and it was in the process of ensuring the contract was updated. The Level 2 provider stated that it had continued marketing using the third party verifier as a robust verification platform as Circle had done previously.

The Level 2 provider explained that when a consumer was sent a WAP marketing message from its system, it allocated a unique in-house PIN that was stored on its secure database. The Level 2 provider had supplied these unique PINs to the Executive. As the Level 2 provider saw the number of complaints increase towards the end of May 2014, it became apparent that although from within the third party system it could see PINs being verified, it did not reflect what it was observing on its platform. Accordingly, on 22 May 2014, the Level 2 provider stated that it ceased promoting the Services until it was satisfied that any consumers coming into their platform via WAP could be fully verified by the third party verifier. The Level 2 provider supplied a sample of ten consumers that it stated had been verified by the third party verifier in May 2014.

The Level 2 provider assured the Tribunal that it had contacted every consumer that was not satisfied with the Services and offered them a full refund. Of the 32 complaints, one had not reached its platform but it had issued full refunds to 24 of the complainants that it had made contact with. The Level 2 provider provided a detailed list of the complainants that it stated it had refunded.

During the informal representations, the Level 2 provider stated that it had relied on the third party verifier service to provide robust verification of consumers' consent to be charged. The contract had been in place for a lengthy period of time and it was a system that it was aware the Executive had access to, in order to obtain the verification information. It clarified that the system operates when a Level 2 provider buys credit which is used against the number of verifications obtained.

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

In relation to the first reason raised by the Executive, the Tribunal noted that the versions of the Application obtained from the RMIT's monitoring and the sample from the Level 2 provider both contained a landing page which was an active "link" menu page. 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 by zooming in on the page, they risked activating a subscription. The Tribunal noted that there was no particular acceptance page or button for a consumer to consent to charges and consequently the Tribunal found that clicking any part of the screen did not constitute valid consent.

The Tribunal noted that the Level 2 provider had been requested to provide robust and properly verifiable evidence of consent to charge in relation to the complainants that had accessed the Services via a WAP opt-in. The Tribunal was not satisfied with the evidence provided by the Level 2 provider as no evidence had been provided by a third party verifier and the internal records supplied by the Level 2 provider were not sufficiently robust as they there was not a clear audit trail that categorically could not have been interfered with. The Tribunal took into account the 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 confirmed that it had purchased marketing lists from a third party**.** The Level 2 provider supplied a contract between the third party and the Level 2 provider dated 24 January 2014. The Level 2 provider supplied screenshots of the third party's promotion which stated, in small text, that ran across the bottom of the screen:

"From calling the show you may receive marketing messages, your data may be passed onto third parties Customer Service Helpline: 08442439888."

The Executive noted that the Level 2 provider had not provided any evidence that a hard opt-in had been obtained from the consumers of the third party service. 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 denied that a breach of rule 2.4.2 of the Code had occurred and stated that it had obtained consumers' details from a third party and it had provided a copy of the third party's promotional material, as evidence of the consumers' consent to be contacted.

The Level 2 provider supplied a signed contract with the third party dated 24 January 2014 which it stated revealed that it had not purchased the data, but instead, the third party provided the data on a revenue share basis.

The Level 2 provider explained that the third party advertised its services on-line or via live broadcasts. A consumer of the third party service could decide if s/he wanted to interact with any of these services. On the live screenshots, shown in a terms and conditions section, the consumer was informed that by engaging with the advertised service it may receive promotional material from third party partners.

Further, the wording at the bottom of the live broadcast stated that any consumer may be contacted by a third party partner and s/he could opt out of by texting STOP or STOP ALL. The Level 2 provider stated that a consumer of the third party service was given full terms and conditions via an interactive voice response ("**IVR**") when they called the third party's service. The Level 2 provider supplied a copy of the IVR that warned consumers that they may receive third party marketing messages and advised them how to opt-out.

The Level 2 provider gave five examples of complainants that had heard the IVR and had been made aware that they may receive third party marketing. Moving forward, the Level 2 provider stated that it had decided to cease promoting using the data provided by the third party and it intended to concentrate solely on campaigns verified by the third party verifier.

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

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 commented that for there to be valid consent, consumers must be clearly informed about the use of their data and positively confirm their acceptance. It considered the evidence of consumers' consent provided by the Level 2 provider but found that it was a soft opt-in and not a hard opt-in. It concluded that the evidence provided by the Level 2 provider was not sufficient and accordingly, consumers had not provided valid consent to be contacted by the Level 2 provider.

For the reasons presented by the Executive, the Tribunal found that the Level 2 provider had contacted consumers without their consent and upheld a breach of rule 2.4.2 of the Code.

Decision: UPHELD

ALLEGED BREACH 4
Paragraph 3.9.2

"Where certain premium rate number ranges, shortcodes or other means of access to services have been designated by either Ofcom or a Network operator for use only for particular purposes or for the provision of particular categories of service, or where Ofcom or a Network operator has

restricted certain premium rate number ranges, shortcodes or other means of access to services from being used for particular purposes or for the provision of particular categories of service, those number ranges, shortcodes or means of access must not be used in contravention of these restrictions. Ofcom's designations will have precedence over any issued by a Network operator."

1. The Executive asserted that the Level 2 provider had acted in breach of paragraph 3.9.2 of the Code as it operated a sexual entertainment service on a non-sexual entertainment shortcode. The Executive relied on the content of PhonepayPlus Guidance on "The appropriate use of number ranges". The Guidance states:

Paragraph 1

"It is a requirement for providers to ensure that appropriate number ranges are used for the operation of their services for the following reasons:

- Number recognition (including per minute call charges) – in order for trust to be built in the premium rate market, consumers must be given the opportunity to gain an understanding of the types of service that number ranges are associated with, and this includes the cost that they will be charged per minute for calling those services. For example, consumers should be able to easily recognise that an '09' or '118' prefixed number is associated with a service that will be charged at a 'higher rate' (i.e. that they will be paying for a 'service', when dialled). Likewise, they should have some knowledge that an '0871/2/3' prefixed number will be charged at between 5p and 10p per minute (i.e. a 'lower rate', but that they will still be paying for a 'service').
- Consumer protection and call barring – certain number ranges are blocked from being dialled from a mobile phone by default; number ranges that are reserved for either sexual entertainment services ('SES') or gambling services – see below for the full list of 'adult' reserved number ranges. This block may be removed by adult consumers if they contact their Mobile Network Operator. Consumers can also request 'call barring' be put in place on their landline and/ or mobile phones, meaning that their phone will be disabled from the dialling of either specific '09' prefixed numbers (i.e. SES-prefixed numbers), or from the dialling of '09' prefixed numbers in general.

Paragraph 2.2

"Mobile shortcode service use (as designated by the Mobile Network Operators):

- 69x/79x/89x – these shortcode ranges are reserved for SES (adult services which require consumer age verification prior to use). They can be charged at either between 10p and £10 per text message received by a consumer, or at between 10p and £5 per minute when operating as a SES voice shortcode (i.e. a consumer dials the shortcode from a mobile phone to receive a voice-based SES, as opposed to texting the shortcode to receive a text-based SES).
- 60000-68999 and 80000–88999 – these shortcode ranges can be used for the operation of any service type, other than SES. As with the above ranges, charges can be between 10p and £10 per text message received by a consumer, or between 10p and £5 per minute when operating as a voice shortcode, which a consumer can dial for a voice-based service. Services operating above £1.50 per minute require permission from PhonepayPlus prior to commencing operation – please refer to the PhonepayPlus website www. phonepayplus.org.uk for further information on prior permission…."

The Executive noted that the Fun-sexygirls Service operated on shortcode 88150, which was a non-adult designated shortcode. The Executive obtained a webpage promotion for the Service which contained explicit adult images which were clearly of a sexual nature **(Appendix E).**

Accordingly, the Executive submitted that the Level 2 provider had operated a Service on a non-adult shortcode, when it should have operated on a designated shortcode for sexual entertainment services, in breach of paragraph 3.9.1 of the Code.

2. The Level 2 provider partially accepted that a breach of paragraph 3.9.2 of the Code had occurred. It stated that the content of Service that operated on the shortcode 88150 was entirely of a non-adult nature. The Level 1 provider for this shortcode had confirmed that the Service was fully acceptable for a non-adult shortcode.

However, the Level 2 provider accepted that the promotional material was of an adult nature **(Appendix E)**. This had occurred due to it regularly changing its online banners to keep the marketing fresh. Unfortunately, it had used the adult marketing for the Service in error as a result of it operating a number of different Services on adult and non-adult shortcodes.

The Level 2 provider stated that it was currently addressing why and how this error had occurred as a matter of urgency.

3. The Tribunal considered the Code and Guidance and all the evidence before it, including the Level 2 provider's partial admission of the breach.

The Tribunal was satisfied that the promotion was of a clearly sexual nature. It noted that the Code defined a sexual entertainment services under paragraph 5.3.31 of the Code and the definition included, "…any service for which the associated promotional material is of a clearly sexual nature, or indicates directly or indirectly that the service is of a sexual nature". Accordingly, the Tribunal found that the promotion came within the definition of a sexual entertainment service and should not have operated on a non-adult shortcode. Consequently, the Tribunal upheld a breach of paragraph 3.9.1 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.

Paragraph 3.9.2 - Appropriate use of a number range

The initial assessment of paragraph 3.9.2 of the Code was **serious**. In determining the initial assessment for this breach of the Code the Tribunal applied the following criterion:

- The service has been operated in such a way that demonstrated a degree of reckless non-compliance with the Code.

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; and
- The Level 2 provider had not taken adequate steps to ensure that the Services were compliant when they were novated to the Level 2 provider in January 2014 and the Level 2 provider should have been on notice of potential issues, particularly in light of the previous adjudication against the Service in February 2013 for breaches of rule 2.3.3 and 2.4.2 of the Code.

