Tribunal meeting number 161 / Case 1

Case reference:	**28354**
Level 2 provider:	**Syncronized Ltd (UK)**
Type of service:	**Adult/glamour video subscription Services**
Level 1 provider:	**GSO MMBU (Private Company) Limited (UK), 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 18 May 2013 and 12 August 2014, PhonepayPlus received 125 complaints from consumers in relation to adult and glamour video subscription services (the "**Service(s)**") operated by the Level 2 provider, Syncronized Ltd (the "**Level 2 provider**"). The Services operated under the names "Fuck Hunter", "Titty Tingle, "Glam Pleasures" and "Sex Dose" on the premium rate shortcodes 89066, 85033, 69063 and 88150. Consumers were charged between £1.50 and £4.50 per week depending on the Service they engaged with. The Services commenced operation in May 2012, October 2012 or April 2013 and they continue to operate, save for the Fuck Hunter Service which ceased to operate in March 2014.

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

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**") for monitoring, 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

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 6 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

The Level 2 provider responded on 22 October 2014. On 28 October 2014, the Executive responded to the Level 2 provider's response and provided further evidence to address some of the points made by the Level 2 provider. The Level 2 provider further responded to the Executive on 6 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 1 November 2013, 4 November 2013, 3 March 2014 and 18 March 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";
- The breach letter of 6 October 2014 and the Level 2 provider's response of 22 October 2014; and
- The Executive's letter of 28 October 2014 and the Level 2 provider's response of 6 November 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 113 of the 125 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 Services due to the suppression of Service messages.

Extracts from a sample of complainants' accounts included:

"I suddenly received an unsolicited text message from this number on the 15th May 2013 (which appears to have been free). I ignored it as I didn't want to give this spammer confirmation of my number. But I then received 3 more on the 17th that reduced my balance by about £4. I didn't sign up for this "service" but suddenly received messages from them and was deducted money. The "service" is offering me access to, I believe, a porn website "Sex Dose", which I didn't request. I don't know how this service provider came to have my number. I want a refund and assurance this company will not contact me again."

"They started sending me text messages from November saying I was subscribed to Tittytingle for £1.50 per week until I send stop to 85033. Or help? 02476998420 or simply marta@sycronized.co.uk t mobile my provider has blocked them as they have charged me £13.50 over the last few months [sic]. I have only just noticed on the bill that they have been taking £1.50 out at different times. I was ignoring the messages as I thought it was spam and that if I replied they might charge me. I have never subscribed to them and have never heard of there companies [sic]."

"I have not or would not agree to receiving these spam texts. I get 2 messages on the same day at least once a week with no option to stop them. This has now cost me £108 as a result and desperately want a refund and the text messages to stop. I have no idea what the services are as i have never used them!"

"I have not subscribed to these services and they started last month , I have been charged £2.50 plus vat on each bill - the service advertised is of a adult nature and my phone is used by myself, my girlfriend and at times my friends children who play games, I don't want these text messages."

In addition, one complainant who had interacted with the Service via an MO opt-in reported receiving unsolicited charges but stated s/he had not received any text messages from the Services:

"Consumer has had no messages on his phone
T-mobile have not given him no information [sic]
His bill shows messages being received.
The bill shows 2 messages coming up every tuesday, but he is saying he has not requested them."

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 16 were identified as relating to the Services. RMIT conducted testing on two of these Applications for the Sex Dose and Glam Pleasures Services between 1 November 2013 and 4 November 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 and Appendix C**). The RMIT noted that the whole screen of the landing page 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, on 3 March 2014 the RMIT monitored an Application for the Fuck Hunter 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 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 "45fh1-1.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 a landing page for the "Fuck Hunter" Service (**Appendix D**). 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.

On 18 March 2014 the RMIT monitored the Application that had been obtained during the monitoring session on 3 March 2014, on a different handset (a Samsung S3 Mini handset operating on the Jellybean operating system). The RMIT found that the Application behaved in the same manner when operating on this operating system, as the Application suppressed Service messages.

In addition to the monitoring of the Applications, during the course of the investigation the Level 2 provider supplied the Executive with a sample of the Application. On 19 September 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 by the RMIT on 3 March 2014.

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 3 March 2014, detailed in the "Background" section above. The Executive noted that the Application downloaded automatically when a new browser webpage (fuck-hunter.com) opened in the background while the RMIT was browsing on hardsextube.com and after it had selected a thumbnail.

    The Executive acknowledged that the RMIT were 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 Kaspersky samples between 1 November 2013 and 4 November 2013 and the Application found on the internet on 3 March 2014, detailed above in the "Background" section.

The Executive noted that during the monitoring sessions, 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 1 November 2013, four Service messages (of which three were chargeable) were sent to the handset but suppressed and they stated:

Message 1
"FreeMsg:U have subscribed to Glampleasures videos costs £4.50 per week until you send STOP to 88150, Help:02476998420 Service Provided by Syncronised ltd 16+"

Message 2
http://glampleasures.com//?sync=a38ea1250

Message 3
"Your new sexy content is on its way"

Message 4
"Hope you enjoy!"

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 the Level 2 provider stated that it had received the Application from a third party advertising network in December 2013 and it had not been designed to suppress any messages. 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:

- The monitoring of the samples provided by Kaspersky and conducted by the RMIT 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 for the Glam Pleasures, Sex Dose and Fuck Hunter Services were digitally signed on 24 June 2013, 26 April 2013 and 5 February 2014 respectively. 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 around 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 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 and 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 it stated that it did not accept the monitoring of the Kaspersky samples was a genuine consumer journey, as it stated that the Application was not available to consumers until January 2014. The Level 2 provider submitted that very basic versions of the Application were used on a trial basis by the third party advertising network in early 2013 but only limited consumers would have acquired the Application. It submitted that it could only assume that it was during this time that Kaspersky had obtained the Application. Notwithstanding this, the Level 2 provider stated that the Applications had not been used to generate revenue.

   The Level 2 provider took issue with the monitoring conducted by the RMIT as it stated that the Application provided by Kaspersky had been transferred to a monitoring handset instead of being accessed from the internet. As a result, a full genuine consumer journey had not been obtained. It noted that the monitoring conducted by RMIT had been conducted on an Android 2.2 operating system which it submitted was outdated and not compatible with any modern Android applications. It had been informed that the Application was designed to operate on an Android 3.0 or above operating system. It submitted that use of the Android 2.2 operating system, would affect the warning alerts that a consumer would receive as part of the installation process, and the pop-up windows that would appear on the Application when a reverse billed premium rate charge was about to be incurred which would require a consumer to positively consent to the charges.

   The Level 2 provider stated that the RMIT's monitoring of the Kaspersky samples was not supported by any corroborative evidence of a live online monitoring journey. It raised the issue of the software samples being composed on a system and stored in an unsecured manner by an unrelated third party, which led it to believe that this was not valid evidence.

   The Level 2 provider explained that the Application used an MO opt in, in the same manner that the Glam Pleasures and Sex Dose Services did, as consumers were required to text a keyword to one of the Service shortcodes. It was for this reason that the Level 2 provider stated it did not disclose the use of the Application in early correspondence with the Executive. Notwithstanding this, the Level 2 provider submitted that it believed that any queries regarding the Application should be referred to the third party advertising network.

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

The Level 2 provider denied that the Application was the subject of an automatic download as asserted by the Executive. It submitted that the Application was promoted by online banners advertisements, which included the full cost of the Service and the billing frequency (**Appendix E**). Accordingly, consumers were made aware of the pricing information at the first point of access to the Service. The Level 2 provider highlighted that downloading the Application to a handset did not result in any cost to the consumer other than the cost of internet data and accordingly consumers had been treated fairly.

The Level 2 provider submitted the downloading of the Application was part of a much larger journey involving six steps, where the consumer would have been made aware of the nature and the cost of the Service. In particular, the Level 2 provider stated that the consumers were required to actively install the Application from an unknown source and s/he would be presented with a warning message that informed them that the Application may send messages that cost. The Level 2 provider used the analogy of a train passing through six stations to reach its destination. It stated that at each stage of installation process, there was a specific requirement for the consumer to provide his/her express consent to continue and the consumer was free to withdraw from the process at any point. The Level 2 provider asserted that the six-step process was omitted from the RMIT's analysis of the Kaspersky samples of the Application, which it stated was disappointing.

The Level 2 provider highlighted that for a consumer to download the Application they would be required to unlock a control on their device that grants permission to install applications from outside of the Google Play store. Further, it wished to clarify that downloading the Application did not cause the consumer to be charged.

Reason 2 - the Application suppressed service messages.

In relation to the second reason raised by the Executive, the Level 2 provider reiterated its written submissions regarding the technical problems that it believed existed with the monitoring of the Kaspersky samples of the Application. Further, it stated that as the RMIT had rooted the monitoring handset during its analysis of the Kaspersky samples, this could have led to below average handset performance.

The Level 2 provider strongly asserted that the third party advertising network should be contacted regarding any problems with the Application. It clarified that the third party advertising network was the supplier of the Application software which was a marketing tool for the Services. It had made its Service domains available to the third party advertising network to temporarily integrate the Application software with its Services. The Level 2 provider submitted that the third party advertising network's servers had been hacked by unknown third parties and the Application had been injected with malware.

The Level 2 provider stated that it was reckless to underestimate a hacker's ability to hack websites and servers. Specifically in relation to the Executive's submission that the signature on the Application demonstrated that it had not been tampered with and injected with malware, the Level 2 provider stated that it would be, "a "piece of cake" to redesign an application and then patch it with a fake signature date to make it less suspicious. Further, it submitted that there may be a financial motive for a hacker as they may be aware of the possibility of using the Google push method to take over the Level 2 provider's channels by ensuring that the premium rate text messages were diverted to the hacker's shortcode. It submitted that there

were many reasons why a hacker may be motivated to inject malware and having a financial motive may not necessarily have been the sole reason.

The Level 2 provider submitted that the RMIT monitoring was incomplete because it did not monitor the Service over one calendar month or until the cost of the Service had exceeded £20.00 which would have generated a monthly reminder Service message. Consequently, it submitted that it was incorrect for the Executive to submit that Service messages were not sent when they were not required to be sent.

The Level 2 provider took issue with the Executive's assertion that the complaints for the Services involving an MO opt-in were low due to the suppression of messages. It submitted that the core advertising for Services involving MO opt in produced a low consumer response and accordingly, it disputed that the suppression of messages would have been the sole reason for the lack of complaints.

The Level 2 provider supplied further written submissions following receipt of the monitoring conducted by the RMIT on 18 March 2014. Its submissions reiterated its earlier written submissions and stated that it was concerned about the Kaspersky samples that were provided to the RMIT, as the individual that had provided the samples was not named. It asserted that a member of the RMIT was in fact working for Kaspersky and therefore it stated, "…it is raising a doubt on whose interest is supported by this (dubious) cooperation with individual of unknown identity who provided the offline software samples". Further, it submitted that the evidence from Kaspersky was not valid evidence because it had not been verified by an independent third party.

The Level 2 provider also submitted that it had analysed 11 complaints that it stated had subscribed to one of the Services via an MO and it had found that the consumers had received messages to their phones.

In relation to the monitoring that was conducted on 18 March 2014 using a different handset and operating system, the Level 2 provider stated that it did not accept it as valid evidence as it asserted that the evidence was not conducted live on the internet and did not represent a full consumer journey.

During detailed oral submissions, the Level 2 provider reiterated its written submissions. In addition, the Level 2 provider gave some background information regarding the Level 2 provider's company. It submitted that its advertising budget did not allow it to make the Application fully live until January 2014. It had not gained any significant profit in connection with the Android application as it accounted for a lot less than 20% of its revenue.

It explained that the third party advertiser had provided the Application without charge as part of its marketing consultancy services to the Level 2 provider. It remunerated the third party advertising network on a pay-per-click basis.

The Level 2 provider asserted that the consumer experience of the Application was tested by the Level 2 provider on numerous occasions and it had seen no faults in the service flow. It had no reason to be concerned about the method of operation. The Level 2 provider confirmed that this testing had not required any technical knowledge because it had viewed what a typical consumer would view upon accessing the Services.

In relation to the steps taken by the Level 2 provider to ensure that the Application was safe to use, it referred to the in-house tests that it had conducted before operation and stated that it

had no doubts about the third party advertising network, which was similar to any other consultancy company on the market and the advertising network's reputation would be at issue if there were problems.

The Level 2 provider stated that as soon as it was informed about the malware infection by the third party advertising network, it took all actions to minimise any potential harm. The Level 2 provider stated that it would have taken action at an earlier stage if it had been informed of the problem by the Executive when it had first became aware of the Application. The Level 2 provider confirmed that no Android application was currently being used as a promotion or a method of entry to the Services.

The Level 2 provider set out three methods in which it believed that the Application could have been hacked:

- A hacker may have had the keys for signing the Application, which would have enabled it to "inject" the malicious code into the Application;
- A hacker could obtain access to the signature file but not to the source code which would have involved using a tool "to generate an environment back into a source code". It asserted that a hacker would be able to "inject" malicious code into the Application; and
- A hacker could decompile the file and "inject" malicious code and its own signature into the Application.

In conclusion, the Level 2 provider submitted that a hacker had injected malicious code into the Application and as soon as it had become aware of the problem it had acted to prevent any consumer harm.

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 revenue figures provided for the Services' shortcodes that utilised an MO opt-in revealed a decline in revenue from March 2014 onwards. The Tribunal commented that this appeared to support the Level 2 provider's explanation that upon being informed of the third party network's servers being compromised, it had discontinued the Application, and that this had taken place before notification from the Executive.

The Tribunal noted that the monitoring conducted by the RMIT in March 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 noted that the Level 2 provider had stated that it had tested the Application in early 2014 and had not experienced the suppression of messages. However, 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. The suppression of the Service messages was a feature of the Applications found both by Kaspersky and the Executive in its monitoring in March 2014. Accordingly, the Tribunal concluded that, on the balance of probabilities, the Application in this format had been available to consumers online (whether promoted or not during this entire period) at least from the date the Application was first obtained by the Executive. The Tribunal was satisfied that the suppression of Service messages did not treat consumers 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, C and D)**.

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 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 charges.

In addition, the Executive relied on the Guidance, which it stated makes it clear that all charges must be robustly verifiable. The Executive stated that although the Guidance is not binding on providers, where a provider fails to follow Guidance there is an expectation that it will take equivalent alternative steps to ensure that it fulfils PhonepayPlus' expectations (and compliance with the Code).

During the investigation, the Level 2 provider was directed to provide information in relation to consumers' consent to be charged. The Level 2 provider stated that it had established an ongoing and close working relationship with a third party verifier and had utilised its verification procedures since September 2012. It provided a copy of its agreement with the third party verifier dated 10 December 2013. In response to a further direction for information in relation to the Sex Dose Service, the Level 2 provider stated that there had been an error with the third party verifier's system which had resulted in the systems being bypassed between February 2013 and early June 2013. The Level 2 provider asserted that it was an isolated incident which affected one URL and it had ceased all marketing of this URL as soon as it became aware of the issue and took all possible measures to limit consumer harm.

On 3 September 2014 the Executive contacted the named third party verifier to confirm whether any verification data was available for selected complainants who had interacted with the Titty Tingle Service after June 2013. The third party verifier stated that it "held no data" on the sample of complainants' MSISDNs provided.

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 clicking the screen was part of a much longer process during which a consumer would be made fully aware that they were consenting to be charged. In relation to the second reason, the Level 2 provider did not accept that a breach of the Code had occurred on this basis and stated that it had encountered a technical issue with the third party verifier but in any event it had stored PINs on its internal system, which provided evidence of consumers' consent to be charged.

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 emphasised that the Application landing page was one of the last stages of the Application experience for a consumer (**Appendix B, C and D**). During the earlier stages of the process on online advertising banners, pop-up windows and on-screen alerts, it submitted that a consumer would view pricing information for the Service and accordingly it was not possible for consumers to be unaware of the cost of the Service (**Appendix E**).

The Level 2 provider submitted that all the required information such as pricing information, that it was a subscription Service, the Level 2 provider's name, the opt-out procedure and the customer care number were visible on the Application landing screen. The Level 2 provider submitted that the Code does not define nor state the actual font size required and it could not be held responsible for whether a consumer had read the full terms and conditions or chosen to ignore them.

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.

With regards to the WAP opt-in, the Level 2 provider submitted that it had been using a third party verifier to provide robust evidence of consumers' consent to be charged since September 2012. It highlighted that the third party verifier's system is a robust third party verification system which PhonepayPlus is aware of and has approved previously.

The Level 2 provider explained that it had encountered technical problems on the integration of the third party's verification system. It had obtained a daily record of the webpage from the third party verifier which demonstrated that the terms and conditions had not been interfered with. It had used this in conjunction with its own record of PINs that it kept internally. The Level 2 provider accepted that the Executive had not obtained records from the third party verifier and stated this was likely to be due to the technical error it had encountered. Notwithstanding this, it stated that it had passed the Level 1 provider's due diligence checks each time.

The Level 2 provider explained that it had kept an internal record of consumers' consent to be charged which it had provided to the Executive. It stated that the PINs were stored on its internal static system tool. In addition, the Level 2 provider had implemented an additional step into the opt-in process whereby a further page would be displayed with the terms and conditions and a consumer had to agree before a subscription could be initiated. The Level 2

provider said it had interpreted the Guidance as permitting the storage of unique PINs within the Level 2 provider's internal database providing it was free from external interference.

In addition, the Level 2 provider stated that it had been advised by the third party verifier that the form of verification it was utilising was the best available. In summary, the Level 2 provider stated that it was impossible for a consumer to subscribe to the Services unwillingly because the opt-in flow consisted of two stages, the web MSISDN entry form and a unique internal PIN access through a text message.

The Level 2 provider confirmed that the full online verification system was now in place for all the Services utilising a WAP opt-in. The Level 2 provider stated that it had established a relationship with another independent third party verifier which it hoped would ensure there were no further problems.

During oral representations, the Level 2 provider reiterated its written submissions and stated that the problems had begun in September 2012. Consumers had experienced delays when they visited the relevant third party verifier's webpage and many consumers saw a blank loading page for at least a minute. The Level 2 provider was concerned that consumers would not wait and subscribe to the Service, therefore it had chosen to store its PIN protected opt-ins internally on these occasions, rather than lose subscribers.

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

In relation to the first reason raised by the Executive, the Tribunal noted that the versions of the Application obtained from Kaspersky, the RMIT's monitoring and the sample from the Level 2 provider, all contained the 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 the Level 2 provider's submissions that consumers were provided with the cost of the Service prior to arriving at the landing page of the Application. However, the Tribunal commented that this was not seen during the RMIT's monitoring journey on 3 March 2014 and in any event, 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 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. 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 there was not a clear audit trail that could not have been interfered with. The Tribunal took into account the large number of consistent complaints that routinely stated that consumers 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

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 breach 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.

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 the numerous previous adjudications published concerning the requirement to have and produce, when requested, robustly verifiable evidence of consent to charge; and
- The Level 2 provider had been subject to an adjudication in January 2013 in which sanctions including a fine of £90,000 had been imposed for breaches of the Code including a breach of rule 2.3.3. 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 took into account the following three mitigating factors:

- The Level 2 provider stated that it had suspended use of the Application as soon as it had become aware that it may be causing consumer harm and it had taken action to ensure that such breaches reoccurring were minimised, by ceasing use of any Android applications;
- The Level 2 provider stated that it had proactively approached complainants to offer refunds and many had been refunded.

The Level 2 provider stated that the Tribunal should rely on the revenue figures provided by the Level 1 providers. 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 and mitigating 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

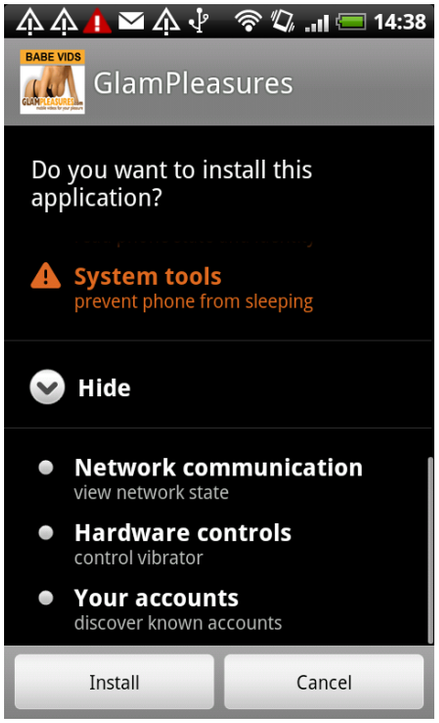
Having regard to all the circumstances of the case, the Tribunal decided to impose the following sanctions:

- 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 £120,000 (which includes a £20,000 uplift that was imposed as a result of the Level 2 provider's relevant breach history);
- a requirement that the Level 2 provider submit to a compliance audit of its procedures for ensuring consumers provide valid consent to be charged and that it has robustly 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

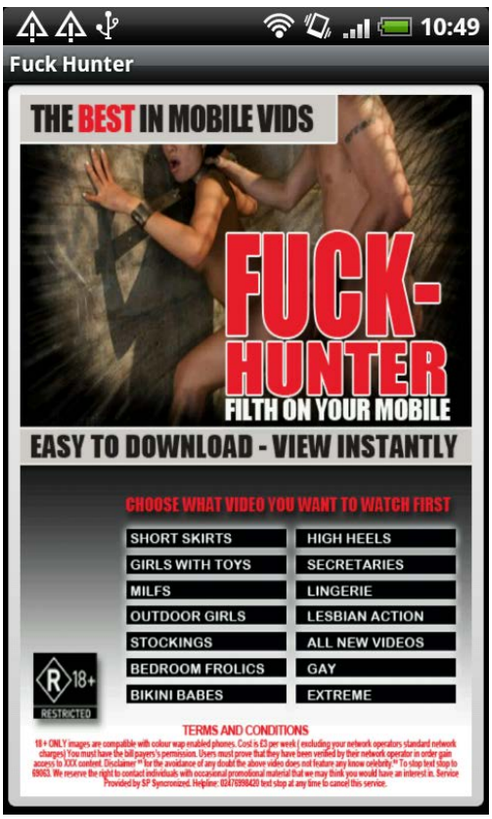
Appendix A – A screenshot of the Application installation process:



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

Appendix C – A screenshot of the Application landing page for the Sex Dose Service:

Appendix D – A screenshot of the Application landing page for the Fuck Hunter Service:



Appendix E – An example of a banner advertisement for the Titty Tingle Service provided by the Level 2 provider: