

BETWEEN:

PHONE-PAID SERVICES AUTHORITY LIMITED

Executive

-and-

THE HUB GROUP LIMITED

Respondent

---

**ADJUDICATION BY CONSENT (“CONSENT ORDER”)**

---

ON the matter being considered under the Phone-paid Services Authority case reference 98530

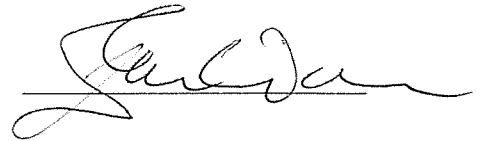
AND ON the parties having agreed breaches of the Phone-paid Services Authority Code of Practice (“the Code”) as set out in the Case Report (Warning Notice Settlement) produced in the Schedule to this order, and appropriate sanctions and administrative costs to be imposed on the Respondent, in order to dispose of the matter

***By consent it is ordered that***

1. *The alleged breaches of the Code set out in the Case Report (Warning Notice Settlement) and produced in the Schedule shall be upheld.*
2. *The following sanctions shall be imposed in respect of those upheld breaches:*
  - a. *a fine of £150,000;*
  - b. *a formal reprimand;*
  - c. *A requirement that the Respondent seek and implement compliance advice to the satisfaction of the Executive, prior to the commencement of any premium rate services, for a period of 5 years from the date of this consent order*
  - d. *a requirement that the Respondent 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 the Phone-paid Services Authority that such refunds have been made.*

3. *The Respondent shall pay administrative charges incurred by the Phone-paid Services Authority in relation to this case in the sum of £5,820 within 28 days of this order.*

A handwritten signature in black ink, appearing to read 'Ian Walden', written over a horizontal line.

*Professor Ian Walden (Chair)*

*On behalf of the Phone-paid Services Authority Tribunal*

*6 February 2018*

# Case Report (Warning Notice Settlement)

## Background

### The parties

The case concerned a games subscription service operating under the brand name 'Playzone' on shared shortcode 65466 (the "Service").

The Level 2 provider for the Service was The Hub Group Ltd (the "Level 2 provider"). The Level 2 provider registered with the Phone-paid Services Authority on 14 December 2015.

The Level 1 provider for Service shortcode 65466 was Zamano Solutions Limited ("Zamano").

### The Service

The Service was stated to be a games subscription service charged at £4.50 per month. The Executive understood that consumers could enter the Service via a wireless application protocol ("WAP") PIN opt-in or mobile originating ("MO") opt-in.

The Level 2 provider stated that the service was promoted from 20<sup>th</sup> January 2016 to 29<sup>th</sup> February 2016 and ceased operation on 30 April 2016.

The Level 1 provider stated that the service commenced operation on 25 February 2016 and was suspended on 9 May 2016.

The Level 2 provider amended its organisation registration on the PSA Registration Scheme from 'registered - paid' to 'Left the PRS market' on 5 July 2016. The Executive therefore understood the Level 2 provider no longer operated in the UK premium rate market.

The Level 2 provider has provided the following user flow for the Service:

USER DISCOVERS PROMOTIONAL BANNER ON--LINE.  
USER RESPONDS TO AD AND LANDS ON GAMES NATION OFFER PAGE  
USER DIGESTS OFFER AND FOLLOWS INSTRUCTIONS  
USER ENTERS THEIR MSISDN IN THE MSISDN ENTRY BOX AND CLICKS THE ENTER  
BUTTON  
PLAYZONE RECEIVE THE REQUEST VIA IP AND GENERATE A REQUEST TO PIN  
PROVIDER (GO VERIFY OR RELIANCE--IOM) FOR A PIN TO BE SENT TO THAT MSISDN.  
THERE IS ERROR HANDLING ON THE SITE IN EVENT OF INCORRECT MSISDN BEING  
ENTERED.  
PAGE RE--DIRECTS TO AN ENTER YOUR PIN BOX.  
PIN PROVIDER SEND THE PIN BY TEXT WHICH ARRIVES IMMEDIATELY  
USER GRABS THE FOUR DIGIT PIN AND ENTERS IN THE PIN BOX.  
USER HITS THE SUBSCRIBE BUTTON.  
THE USER IS SENT A PREMIUM--MT MESSAGE THAT CONTAINS THE PROSCRIBED  
SUBSCRIPTION WELCOME TEXT AND LINK TO THE BROWSER PORTAL.  
THE USER CAN REPLY STOP TO END THEIR SUBSCRIPTION  
THE USER CAN CLICK ON THE LINK TO ACCESS THEIR CONTENT

THE LINK REMAINS PERMANENTLY ACCESSIBLE AS LONG AS THE USER REMAINS SUBSCRIBED  
THE LINK IS SENT TO THE USER EACH MONTH AS PART OF THE MONTHLY CHARGING.  
THE USER WILL NEVER PAY MORE THAN £4.50 PER CHARGING PERIOD OF 30 DAYS.  
THE USER CAN CEASE THE SUBSCRIPTION AT ANY TIME BY SENDING STOP TO THE SHORTCODE.

### **Summary of complaints**

The Executive received 37 complaints concerning the Service since 2 March 2016.

Complainants variously alleged that the Service charges were unsolicited.

A sample of complainant accounts is below:

*"I noticed this charge in my mobile phone bill. It appeared as a Premium Shortcode Text Service. No number or other details appear on the bill. The charge appeared twice on the last and previous bills. I checked my text messages and found 2 messages from 65446 which appears to be a Premium Shortcode for a service called "PlayZone".*

*"To the best of my knowledge I have not signed up for this 'service'. To my mind this 'service' and its associated charges are completely unsolicited."*

*"Reading up on your recommended course of action I have tried to contact the provider but they are never available. My understanding is that this is a third-party service."*

*"I wish to stop further charges for this 'service'."*

*"I didn't sign up to this service. This is an unsolicited text, charging me £4.50 for the privilege of receiving it."*

### **Breaches of the Code**

The Executive believed that the service contravened the Phone-paid Services Authority Code of Practice 13<sup>th</sup> and 14<sup>th</sup> Editions (the "Code") and in particular alleged breaches of the following Code provisions:

Code 13 rule 2.3.3 – Consent to charge

Code 13 para 4.2.4 and Code 14 para 4.2.2 – Provision of false information to the Phone-paid Services Authority.

#### **Breach 1**

Outcome 2.3 provides:

**"Fairness**

***That customers of premium rate Services are treated fairly and equitably."***

Rule 2.3.3 of the Code:

***"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 Executive submitted that the Level 2 provider had breached rule 2.3.3 of the PSA Code of Practice, 13th Edition as the Level 2 provider had charged consumers without their consent and had not provided evidence of robust verification to establish consumers' consent to be charged.

The Executive relied on correspondence exchanged with the Level 2 provider and Level 1 provider, complainant accounts, and PSA's General Guidance Note 'Consent to Charge' in support of the PSA Code of Practice, 13th Edition (the "**Code 13 Guidance**")

The Level 2 provider stated that opt-ins were via PIN only, and were verified by third party verification companies Go Verify It (GVI) and Reliance IOM:

*"The Hub Group signed up subscribers between early January and late February 2016 using Web PIN Flow model with a 3<sup>rd</sup> party independent verifier, as advised in previous correspondence. The offer was for a £4.50 per month subscription service with first month free, offering unlimited game downloads. The independent verifiers were GVI and Reliance India."*

According to the Level 2 provider, the service was promoted from 20<sup>th</sup> January 2016 to 29<sup>th</sup> February 2016 and ceased on 30 April 2016. The time period for the operation of the service as stated by the Level 1 provider was 25 February 2016 to 9 May 2016, at which point the Level 1 provider had taken the decision to suspend the service, as confirmed in correspondence to the Executive.

The contract between the Level 1 provider and the Level 2 provider in respect of the service was signed and dated 26 February 2017 (the day after the Level 1 provider confirmed the service commenced operation).

Message logs were supplied to the Executive by the Level 2 provider. The message logs demonstrated that the consumer opt-ins to the service pre-dated 25 February 2016, which is the date the Level 1 provider confirmed the service commenced operation on its platform.

The Executive asserted that the Level 2 provider did not hold robust evidence of consent to charge for any consumer subscribed to the service, for the following reasons:

#### Go Verify It (GVI)

The correspondence with GVI made it clear that the Level 2 provider never contracted with GVI and that GVI had never provided the Level 2 provider with a 3<sup>rd</sup> party verification service. As such, there were no records of consent to charge held by GVI and the Level 2 provider had therefore not provided robust verification of consent to charge consumers via GVI.

#### Reliance IOM

The Reliance IOM verification web portal was not robust or adequate as the data was not in a secure format and could be interfered with as information was only uploaded onto the Reliance IOM web portal on request.

The Level 2 provider had supplied evidence of a contractual relationship with Reliance IOM. The contract with Reliance IOM ran from January 2016 and that the PIN verification operation commenced on 14 January 2016.

In response to the Executive's request for service opt-in information (including third party verification) for a sample of complainant mobile telephone numbers, the Level 2 provider supplied opt-in dates and 3<sup>rd</sup> party verification information from Reliance IOM showing same day verification.

The Executive subsequently made direct enquiries of Reliance IOM requesting robustly verifiable evidence of consent to charge, but the Executive did not receive a response. The Executive therefore requested that the Level 2 provider obtain the requested information directly from Reliance IOM. The Executive was subsequently provided access to a Reliance IOM online web portal by the Level 2 provider, to enable the Executive to verify MSISDN PIN opt-ins, by entering MSISDNs on the web portal.

The Executive noted there was no real-time access to the opt-in data upon request and issued a further direction for information to the Level 2 provider, which stated:

*"The Executive has found no evidence of consent to charge for the following MSISDNs on the Reliance portal or Go Verify It. A search on the Reliance portal returned no data for the MSISDNs and Go Verify It have advised The Hub Group have never been a client."*

The Level 2 provider was requested to provide robust verifiable evidence of consent to charge for a number of MSISDNs.

The Level 2 provider responded by supplying message logs containing free and chargeable messages. It suggested that the difficulties may have been due to Reliance IOM only uploading data to the portal that had been specifically requested.

The Executive's view was that the Reliance IOM verification web portal was not robust or adequate, as the data was not in a secure format and could be interfered with as information was only uploaded onto the Reliance IOM web portal on request.

When the Executive viewed the message logs supplied by the Level 2 provider for the same MSISDNs, it saw that the opt-in dates supplied to the Executive by the Level 2 provider were different from the opt-in dates shown in the message logs. In addition, when the Executive viewed the information from the Reliance IOM web portal, the verification date was shown as the date of first billing and not the date of opt-in. When the Executive queried this, the Level 2 provider advised:

*"Playzone policy was then to return to users with the free SMS message containing a landing page link on the intended date of first billing and would then record the user's continued consent to charge"*

Upon being informed of the discrepancies, the Level 2 provider informed the Executive that a free SMS message containing a landing page link on the date of first billing recorded the user's consent to charge.

The Executive noted that, while there was evidence in the message logs of users being sent a free SMS message in the Level 2 provider's message logs, there was no evidence that this SMS contained a landing page link. In addition, the "user flow" and the promotional material

supplied by the Level 2 provider made no mention of any double/second opt-in on the date of intended first billing. There was also no real-time access granted to the opt-in data from Reliance IOM upon request. As such, the Executive's view was that the Level 2 provider's response of 22 was not a credible explanation for the discrepancy in recorded opt-in dates.

Due to the discrepancies between what was contained in the response to the request for information, the Reliance IOM portal and the message logs supplied by the Level 2 provider, the Executive asserted that there was no robust evidence of consent to charge via the Reliance IOM verification method.

### Zamano

Additionally, the Level 2 provider told Zamano on its Due Diligence and Risk Control form as part of the process of contracting with Zamano to provide the service, that it was migrating a database from another aggregator. However, the Level 2 provider had stated in correspondence with the Executive that there had been no migration of the database from another aggregator. The Executive considered this to be a significant inconsistency, with the consequence is that there was no robust evidence of consent to charge consumers in the form of a migrated database.

For the reasons set out above the Executive submitted that the Level 2 provider had been unable to provide sufficient evidence which established consent to charge complainants and that, accordingly, the Level 2 provider had acted in breach of rule 2.3.3 of the Code.

### **Provider's response**

The Level 2 provider accepted that it did not conclude a contract for independent third party verification with GoVerifyIt ("GVI") during the lifetime of the service. It had, however, been in discussions with GVI to provide third party verification between December 2015 and February 2016. The Level 2 provider had shared a technical integration document with GVI and a high degree of readiness was achieved on the Level 2 provider's side to proceed with the GVI third party verification solution. The existence of discussions had been confirmed by GVI. The Level 2 provider had never purported to rely on logs or other materials from GVI as evidence of consent to charge in respect of any of the complaining MSISDNs.

The Level 2 provider relied on message logs and opt-in verification from Reliance India O.M. LLP ("**Reliance**"). The Level 2 provider maintained that the Reliance logs – being held by a disinterested third party verifier – did provide credible evidence of consent to charge. However, the Level 2 provider accepted that Reliance did not allow for real time access to opt-in data and, therefore, was not as robust as it could have been.

### **Parties' agreement on Breach 1**

The Level 2 provider was, accordingly, prepared to admit a breach of rule 2.3.3 of the 13th Code on the basis that the evidence it held of its consent to charge was not sufficiently robust. On consideration of the provider's response the Executive accepted that the logs were held by a disinterested third party and noted the provider's acceptance that the lack of real time access to opt-in data rendered the evidence of consent to charge insufficient. Accordingly, the parties agreed that a breach of rule 2.3.3 should be upheld.



## **Breach 2**

Paragraph 4.2.4 – Provision of false / misleading information (Code 13) and  
Paragraph 4.2.2 – Provision of false / misleading information (Code 14)

***“A party must not knowingly or recklessly conceal or falsify information, or provide false or misleading information to the PSA (either by inclusion or omission).”***

The Executive submitted that the Level 2 provider had breached paragraph 4.2.4 Code 13 and 4.2.2 Code 14, as the Level 2 provider had supplied information to the Executive on two occasions which was false and misleading. On the first occasion, the information it had supplied regarding the company it used in order to provide robust third party verification for the Service was false. On the second occasion the Level 2 provider had supplied misleading opt-in and PIN verification information.

### Go Verify It contract information

The Level 2 provider had stated to the Executive on two occasions that it was using the services of GVI to verify consumer opt-ins. There had been a significant lapse of time between these representations being made and the Executive therefore submitted that the Level 2 provider must have known that there was no contractual relationship in existence. This view was supported by the fact that the Level 2 provider had supplied a written contract to evidence its relationship with Reliance IOM, but had not provided any such contract with GVI.

Although the Level 2 provider has stated that there was a contract with between it and GVI, this was disputed by GVI and there was no other available documentary evidence to support the Level 2 provider’s statement. In particular, the Level 2 provider had not provided a contract, or any other written communication.

The Executive therefore submitted that the statement made by the Level 2 provider, namely that it had engaged the verification services of GVI, was false. Furthermore, the Executive submitted that the Level 2 provider had made the false statement with the intention of misleading the Executive into believing that the Level 2 provider had obtained third party verification of consent to charge consumers of the service through GVI, when in fact this was not the case.

Accordingly, The Executive submitted that the Level 2 provider had provided false and misleading information to the PSA during the investigation into the Service, in breach of paragraph 4.2.4 Code 13 and 4.2.2 Code 14.

### Opt-in and PIN verification information

As stated for the reasons given above for a breach of Code rule 2.3.3 Consent to charge, the Executive submits that a breach of Code paragraph 4.2.4 (Code 13) and 4.2.2 (Code 14) has also occurred for these reasons.

On 10 May 2016 the Level 2 provider had supplied opt-in data to the Executive’s Contact Assessment Team in respect of a sample of complainant MSISDNs . The information supplied showed the purported dates of opt-in and showed that Reliance IOM had verified the opt-ins



on the same dates shown. However, the Reliance IOM web portal subsequently showed that the opt-in verification occurred on the date of first billing and not the date of actual opt-in as previously stated by the Level 2 provider.

In light of the above, the Executive submitted that the Level 2 provider had provided false and misleading information to the PSA during the Executive's investigation into the Service in breach of paragraph 4.2.4 Code 13 and 4.2.2 Code 14.

### **Provider's response**

The Level 2 provider had been in discussions with GVI concerning the provision of third party verification services between December 2015 and February 2016. The Level 2 provider had shared a technical integration document with GVI and a high degree of readiness was achieved on the Level 2 provider's side to proceed with the GVI third party verification solution. In light of those advanced discussions, it was open to the Level 2 provider to use GVI for independent third party verification on any date from 24 February 2016 onwards. However, for reasons of cost, it had ultimately decided not to proceed with GVI, but to call on the third party verification services of Reliance instead. No contract was ever concluded with GVI.

At no point during the investigation procedure did the Level 2 provider purport to rely on GVI logs, records or data as evidence of consent to charge the complaining MSISDNs. On the contrary, it had consistently referred the Executive to logs and a records portal maintained by Reliance – which was the third party verification provider it had ended up using.

In the circumstances outlined above, the Level 2 provider's indication to the Executive that the GVI service was available to it from 24 February 2016 was neither false nor misleading - in that the Provider had the potential to call on GVI's services from that date onward. With hindsight, it could perhaps have been clearer that GVI had not actually provided verification services for the complaining MSISDNs. However, at the relevant time, the Level 2 provider considered that this would be reasonably clear to the Executive from the fact that it had referred to the Reliance logs and records. The Level 2 provider strongly denied that it knowingly or intentionally misled the Executive in this regard.

The Executive had not identified any discrepancy between the records of the first chargeable transaction for any complainant held by the Level 2 provider in its Customer Relationship Management (CRM) helpdesk database and (ii) Reliance on its on-line portal.

The Executive had, however, identified a discrepancy between the records of the initial customer contact dates and times held on the Level 2 provider's CRM database and (ii) the Reliance portal. The Warning Notice represented the first instance on which the Executive had highlighted this discrepancy – which was not previously raised with the Level 2 provider notwithstanding that the CRM logs were provided in May 2016 and the Reliance data was provided in October 2016.

The Level 2 provider had been given a very limited time to carry out the technical investigation required to reconcile the discrepancy. Its request for a 17 day extension of time for responding to the Warning Notice was refused on the 27th October – albeit a much more limited extension was granted on 7 November 2017 in light of IT difficulties experienced by the Level 2 provider.

A proper technical investigation of the discrepancy involved:

- 1) Examining log-files of tens of thousands of traffic visits, and marrying these with a SQL table containing MSISDN's that were inputted by the user and stored.
- 2) Establishing the true dates and times of each contact between THG servers and the user's on-line visit and MSISDN entry before a successful transaction was executed by PIN.
- 3) Ascertaining the type of transaction undertaken on each log-file stored.

For example many users arrived on the web-site, entered the MSISDN and then did not proceed to register. The same user may return to seeing the same promotion a week later and proceed to registration.

The Level 2 provider had not yet been able to determine whether all the marketing traffic log files, which were often held in temporary memory and dated back to January 2016, were even still stored.

In light of the above, the Level 2 provider had been unable to undertake a proper reconciliation of the opt-in data held by the CRM database and the data provided to the PSA from the Reliance on-line portal within the short space of time available to respond to the Warning Notice. The Level 2 provider continued to undertake the necessary enquiries and reserved the right to provide further information/make further submissions to the PSA on this point once those enquiries were completed.

Based on the enquiries that the Level 2 provider had been able to carry out to date, the Level 2 provider believed its own CRM helpdesk report had captured a first visit by a user and logged it incorrectly as a completed visit (although no transaction or billing event was made).

The Level 2 provider strongly denied that it knowingly or intentionally misled the Executive in this regard. Based on its investigations to date, any discrepancies were likely to be due to problems in the CRM logs.

## **Parties' agreement on Breach 2**

The Level 2 provider was, accordingly, prepared to admit a breach of paragraph 4.2.2. (13th Code) and 4.2.4 (14th Code) on the basis that, during the course of the investigation, it had informed the Executive that it held a contract with Go Verify It (GVI) to provide independent third-party verification when this was not the case. The Level 2 provider was also prepared to admit a breach of paragraph 4.2.2. (13th Code) and 4.2.4 (14th Code) on the basis that accepts that there were discrepancies between respondent information, third party verifier Reliance IOM information and message logs provided to the Executive, which was likely caused by technical problems with its systems.

On consideration of the provider's response the Executive accepted that, although false information had been supplied by the Level 2 provider, it was satisfied that the Level 2 provider had not done so knowingly or intentionally. Accordingly, the parties agreed that a breach of paragraph 4.2.2. (13th Code) and 4.2.4 (14th Code) should be upheld on this basis.

## **Service Revenue**

The Level 2 provider's gross revenue for the Service was in the range of Band 4 (£100,000 - £249,999).

### **Executive's Assessment of Breach Severity**

Rule 2.3.3 (Code 13) Consent to charge - Very Serious

Para 4.2.3 (Code 13) and Para 4.2.2 (Code 14) Provision of false information to the Phone-paid Services Authority - Very Serious

### **Recommended Initial Sanctions**

The Executive recommended the following initial sanctions:

- a formal reprimand
- a prohibition on the Level 2 provider for a period of 5 years from publication of this decision or until payment of the outstanding fine amount in full, whichever is later
- a requirement that the Level 2 provider 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 provider evidence to the Phone-paid Services Authority that such refunds have been made
- a £500,000 fine

### **Overall Case and Proportionality Assessment**

#### **Overall case seriousness**

The Executive considered the case overall to be very serious.

The Level 2 provider considered the case overall to be **significant** or **serious** in light of the following features of the admitted breach of rule 2.3.3:

- the very limited duration of the breach
- the limited number of complaints, which were indicative of limited (if any) consumer harm
- the fact that the Level 2 provider sought to put in place appropriate third party verification procedures, but these unfortunately fell short. This demonstrated that any breach was (if anything) negligent rather than intentional or reckless

#### **Aggravating and mitigating factors going to the case as a whole**

The Executive noted the following aggravating factor, which was accepted by the Respondent:

- previous adjudications have made clear the importance of ensuring that consumers' consent to charge is obtained and that robustly verifiable evidence of this is held and supplied upon request

The Respondent noted the following mitigating factor, which was accepted by the Executive:

The respondent sought to redress consumer harm by offering refunds upon request. When the Executive contacted a random sample of complainants, they had confirmed that they had received a refund.

### **Need to remove financial benefit/achieve deterrence**

The Executive's estimate of service revenue flowing from apparent breaches was £318,223. The Level 2 provider had charged consumers in the knowledge that it did not have robust, verifiable evidence to demonstrate consent to charge the consumers over the relevant time period, and the Executive therefore estimated that the entirety of the service revenue generated flowed from this breach.

The Executive considered there was a need to recommend sanctions which would remove the financial benefit derived from the breaches in order to achieve the sanctioning objective of credible deterrence.

### **Impact and Proportionality of Sanctions**

In light of the seriousness of the breaches and the conduct of the provider as a whole and the need to deter conduct of this nature, the Executive's view was that the recommended sanctions were proportionate and justified in all the circumstances.

### **Proportionality Adjustment**

In light of the overall case and proportionality considerations, the Executive considered that a fine of £200,000 would be proportionate in the circumstances of the case and adjusted the recommended fine accordingly.

### **The Level 2 provider's representations on recommended sanctions**

The Level 2 provider was content to accept all of the sanctions proposed, save for (i) the five year prohibition and (ii) the fine of £200,000.

In respect of the proposed prohibition, the Level 2 provider considered this remedy to be wholly disproportionate to the severity of the breaches. However, as the Level 2 provider had already exited the premium rate services market and had no intention of re-entering that market, it was prepared to enter into a voluntary agreement with the PSA not to provide premium rate services for a period of five years. The Provider, however, maintains that a prohibition of equivalent duration is wholly disproportionate.

In respect of the proposed fine, the Level 2 provider stated that any fine should be limited to £150,000 as this was more proportionate in light of the duration and severity of the breach. The Level 2 provider had already offered refunds to customers on request. In the circumstances, it would be inappropriate double-counting to settle the level of fine by reference to an alleged need to remove the benefit of the breaches.

## Parties' agreement on Sanctions

The Executive considered the Level 2 provider's response, including the basis upon which the breaches were agreed to be upheld. The Executive was satisfied that the Level 2 provider had shown a good degree of co-operation and willingness to settle this matter. In the circumstances the Executive was satisfied that a fine of £150,000 (rather than £200,000) and a compliance advice requirement (rather than a prohibition) would be proportionate and appropriate sanctions on the facts of the case. Accordingly, the parties agreed that the following sanctions should be imposed:

- a requirement on the Level 2 provider to seek and implement compliance advice, prior to the commencement of all premium rate services, to the satisfaction of the Executive for a period of 5 years from publication of this decision.
- a Formal reprimand
- a fine of £150,000
- 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 the Phone-paid Services Authority that such refunds have been made.

The Level 2 provider agreed to pay 100% of the Executive's administrative costs.