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

- The Level 2 provider stated that it had suspended use of the Application in May 2014 and it had taken action to ensure that such breaches reoccurring were minimised, by ceasing to promote the Services through Android applications and data obtained by third party marketing lists; and
- The Level 2 provider stated that it had proactively approached complainants to offer refunds and many had been refunded.

The Level 2 provider revenue in relation to the Services was in the range of Band 4 (£100,000 - £249,999).

Having taken into account the aggravating and mitigating factors, the Tribunal concluded that the seriousness of the case should be regarded overall as **very serious**.

Sanctions imposed

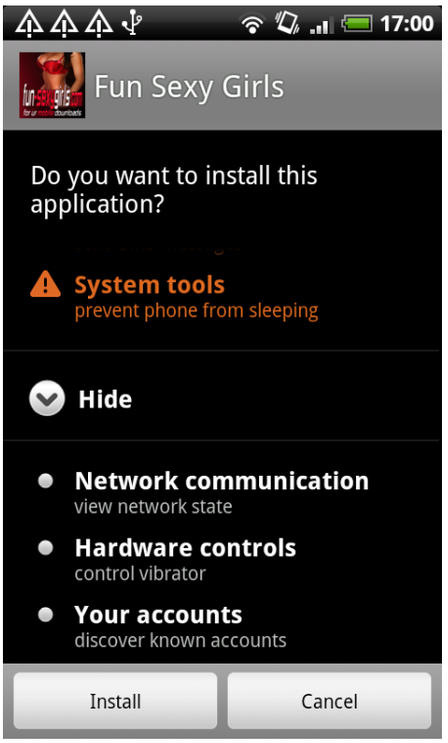
Having regard to all the circumstances of the case, the Tribunal decided to impose the following sanctions:

- 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 £80,000;
- a requirement that the Level 2 provider remedy the breaches of the Code by implementing adequate consent to charge and consent to market procedures for the Services and ensure that the Services operate on the appropriate premium rate shortcode, and produce evidence to the satisfaction of PhonepayPlus, within four weeks from the date of publication of this decision; 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 Services, 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%

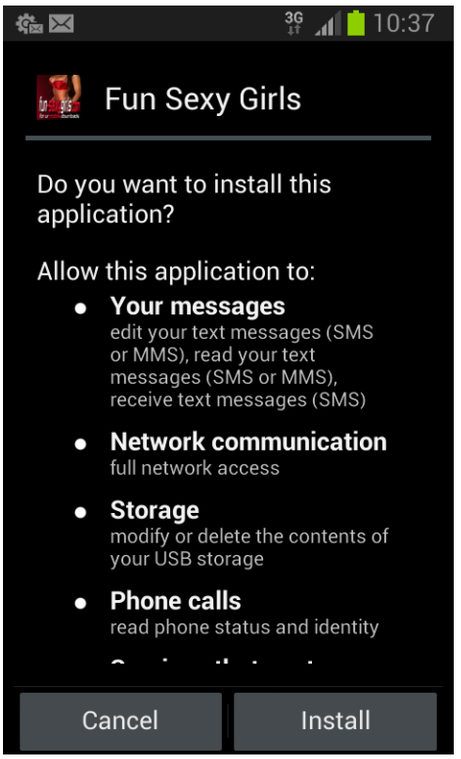
Appendices

Appendix A – screenshot of the Application installation process:

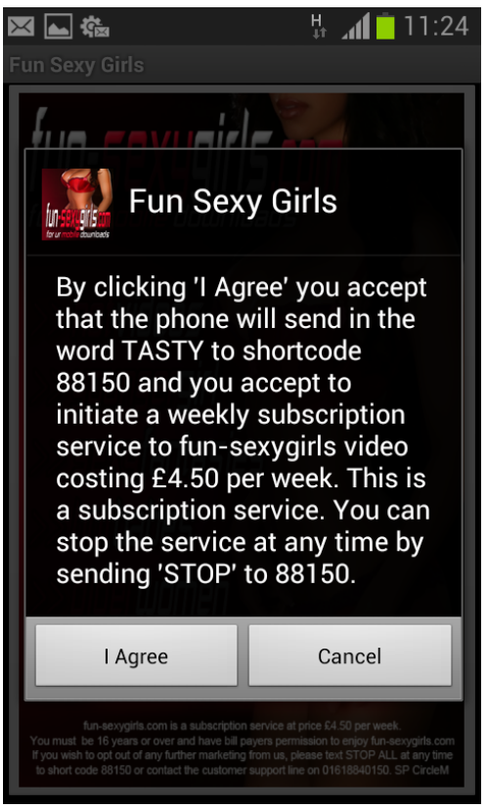


Appendix B – A screenshot of the Application landing page for the Fun-sexygirls Service:

Appendix C – A screenshot of the Application installation process provided by the Level 2 provider:



Appendix D – A screenshot of an Application pop-up provided by the Level 2 provider:



Appendix E – A screenshot of the promotional webpage for the Fun-sexygirls Service: