Tribunal Sitting Number 128 / Case 1

Case Reference: 11743

Level 2 provider	Blue Stream Mobile Limited
Type of service	Entertainment - Adult
Level 1 provider	OpenMarket 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 October 2011, PhonepayPlus received 94 complaints from consumers, regarding an adult pay-per-page WAP video service operated by the Level 2 provider Blue Stream Mobile Limited ("**the Service**"). The Level 1 provider was OpenMarket Limited.

The Service was operated on the premium rate shortcode 69155. The cost of viewing a "set" of videos was £4.50 (or £6.50 for "premium" content). The Service was promoted using mobile text advertisements and banners, which appeared when consumers searched for adult content on the mobile internet.

The majority of complainants stated that they had received unsolicited, reverse-billed text messages and that they had not engaged with the Service. Others acknowledged using the Service, but claimed not to have consented to the amount billed or that they were not aware that any charges would be incurred.

How the Service operated

Consumers, who clicked on an online promotion for the Service (**Appendix A**), were directed to the Service content delivery site (**Appendix B**). Video pages on the website were charged at £4.50 and "premium" content pages at £6, with a minimum of three downloadable items on each page. Consumers were reverse-billed for the Service in increments of £1.50 per text message.

The Level 2 provider stated that for new users the Service worked in the way set out below:

1. Consumer searches for adult content on the mobile internet.
2. Consumer clicks on a mobile text advert/banner.
3. Consumer is routed to a page providing an introductory offer.
4. If the offer is accepted, consumer is routed to the Level 2 provider's Payforit service.
5. Consumer enters his/her MSISDN and consents to an access charge by clicking 'Continue'.
6. Consumer is sent a four-digit Payforit code via SMS.
7. Consumer enters the pin on the Payforit page and clicks 'Buy Now'.
8. Payment is confirmed and consumer is sent a receipt via SMS.
9. Consumer is taken to the Service landing page (WAP landing page) on his/her handset, where the mobile content available for purchase and viewing and/or download is contained.
10. Consumer selects and views the pages that s/he wishes to view and/or download.

The Level 2 provider stated that for return users the Service worked in the way set out below:

1. Consumer searches for adult content on the mobile internet.

2. Consumer clicks on a mobile text advert/banner.
3. Consumer is taken to the Service landing page (WAP landing page) on his/her handset, where the mobile content available for purchase and viewing and/or download is contained.
4. Consumer selects and views the pages that s/he wishes to view and/or download.
5. Consumer receives reverse-billed charges from the service shortcode 69155 for the content that they selected.

The Level 2 provider was not responsible for the Payforit mechanism; therefore, the adjudication did not concern new users who had incurred Payforit charges.

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 31 May 2013. Within the breach letter, the Executive raised the following breach of the Code:

Rule 2.3.3 – Consent to charge

The Level 2 provider responded on 14 June 2013. On 27 June 2013, the Tribunal reached a decision on the breaches raised by the Executive.

SUBMISSIONS AND CONCLUSIONS

ALLEGED BREACH 1

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 acted in breach of rule 2.3.3 of the Code as it was unable to provide robust evidence which established consent to charge for every premium rate transaction.

   The Executive asserted that the Level 2 provider breached rule 2.3.3 for the following reasons:

   Reason 1: The Level 2 provider's records for returning consumers were not held by an independent third party, or in a way that meant that they could not be tampered with.

   Reason 2: Some consumers accessed the Service through a separate application ("App"). The Level 2 provider was unable to provide evidence that established consent to charge for these consumers.

   The Executive relied on the content of PhonepayPlus Guidance on Privacy and consent to charge material. The Guidance states:

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.*"*

The Executive received the following complaints from consumers:

"My phone suddenly started receiving unsolicited text messages late on Saturday night whilst I

was working on my accounts…"

"On the very early hours of Sunday morning I received 47 text messages…I do not know why I started receiving these texts nor did I request as I do not go onto adult sites."

"[H]ave never subscribed to this. received 21 txts charged at £1.50 each within 20 minutes on 3/8. [sic]"

The Level 2 provider confirmed that the complaints listed above were from consumers who were already registered on its database (return users) and therefore the three consumers were not directed through Payforit on their return visits to the Service landing pages.

Reason 1: The Level 2 provider's records were not held by an independent third party, or in a way that meant that they could not be tampered with.

On 23 April 2013, the Executive submitted 50 MSISDNs to the Level 2 provider and requested the following information:

"1. If an independent third party supplies verification for this service, please include full contact details for that third party and a copy of the contract.

"2. If verification data is held internally, please provide details of how it is stored and how this means that it categorically could not have been interfered with.

"3. Please provide evidence of how you are able to robustly verify consent to charge for all of the MSISDNs listed…"

On 30 April 2013 in response to the Executive's request for information, the Level 2 provider supplied an 'Order History' spreadsheet and a 'Transaction log' for each of the 50 MSISDNs. The Level 2 provider confirmed within its response that 32 out of the sample of 50 MSISDNs provided by the Executive were new consumers and therefore 18 MSISDNs related to returning consumers.

The Executive noted that, with respect to the data provided for the 18 returning consumers, the data was not held by a third party and nor was it held in a way which meant it categorically could not have been tampered with since creation.

In addition, within the response to the Executive's request for information, the Level 2 provider clearly stated that a decision had been taken not to implement a third party robust verification process purely on the basis of the cost implications involved.

"…[W]e considered the PhonepayPlus guideline suggestions for robust verification for consent to charge in terms of witnessing of all transactions and determined that it would have required considerable investment and change to our systems to introduce third party witnessing."

The Level 2 provider has stated an intention to, "gradually move our services to the Payforit scheme to provide the independence of charging functionality". However, at the time of the investigation letter only new consumers (such as the 32 MSISDNs referred to above) were routed through Payforit. The Executive noted that the Guidance makes it clear that all charges must be verifiable.

Although 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 fulfills PhonepayPlus' expectations (and compliance with the Code). By its own admission, the Level 2 provider made a conscious decision to ignore Guidance and not implement any alternative robust method of verification. As a result, the Executive submitted that the Level 2 provider did not have sufficiently robust systems in place to provide evidence of consent to charge in breach of rule 2.3.3 of the Code.

Reason 2: Some consumers accessed the Service through a separate application ("App"). The Level 2 provider was unable to provide evidence which establishes consent to charge for these consumers.

As part of the Level 2 provider's response to the Executive's request for information, a 'Robust verification of consent to charge' table was provided for each complainant. The Level 2 provider submitted that two of the sample of 50 MSISDNS had accessed the service via an App.

With respect to the two MSISDNs, the Level 2 provider stated the following:

> "This user used our services via a handset App that was distributed into app stores in 2011 and prior to Moko purchasing the company. There is limited knowledge of how the app works other than it pulls in the same page information that is available on a browser and the App stores the MSISDN of the handset and transfers it to our systems when the user accesses the App."

The Executive noted that the Level 2 provider appeared to have inherited the App, which provided users with pay-per-page content from its website, but had little knowledge of the functionality of the App. The Level 2 provider did not provide the Executive with any details regarding its relationship to Moko.

The Executive asserted that the information provided by the Level 2 provider, to evidence that complainants had consented to charges, was not sufficient to provide robustly verifiable evidence that could disprove the consistent complainant statements that they had not consented to receive charges from the Service.

As a result, the Executive asserted that the Level 2 provider has failed to establish that it is, "[A]ble to provide evidence which establishes…consent," for consumers who used the Service through the App.

In light of the above, the Executive submitted that a breach of rule 2.3.3 of the Code had occurred.

2. The Level 2 provider denied that it had acted in breach of the Code.

The Level 2 provider stated that the Executive had quoted selectively from previous correspondence to support a series of assertions, including that, "the Level 2 provider made a conscious decision to ignore Guidance and not implement any alternative robust method of verification". The Level 2 provider stated that this was not correct, as consideration of the full explanation in previous responses made clear. It stated that it was regrettable that the Executive has misrepresented the position in this way.

The Level 2 provider added that the scope of the adjudication was "ambiguous", on the grounds

that a number of complaints that did not relate to the shortcode under investigation were referred to by the Executive, and to various references by the Executive to consumers who have in fact been identified as "new consumers", where the required level of verification has been accepted as being provided by the Level 1 provider.

The Level 2 provider noted that the Executive had stated that it had, "only considered the return user journey, as the responsibility to provide robust verification for return users lies solely with Blue Stream Mobile Limited". The Level 2 provider asserted that in reality, this meant that the Executive's criticisms related to 18 complaints for returning users and two App users. The Level 2 provider submitted that each of these returning users were verified by the Level 1 provider at its request.

The Level 2 provider asserted that the fact that the complaints from "new users" had been found to be unsubstantiated in the light of the verification provided by the Level 1 provider, would tend to suggest that the complaints by the remaining 18 "return users" and two App users should have also been approached with some skepticism. It asserted that the Executive, "will no doubt have had the benefit of speaking to the complainants and putting it to them that the records show that they consumed our services on many occasions. We have not been informed of any follow up with the complainants."

Evidence of consent to charge

The Level 2 provider stated that it had previously supplied PhonepayPlus with the "raw data" logs for each MSISDN referred to, which was, "a table of raw information which is dated/timestamped securely for each click a consumer makes whilst they navigate throughout our site." The Level 2 provider stated that the logs are, "industry-recognised as a robust and accurate method of demonstrating consent to charge". Further, it asserted that the fact that the process for repeat customers was not witnessed by a third party did not mean that the evidence could be discounted.

The Level 2 provider noted that the requirement of rule 2.3.3 is that:

> "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".

The Level 2 provider submitted that the concept of "robust verification of consent" was not an element of the Code or the underlying legislation, rather a construct of PhonepayPlus Guidance. It asserted that it should not be treated as if that were the text of the Code. It added that:

> "The position is that our internal logging system records were and are sufficient to demonstrate a user's activity and to establish consent, and provide a clear audit trail of such activity. The Executive does not say that the records have been tampered with, nor is there any reason or evidence which could support any such allegation. At no time has PPP asked for direct access to our logging systems, despite us having an open dialogue with them and having previously indicated that we would be willing to discuss such options."

In addition, the Level 2 provider stated that :

> "[O]nce a customer has been securely verified through Payforit during their first interactions, the customer is always passed back to OpenMarket during any subsequent visits in order for us to securely establish whether the alias is pre-existing in our records or not. It enables us to

verify the consumer's identity for billing purposes. Therefore, even in relation to the 18 complaints which relate to "return users" on this short code, Open Market will be able to independently produce records of the users being passed through their systems on the date and times that our records show the users were accessing our services.[sic]"

Complaints relating to the App

The Level 2 provider stated that, "a small percentage" of users obtained content via the App. It noted that the examples referred to by the Executive represented about 4% of the total number of complaints relied on in this investigation. It added that, the App required a user to download it, meaning that the consumer had to take specific, positive action. Prior to installation, every user would have clicked on an "accept" button stating that the App will use the MSISDN information. Pricing information was clearly provided at that stage.

Installation was free and charges were incurred in the same way as the user flow for WAP users, as tested by the Executive. The Level 2 provider asserted that in its view it was difficult to see how it can be alleged that there was no evidence of consent to charge in circumstances where contact had clearly been initiated by the consumer; the consumer had to proactively download and install an App, and clear charging information had been provided prior to installation and on each and every subsequent use. Moreover, any users who did proactively download and make use of the App were subject to the same method of secure data logging through the systems referred to above. It reiterated that it was able to provide "raw data" logs for each transaction which instigated a charge to the consumers' handset.

The Level 2 provider reiterated that the App model was deployed by its previous owners and had ceased operating. It noted that the Executive had not previously asked for an explanation of the relationship between itself and its previous owners in writing; however it had advised the Executive that MOKO was the new parent company in or around December 2011. The registration details of active directors were updated. Although aware of the existence of the App, the new owners did not focus on that element of the Services, given its small overall contribution to the business. As confirmed above, the App service was terminated.

The Level 2 provider stated that it had a generous refund policy and that it was willing to issue full refunds to any consumers who have specific complaints about the App. However, it added that the majority of consumers, who contacted its support centre to query charges, and who did download the App, recalled and acknowledged having interacted with its Services.

Approach to verification and discussions with PhonepayPlus

The Level 2 provider stated that it had had many discussions with PhonepayPlus regarding its services. However, its evidence of its consent to charge mechanism had never been an agenda item in those discussions. It added that the Executive's statement that it, "made a conscious decision to ignore Guidance and not implement any alternative robust method of verification," was simply untrue. It asserted that at the time that consent to charge was implemented, it was in direct discussions with the Level 2 provider regarding the industry adoption of Payforit4 – which was recognised as an industry-approved mechanism of robust consent. It stated that during March 2012, it instigated the process of integrating the Payforit4 mechanism within its platform and had numerous meetings with the Level 1 provider regarding this. However, in the light of the rapidly changing UK marketplace, both in terms of regulation and competition, it had sought proactively to

update its services in order to remain a key player within the industry, as well as providing a high-level service to its consumers inline with regulations. Consequently, following its development early last year, it sought to obtain and implement the Payforit Single Click mechanism via ImpulsePay. It added that it again recognised this to be an approved and accepted robust method of billing and consent within the industry.

Unfortunately the model was for a time restricted to one Level 2 provider within the marketplace, giving that provider an unfair advantage within the industry. It asserted that despite its best efforts, firstly to obtain this service via its existing (and exclusive) aggregator (the Level 1 provider), and subsequently working alongside other industry members to try and obtain access for all providers, it was only able to secure use of the model at the end of 2012. The model was successfully implemented in February 2013. It stated that it was currently in the process of migrating all its consumers towards this model. After the initial 60 days, over 50% of its revenues were derived through what the Level 2 provider asserted was a "PhonepayPlus/ industry approved" mechanism and this figure had slowly risen over recent months.

The Level 2 provider stated that PhonepayPlus had only recently (29th May 2013) released a document which suggested that Payforit alone is not sufficient to demonstrate consent to charge and that independent witnessing is also required. The Level 2 provider stated that, irrespective of that industry update, in order to achieve the level of "evidence" which PhonepayPlus considers is required by the Code, it had already started the process of integrating with Goverifyit (a third party verification provider) in order to provide third-party witnessing of all consumer transactions. This process was instigated at the beginning of May 2013 and was anticipated to go live within a matter of weeks.

3. The Tribunal considered the evidence, including the Level 2 provider's detailed submissions. The Tribunal accepted that a provider was free to depart from Guidance where it could demonstrate that it had taken steps which are equally as effective at meeting the Code outcomes and rules as those set out in Guidance. The Tribunal found that in this case the Level 2 provider submitted little evidence to demonstrate that it had taken steps which met the Code outcomes and it had not provided robust evidence of consent to charge in relation to the "returning users". In relation to the App, the Tribunal concluded that the Level 2 provider had acted in breach of rule 2.3.3 for the reasons given by the Executive. Accordingly, the Tribunal upheld a breach of rule 2.3.3 of the Code.

   In addition, the Tribunal questioned whether data provided by the Level 2 provider could properly be described as "raw data", as it appeared to have been processed by the Level 2 provider. The Tribunal commented that had the data been provided by an independent third party, a certain amount of presentational processing may have been permitted.

Decision: UPHELD

SANCTIONS

Initial Overall Assessment

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

Rule 2.3.3 – Consent to charge

The initial assessment of rule 2.3.3 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.

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

Final Overall Assessment

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

- A provider is not obliged to follow Guidance. However, the alternative steps that the Level 2 provider maintained that it took were not sufficient to meet the Code outcomes.
- There have been a number of relevant prior adjudications in relation to compliance with rule 2.3.3.
- Although the Level 2 provider terminated the App, from the time the Level 2 provider was first contacted by PhonepayPlus to the time the Service was suspended (for reasons unconnected with the investigations) the breach continued in relation to the non-App consumers.

The Tribunal noted that the Level 2 provider had been subject to an adjudication on 22 December 2011. However, the Tribunal determined that the adjudication did not constitute relevant breach history and therefore did not attach any weight to it.

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

- The Level 2 provider discontinued use of the App.
- The Level 2 provider stated that it had issued a significant number of full and partial refunds to both "new" and "return" users.
- The Level 2 provider stated that it had begun the process of integrating with Goverifyit in order to provide third party witnessing of all consumer transactions.

The Level 2 provider's revenue in relation to the Service was in the range of Band 1 (£500,000+).

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

The Tribunal had regard to the fact that, according to the Level 2 provider, 65% of the revenue was generated from return users and 2% from the App.

The Tribunal noted that the Level 2 provider submitted that it was inappropriate for the Tribunal to consider any revenue prior to 10 May 2012. This was on the basis that a Compliance Update clarifying Guidance on Privacy and consent to charge was published on this date. The Tribunal noted that the May

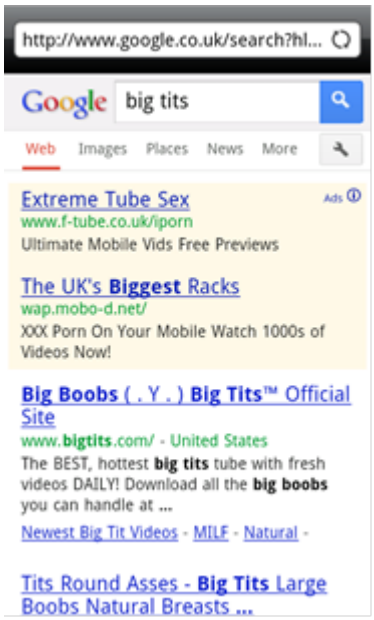
2012 update concerned rule 2.4.2 and soft opt-in; therefore it was not relevant to the issues raised in the instant adjudication. The Tribunal noted that the Guidance relating to rule 2.3.3 came into force in September 2011 (and was published in advance of this date). In addition, the Tribunal commented that the determination of the relevant period of revenue to be taken into consideration was a matter for the Tribunal. The Tribunal noted that there was a discrepancy between the revenue figures provided by the Level 1 and 2 providers. In any event, both figures were in Band 1 (£500,000+). As a result of this and having regard to its maximum fining power for one very serious breach of the Code, the Tribunal determined that it was unnecessary to make a determination as to the exact revenue.

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

- a formal reprimand;
- a fine of £150,000; 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.

APPENDICES

APPENDIX A: Screenshot of promotional material for the Service:



APPENDIX B: Screenshot of a Service landing page: