THE CODE COMPLIANCE PANEL OF PHONEPAYPLUS
TRIBUNAL DECISION

Thursday 10 January 2013
TRIBUNAL SITTING No. 117/ CASE 1
CASE REFERENCE: 10369

Level 2 provider: Syncronized Limited

Type of service: Glamour video downloads

Level 1 provider: Velti DR Limited

Network operator: All mobile Network operators

THIS CASE WAS BROUGHT AGAINST THE LEVEL 2 PROVIDER UNDER PARAGRAPH 4.4 OF THE CODE

BACKGROUND

Since 29 June 2012, PhonepayPlus received 58 complaints from members of the public regarding the "Sex Dose" premium rate subscription service ("**the Service**"), operated by the Level 2 provider Syncronized Limited. The Service was operated on the premium rate shortcode 89066 and offered topless/ glamour video downloads at a cost of £3 per week (via two mobile terminating text message charges at £1.50 each).

Consumers received promotional text messages from shortcode 89066, which presented them with a link. On clicking on this link, consumers were directed to a Service landing page where they were provided with Service cost information and an 'ENTER' link which, when clicked, initiated the premium rate subscription (**Appendix A**).

Generally, complainants reported that they had received promotional material without consenting to receive marketing material and/or they had not consented to incur charges.

The Investigation

The Executive conducted this matter as a Track 2 procedure 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 17 December 2012. Within the breach letter the Executive raised the following potential breaches of the Code:

- Rule 2.3.3 – Consent to charge
- Rule 2.4.2 – Consent to market

The Level 2 provider responded on 4 January 2013. On 10 January 2013, the Tribunal reached a decision on the breaches raised by the Executive.

SUBMISSIONS AND CONCLUSIONS

ALLEGED BREACH ONE
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 submitted that the Level 2 provider had breached rule 2.3.3 of the Code as it had failed to provide robust evidence of consumers consenting to incur charges.

The Executive noted that it had received 58 complaints from consumers in relation to the Service, the majority of whom had explicitly stated that they had not consented to be charged. PhonepayPlus requested evidence of consent to charge in relation to all of the complainants. The Level 2 provider provided spreadsheets containing information from its call logs.

On 2 August 2012, the Executive requested further evidence that would establish that a sample of seven complainants had consented to be charged by the Service. On 14 August 2012, the Level 2 provider confirmed that the complainants, and other consumers, consented to incur charges by clicking on the relevant part of the Service's WAP landing page. The Level 2 provider stated that the Service was monitored by a third party company, which does not derive income from premium rate services and which could be contacted to validate this information. As a result of communication with the third party verification provider, it transpired that it could only verify that a consumer had visited a particular Service landing page. It could not verify that a particular consumer had opted-in to receive charges by clicking on the relevant part of a page.

The Executive relied on PhonepayPlus Guidance in relation to 'consent to charge'. Specifically the Guidance states:

> "[it is] essential that providers can provide robust evidence for each and every premium rate charge…Robust verification of consent to charge means that the right of the provider to generate a charge to a consumer's mobile bill is properly verifiable...By properly verifiable we mean a clear audit trail that categorically cannot have been interfered with since the record, either of consent to purchase or simply of consent to future marketing…was created."
>
> "…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."
>
> "…[Specifically appropriate to the Level 2 provider's service] we would expect providers to be able to robustly verify consent to charge. Factors which can contribute to robustness are:
> - …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;
> - …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; and
> - …Any other evidence which demonstrates that the opt-in cannot be interfered with."

Rule 2.3.3 of the Code states that Level 2 providers must be able to provide evidence which establishes consent. The Executive asserted that the Level 2 provider did not have in place a process that was capable of providing robust evidence of consent and, as a result, the Level 2 provider had not provided evidence which established consent to charge.

The Executive asserted that the evidence of consent provided by the Level 2 provider fell short of being robustly verifiable evidence that could disprove the consistent complainant statements that they had not consented to be charged by the Service. In light of the complainants' accounts that they did not consent to the charges and the Level 2 provider's failure to provide robust verification of consent to charge, the Executive submitted that a breach of rule 2.3.3 of the Code had occurred.

2. The Level 2 provider denied the breach and asserted that it had met PhonepayPlus' requirements. The Level 2 provider stated that it had third party verification in place, which was the best available at the time and provided full and robust verification of consent to charge. However, the Level 2 provider added that it had now implemented a fuller version of the verification service which was able to confirm that a consumer has clicked on a page (rather than just landed on it). In addition, the Level 2 provider asserted that it had never been told that any part of its opt-in process was not compliant with the Code.

3. The Tribunal considered the evidence in detail, including the written submissions made by the Level 2 provider. The Tribunal determined that evidence generated from a provider's own records that had not been independently verified is not robust verification of consent to charge as it is susceptible to interference. The Tribunal acknowledged that the Level 2 provider had subscribed to a third party independent service, which could verify that a particular consumer had visited a Service landing page, but noted that the service could not verify that consumers had completed the required step to opt-in to receive charges. Given the large number of complaints and, in the absence of third party verified records of opt-in to incur charges, the Tribunal was satisfied that not all complainants had consented to the charges and the Level 2 provider had failed to provide evidence that established consent to the required standard in breach of rule 2.3.3. Accordingly, the Tribunal upheld a breach of rule 2.3.3 of the Code.

Decision: UPHELD

ALLEGED BREACH TWO
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 submitted that the Level 2 provider had contacted complainants without obtaining their prior consent and/or had failed to provide sufficient evidence which established that consent to market to consumers had been given.

   The Executive noted that two complainants specifically questioned how they had been contacted without having consented to receive marketing messages from the Level 2 provider.

   On 2 August 2012, the Executive submitted a sample of seven of the complainants' mobile numbers to the Level 2 provider and requested evidence that would establish that the users had consented to receive marketing text messages from the Service. On 14 August 2012, the Level 2 provider confirmed that the mobile numbers received

the direct marketing as they had, "opted in for 3rd party marketing by using a service belonging to one of our 3rd party clients; the customer has given permission to receive marketing of a similar nature". The Executive noted that, in order to market to these consumers in a compliant manner, consumers must have been clearly informed that they were likely to be marketed to and consumers must have taken a positive step to confirm their acceptance (a practice known as hard opt-in).

In addition, the Level 2 provider provided documents from their third party client(s)/data providers in relation to each of the complainants' mobile numbers. The documents contained:

- Screenshots of the third party providers' service that the complainants had previously visited and made a purchased from. The screenshots highlighted a check box that consumers had allegedly ticked to explicitly consent to receiving marketing from third parties, such as the Level 2 provider; and
- Times and dates when the complainants had visited the third party providers' service.

The Executive asserted that the information provided by the Level 2 provider did not evidence that the complainants had in fact ticked the check box. It simply provided the time and date of when consumers had visited the Service's landing pages and a screenshot of what they would have viewed. The Executive submitted that to satisfactorily evidence that the complainants had actually consented to marketing from third parties, such as the Level 2 provider, the Executive would have expected to have received robustly verifiable evidence that the consumer had actually consented. This could have been in the form of a time-stamped record of the consent held by an independent third party as set out in PhonepayPlus Guidance on consent to market. The Guidance states:

> "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 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."

The above Guidance specifically applies to the Level 2 provider's marketing campaign for the Service. Simply providing a screenshot of a consent check box and stating that the complainants had ticked it does not provide robustly verifiable evidence that can be audited by the Executive, to counter the reports by the complainants that they had not consented to receive marketing from the Service.

In light of the lack of robustly verifiable evidence to verify that valid consent to market was given, the Executive submitted that a breach of rule 2.4.2 of the Code had occurred.

2. The Level 2 provider explained that it promoted the Service to consumers who had expressly opted-in for third party marketing whilst using a similar service belonging to one of its third party clients. The Level 2 provider added that, to the best of its knowledge, the numbers it promoted its Service to were opted-in (within six months) and valid mobile numbers of Customers who gave their consent to receive promotional material of adult (18+) genre.

In addition, the Level 2 provider stated that following a recent adjudication (which had been made by consent) against one of its third party data providers, it had terminated relations with that data provider. The Level 2 provider stated that this decision was also due to it having received a high number of complaints in relation to numbers provided by that data provider.

Finally, the Level 2 provider asserted that it had no intention to promote the Service to consumers who did not have an interest in it and that it had no reason to doubt the validity of the data.

3. The Tribunal considered the evidence and noted the Level 2 provider's written submissions. The Tribunal noted the Guidance that providers must be able to provide robustly verifiable proof of each and every opt-in. The Tribunal held that the Level 2 provider had failed to provide such evidence of consent. Further, taking into account the complainants' accounts that they had not consented to receive marketing material, the use of data provided by a third party who had recently accepted a number of breaches of the Code (upon the basis of which the Level 2 had terminated its relationship with that third party) and in the absence of robust evidence of consent, the Tribunal found that consumers had received marketing without their consent. Accordingly, the Tribunal upheld a breach of rule 2.4.2 of the Code.

Decision: UPHELD

SANCTIONS

Initial Overall Assessment

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

Rule 2.3.3 – 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 criterion:

- By being unable to provide robust verification of consumers' consent to charge, which is amongst the most serious of all breaches under the Code, the Level 2 provide committed a breach which is likely to severely damage consumer confidence in premium rate services.

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 breach had a clear detrimental impact, directly or indirectly, on consumers and the breach had a clear and damaging impact or potential impact on consumers.

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

Final Overall Assessment

The Tribunal took into consideration the following aggravating factor:

- The Level 2 provider failed to follow Guidance.

The Tribunal took into consideration the following mitigating factors:

- The Level 2 provider's landing page was monitored by a third party independent company. On being told that the service provided by the third party was not sufficient to verify consent to charge, the Level 2 provider subscribed to a fuller version of the third party's service, which is capable of providing robust evidence of consent to charge going forward.
- The Level 2 provider, prior to receipt of the breach letter, asserted that it had changed its marketing channels by using only Sex Dose marketing banners.
- The Level 2 provider asserted that the Service can now only be accessed using MO opt-in.
- The Level 2 provider asserted that it had provided consumer refunds.

The Level 2 provider's revenue in relation to the Service was in the range of Band 2 (£250,000- £500,000).

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

Sanctions Imposed

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

- A formal reprimand;
- A fine of £90,000; 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.

Appendix

Appendix A: Screenshot of a WAP landing page for the Service: