THE CODE COMPLIANCE PANEL OF PHONEPAYPLUS
TRIBUNAL DECISION

Thursday 10 November 2011
TRIBUNAL SITTING No. 88 / CASE 2
CASE REFERENCE: 01224

Service Provider: OpenMarket Limited, UK

Information Provider: txtNation Limited UK

THIS CASE WAS BROUGHT AGAINST THE INFORMATION PROVIDER UNDER PARAGRAPH 8.7 OF THE CODE

BACKGROUND

PhonepayPlus received 53 complaints from members of the public regarding unknown premium rate charges received from a service called 'Gangster Paradise' (the "**GP Service**"), which was an online gaming service operating on gangparadise.com. The GP Service was administered by an individual trading as Gangster Paradise (the "**Content Provider**").

Players who wished to purchase virtual 'credits' for use in the GP Service could do so by choosing one of a number of payment methods available to them. Among the available purchase methods were two premium rate service methods, facilitated either through (i) reverse-billed SMS, or (ii) by calling a premium rate 0911 number. The Executive noted that all of the complaints received by PhonepayPlus related to the reverse-billed SMS payment method (the "**SMS Payment Method**").

The SMS Payment Method was operated by the Information Provider and used shortcodes provided by the Service Provider. End users were required to text a code to one of the designated shortcodes in order to pay for additional virtual currency. Complainants informed PhonepayPlus that they had been tricked by end users of the GP Service into paying for additional virtual currency using the SMS Payment Method.

(i) The Complaints

Over the period from April 2010 to 6 September 2011 (together with one earlier complaint received in August 2009), PhonepayPlus received a total of 53 complaints in relation to the GP Service 'gangparadise.com'. Of these complaints, 11 related to minors, including one disabled minor.

The Executive noted that the majority of the 53 complainants specifically stated they (or someone else) had been misled into accessing the SMS Payment Method either by text message, or through various social networking sites, games and forums (such as Facebook, MSN Chat and Xbox). The complainants were given a number of false incentives, such as free ringtones, the opportunity to vote for talent contests, a need to help dying relatives, a plea to help the poor in the third world and the chance to access 'sex cams'. All complainants had made reference to 'gangparadise.com'.

The Executive further noted that members of the public had posted messages on the website www.whocallsme.com in relation to the GP Service. A number of these messages gave details of the manner in which members of the public had been mislead into accessing

the SMS Payment Method for the GP Service. Their experiences were very similar to those described by the complainants who had contacted PhonepayPlus.

The Executive noted that the Information Provider and their client, the Content Provider, had also posted messages on this website in response to various consumers' messages.

The earliest posting appeared on 5 January 2010, in which the Information Provider wrote:

"Hi, txtNation are an aggregator providing premium SMS connectivity to clients that operate mobile services to consumers. We take issues like this very seriously, so could you please give us more details so we can block this client and get you a refund as it sounds to be misleading. Please contact txtNation via http://sd.txtnation.com *where we can assist further".*

The Content Provider's earliest posting was on 13 May 2010:

"Hello all. I'm the Admnistrator [sic] *of Gangster paradise [www.gangparadise.com] and I have been looking into this matter now. This is a SCAM and please be aware of those who exploit this. Thanks, Anthony".*

The Executive noted that the Content Provider posted a further message on 17 January 2011 to confirm that he had reported these issues to the West Yorkshire Police.

The Executive also noted further messages posted by the Information Provider on 8 and 10 August 2011 which contained reassurances that the matter would be dealt with.

The Executive noted that PhonepayPlus had previously attempted to deal with the issues that arose from the complaints through both the Informal and Fast-track procedures, but that key recommendations made by the Executive through both of these procedures were not implemented by either the Service Provider or the Information Provider. PhonepayPlus continued to receive complaints in relation to this matter until 6 September 2011.

(ii) How the service operated according to the Executive

<u>The service</u>

The GP Service operated through the website gangparadise.com and was an online role playing game where end users could act under their chosen username to build their reputation, earnings, gangster ranking, money and power. End users could enhance their in-game reputation by completing missions, such as committing a crime, completing a search and kill or buying and selling drugs.

Due to the nature of the game content, which included open references to drugs, gangs, violence and virtual betting, the service was rated 18+. The service had originally been accessible to all age groups, but the 18+ rating was imposed by PhonepayPlus in 2009 during an informal procedure, and following an incident in which a minor had accessed the service and accrued a charge of £2,000 on the household phone bill. Other issues were also identified and dealt with as part of the same informal procedure in 2009, although none of these formed part of the Executive's new concerns in this current adjudication.

<u>Accessing the service</u>

Prior to accessing the service, consumers were required to register by entering (i) a login name (username), (ii) a login password, (iii) their email address, (iv) date of birth, (v) sex and

(vi) country. Once these details had been entered, users could login and commence playing the game.

The Executive noted that registrants were not required to supply their mobile phone number.

Initially a free to play game, each new player was allocated US$10,000 of virtual cash, zero virtual credits and a gangster ranking of 'chav'. The virtual 'cash' could be used to purchase virtual items, such as health or to pay set-up costs for organised crime. The virtual 'credits' (upon purchase) could be used to purchase virtual items, such as weapons, steroids, bullets and time travel.

Purchasing virtual credits using the SMS Payment Method

Virtual credits could be purchased using the SMS Payment Method, and in the following increments:

- 15 credits for £1.50 by texting 'gp1 15' to shortcode 60999;
- 30 credits for £3.00 by texting 'gp1 30' to shortcode 60999;
- 50 credits for £4.50 by texting' gp1 50' to shortcode 60999;
- 70 credits for £6.00 by texting 'gp1 70' to shortcode 60999;
- 85 credits for £7.50 by texting 'gp1 85' to shortcode 60999;
- 115 credits for £10.00 by texting' gp1 115' to shortcode 78878;
- 240 credits for £20.00 by texting 'gp1 240 to shortcode 78878; and
- 375 credits for £30.00 by texting 'gp1 375' to shortcode 78878.

The Executive noted that this was a message originating (MO) charged service; therefore, consumers accessing this service though reverse-billed SMS were charged at the point of successful delivery of their message, and not when the credits were accessed and used for the GP Service.

During the course of this investigation, the Executive registered with the service and found that making the £30 purchase of virtual credits using the SMS Payment Method resulted in the receipt of 3 x £10.00 messages, which appeared in the following format:

- *"Visit via your mobile internet http://wap.txtnation.com (data charges apply) to proceed for content, help and support" ("**Message 1**");*
- *"Buy more Points. Try payments via your Landline Phone" ("**Message 2**"); and*
- *"Thank you for purchasing credits from Gangster Paradise. If have any problems, please log onto gangparadise.com and access GP Support. Your password is: XXXXX" ("**Message 3**").*

Informal Procedure (7 October 2010 – 18 November 2010)

The investigation was initially carried out as an informal procedure which commenced on 7 October 2010.

On 7 October 2010, the Executive requested the message logs for a complaint received on 20 September 2010, in which the complainant's husband had been billed £280 for using the SMS Payment Method. The same message logs had already been requested by another Executive on 22 and 24 September 2010. The Information Provider provided the requested message logs on 7 October 2010. The message logs revealed that the SMS Payment

Method for the GP Service had been accessed via this complainant's mobile phone number over a 12-day period. The Information Provider also provided details of 10 usernames that had used this complainant's mobile phone number to obtain credits.

At this point, it appeared that this and other prior complainants had accessed and used the service themselves.

Following a telephone conversation between the Executive and the Information Provider during the week commencing 18 October 2010, the Information Provider disclosed their knowledge of MSN Chat requests being made to unsuspecting consumers, asking them to enter a competition or vote. Consumers who followed these requests were, in fact, tricked into using the SMS Payment Method to purchase GP Service credits for the person making the request.

The Executive informed the complainant of this, and the multiple usernames that had used her husband's mobile phone number to purchase GP Service credits.

On 22 October 2010, the complainant responded, stating that, after mentioning this issue to her family, her 14-year-old son had said that he had been made to feel comfortable by a person on MSN Chat who had told him to text and send back the code which *'would be free from a contract phone'*. Her son did this using his father's contract phone.

At this point, the Executive became concerned about the GP Service, and was specifically concerned about the mechanism that allowed GP Service users to obtain and use credits, purchased by tricking other consumers online, who were unknowingly accessing a premium rate service and incurring large mobile phone bills as a result.

It was the opinion of the Executive that it was possible for GP Service users to obtain credits in this manner because the SMS Payment Method had no effective mechanism/s to prevent GP Service users from accessing the SMS Payment Method fraudulently through other people's mobile phones, and doing so using multiple usernames. With no link between a mobile phone number and a GP Service username, GP Service users could quite freely use credits purchased through <u>any</u> mobile phone number.

On 1 November 2010, the Executive informed the Information Provider that the service was potentially in breach of paragraph 5.4.3 of the Code *(Services must not be of a nature which encourages unauthorised use)* and requested a full refund for the complainant. The Executive issued a recommendation that the Information Provider should put in place a mechanism to prevent more than one account being used by one MSISDN (mobile number), as this was encouraging unauthorised use of the service (by users misleading others into purchasing GP Service credits on their behalf). The Executive stated that:

"The Information Provider should have in place a mechanism to prevent more than one account being used by one MSISDN….. The required mechanism to prevent similar situations should be placed on the service by COB Monday 8 November 2010"

On 1 November 2011, the Information Provider responded by requesting a call-back, referring to the Executive's recommendation as *'wishy-washy'*, on the basis that the complainant's mobile phone had accessed the service 12 times. During the call-back, the Information Provider stated that they 'did ban accounts that had a large number of usernames relating to one number'. On 2 November 2011, the Executive sought advice from the PhonepayPlus Compliance Team who confirmed the Executive's recommendation that the Information Provider prevent more than one username from using the same MSISDN.

On 4 November 2010, the Executive questioned the Information Provider's assertion that it did ban accounts with a high number of usernames. The Executive highlighted the fact that the Information Provider had not banned the account holder in this case who had used 10 different usernames, but had purchased in-game credits using only one mobile phone number. The Executive again re-iterated its requirements to be met by 8 November 2010 (noting that it was entirely up to the Information Provider as to how they wished to implement the required mechanism). The Executive also requested some background information regarding the Information Provider and email addresses of the usernames who had signed up to the GP Service under the one MSISDN and the date the usernames were created.

On 8 November 2010, the Information Provider responded, questioning whether providing this information to the Executive would be in breach of the Data Protection Act**.** The Executive clarified this concern in its response on 8 November 2010, making reference to paragraph 3.4 of the Code (Data Protection) and re-iterating the requirement for the Information Provider to provide the details for the usernames who had obtained GP Service credits through the complainant's mobile phone.

On 10 November 2010, the Information Provider submitted a statement from their client, the Content Provider, maintaining that unauthorised use was in no way encouraged in their games and that they already had necessary mechanisms in place to prevent users making duplicate accounts. The Executive noted that the Content Provider had also confirmed within the same statement that these mechanisms were, in fact, put in place by the Content Provider for 'game play reasons', such as preventing 'unfair-game advantage', and not to prevent or detect misuse of the SMS Payment Method. The Content Provider did not, therefore, have in place mechanisms to prevent a GP Service user from purchasing GP Service credits through someone else's mobile phone. The Information Provider also supplied details of the usernames in the complainant's case, as requested, and confirmed that the complainant had been refunded.

On 12 November 2010, the Executive sent an email to the Information Provider, acknowledging that the Content Provider had in place a mechanism for users that sign up at the same time, but a separate mechanism was required to track over a longer period. The Executive also requested contact details for the Content Provider for the purpose of communicating with them directly. On 16 November 2010, the Information Provider provided contact details for the Content Provider. The matter was transferred to the Fast-track procedure on 19 November 2010.

Fast-track Procedure

On 19 November 2010, the Executive (using the Fast-track procedure) issued recommendations to the Content Provider to remedy the potential breach of paragraph 5.4.3 of the Code, giving them the autonomy as to how they implemented these. The following three recommendations were made:

- Implementation of a further control on date of birth at registration stage to prevent access by those under 18 years of age;
- Implementation of a mechanism to ensure that access to GP credit could not be obtained in future using a MSISDN not connected to the user's account; and
- Implementation of a mechanism to ensure only one username per MSISDN.

On 23 November 2010, the Content Provider confirmed that they had implemented the control on date of birth (whereby if a user entered the wrong date of birth, they would now be

prevented from further registration). However, they said they had no control over MSN Chat and would not or could not implement the other two recommendations

On 23 November 2010, the Executive responded in an email marked 'high importance', making further recommendations based on advice from the PhonepayPlus Compliance Team, which would overcome the Content Provider's concerns as set out in their responses dated 10 and 23 November 2010 (that users who forgot their username/password and/or users who 'die' would need to create another account). The Executive specified that, if the following recommendations were not implemented, it would be necessary to escalate the matter for formal investigation. The recommendations were:

- *"It is necessary to tie the MSISDN to the "username" and should the account "die", it would be necessary to re-register and again tie the MSISDN with the new username thus preventing unauthorized use.*
- *Should a user forget their username/password, it would be a good idea to use a security question and the MSISDN, which should allow them to gain access to their account again".*

On 27 November 2010, the Content Provider responded stating that locking usernames to MSISDNs would only reduce their legitimate revenue, and that they could not *"find solutions to various issues which will affect revenue".*

The Content Provider stated: *"I refuse to be penalized because a small minority of my target audience prey upon the foolishness of people over MSN or other means, such as offering "free cam sex" if they text a number. You're targeting the wrong person here".* Accordingly, the Content Provider would not implement the Executive's recommendations.

On 3 December 2010, the complainant who had contacted PhonepayPlus on 20 September 2010 confirmed that she had received a refund of £360 from the Information Provider.

On 10 February 2011, the Executive wrote to the Content Provider, reminding them of the need to resolve the outstanding problem of GP Service users obtaining other people's MSISDNs to gain credit. The Executive made a recommendation to link the code (password) to the MSISDN requesting it, and only allow the account holder that had associated this MSISDN to this account to use the credit. The Executive was of the view that this would prevent the possibility of using another person's MSISDN to gain credit.

On 28 February 2011, the Content Provider replied, stating *"we're going round in circles"*, and complained that the Executive was again asking for the same impossible measures.

Accordingly, recommendations made by the Executive regarding the need for mechanism(s) to prevent GP Service users from using other people's mobile phones to obtain GP Service credits were not implemented. Meanwhile, PhonepayPlus continued to receive complaints from other members of the public.

(iii) The current investigation (Standard Procedure)

<u>Further complaints</u>

PhonepayPlus continued to receive complaints about the GP Service, and by 6 September 2011, had received a further 21 complaints (19 of which were before 1 September), making a total of 53 similar complaints since August 2009 (51 prior to 1 September 2011).

The continued and consistent flow of complaints concerning the SMS Payment Method for the GP Service made it clear that the issue of consumers being misled into accessing the SMS Payment Method was systemic. The issue was also further aggravated by the fact that the Executive's earlier recommendations to address the problem throughout the Informal and Fast-track procedures had not been implemented.

The Executives initial concerns

The Executive's initial concerns related to issues regarding (i) consumers being misled by text message or online into accessing the SMS Payment Method; (ii) the number of complaints received regarding minors accessing the service inadvertently; (iii) the Information Provider's and the Content Provider's lack of co-operation in putting in place any mechanism which would have potentially prevented or reduced the number of consumers accessing the service in this manner; and (iv) the Service Provider's failure to take any steps in this regard. The Service Provider was fully aware of the correspondence between the Executive, the Information Provider and the Content Provider in relation to this matter.

THE INVESTIGATION

The Executive initially conducted this matter as a Standard Procedure investigation in accordance with paragraph 8.5 of the Code.

On 3 October 2011, the Executive sent a breach letter to the Service Provider and raised the following potential breach of the PhonepayPlus Code of Practice (11th Edition, April 2008) (the "**Code**") under the following paragraphs:

- Paragraph 5.4.1(a) – Misleading; and
- Paragraph 5.8 – Contact Information.

On 10 October 2011, the Service Provider provided a response to the breach letter which contained responses from the Information Provider, and an Information Provider pass-through request under paragraph 8.7 of the Code. On 13 October 2011, further information was provided by the Service Provider.

The Executive granted the Information Provider pass-through on 17 October 2011.

On 25 October 2011, the Executive sent a re-assigned breach letter to the Information Provider. This version of the breach letter included some amendments to the original breach letter. The Information Provider responded on 1 November 2011.

On 10 November 2011, the Tribunal reached a decision on the breaches raised by the Executive.

SUBMISSIONS AND CONCLUSIONS

ALLEGED BREACH ONE
Fairness (Misleading) (Paragraph 5.4.1)

"Services and promotional material must not: a. mislead, or be likely to mislead, in any way".

1. The Executive noted that complainants reported having been 'misled', 'conned', 'tricked', and 'scammed' into accessing the service after being approached either by text message or online, and then requested to unknowingly access the GP Service.

The Executive said that the complainants' evidence clearly suggested that they had been approached and befriended by GP Service users, whose purpose was to obtain in-game credits for the GP Service through other people's mobile phones. This was demonstrated by the fact that complainants were asked to text the GP Service keyword and shortcode. In most cases, this was the keyword 'gp1 375' to shortcode 78878, which was the most expensive credit purchase allowed when using the SMS Payment Method. GP Service users had then been requested to text or send back the 'code' or 'password' to the person who had contacted them.

In October 2010, the Information Provider voluntarily disclosed to the Executive their knowledge of GP Service users who were using MSN Chat to entice unsuspecting consumers into purchasing GP Service credits for them on the false pretext that they were entering a competition/vote. The Information Provider also provided the Executive with evidence in one case of the same mobile number having been used by 10 different usernames to purchase Gangster Paradise credits. Further, as explained in the background above, members of the public had posted comments on the website www.whocallsme.com, describing consumers' experiences as *"scams".* The Information Provider and the Content Provider posted their own responses to these messages on the same website and acknowledged that consumers (which the Information Provider noted may be "younger members of the community") appeared to have been misled.

The Executive asserted that the manner in which complainants were approached (by text and online) and befriended, coupled with the methods used to entice the complainants to access the SMS Payment Method, was misleading. The Executive noted that complainants had reported that, once they had texted the keyword and shortcode, they were told the following:

- That they would receive a free ringtone (six complainants reported this);
- That they were voting for someone in a modelling or talent contest for free, or for 30p (four complainants reported this);
- That they were entering a competition to win a prize;
- That they could view a 'sex cam';
- That they were being asked to help top-up a mobile phone in order to call a dying grandmother;
- That they were being asked to help a friend win a competition;
- That they could download a game for £10; and
- That they would be donating money help the poor in the third world.

The Executive asserted that the complainants' expectations upon sending the keyword to the shortcode were that they would receive in return the content or item promised, or that their contribution to something or someone would reach the intended party or source, either free of charge, or at the cost stated (where provided). This expectation was defeated when the only content complainants received was chargeable premium rate messages from a service they had not intended to access.

As such, the Executive asserted that complainants had been misled into accessing the SMS Payment Method. The Executive believed that the GP Service users who had misled consumers into accessing this service had done so by providing the consumers with the SMS Payment Method keyword and shortcode and, as such, were promoting the SMS Payment Method.

Paragraph 11.3.27 of the Code defines a promotion as:

"anything where the intent or effect is, either directly or indirectly, to encourage the use of premium rate services, and the term promotional material shall be construed accordingly".

The Executive further quoted paragraph 3.1.1 of the Code (which states):

"*Service providers are responsible for ensuring that the content and promotions of all their premium rate services (whether produced by themselves, information providers or other) comply with all relevant provisions of the Code")".*

In light of paragraph 3.1.1 of the Code, the Executive was of the view that the Service Provider was responsible for the promotions of the GP Service in this case. This responsibility was successfully transferred to the Information Provider by virtue of the Information Provider pass-through which was granted on 17 October 2011.

The Executive believed that, in this case, the Service Provider's and the Information Provider's responsibilities were enhanced in light of their knowledge that GP Service users were promoting their premium rate service in this manner, as evidenced by (i) the Information Provider's disclosure of its knowledge to the Executive during the week commencing 18 October 2010; (ii) the messages posted on the website www.whocallsme.com; and (iii) the Service Provider's knowledge of the communications between the Executive, the Information Provider and the Content Provider during both the Informal and Fast-track procedures.

The conduct of the Service Provider and Information Provider was further aggravated by the fact that, notwithstanding their knowledge as set out above, the Service Provider and/or Information Provider failed to put in place any mechanism which would have potentially prevented or reduced the number of consumers accessing the service in this manner. Their failure to do so was despite the fact that the Executive issued various recommendations that they should do so, on approval from the PhonepayPlus Compliance Team.

The Executive noted in particular that one of the Content Provider's responses to recommendations made by the Executive regarding locking usernames to MSISDNs was that this would only, *"reduce their legitimate revenue",* and, "*couldn't find solutions to various issues which will affect revenue".* The Content Provider stated, *"I refuse to be penalized because a small minority of my target audience prey upon the foolishness of people over MSN or other means, such as offering "free cam sex" if they text a number. You're targeting the wrong person here".*

As such, the Executive asserted that, by virtue of paragraph 3.1.1 of the Code, and by virtue of the successful Information Provider pass-through under paragraph 8.7 of the Code, the Information Provider was responsible for the promotion of their SMS Payment Method which resulted in innocent consumers being misled into using the SMS Payment Method. The Executive further asserted that the Information Provider's degree of responsibility under paragraph 3.1.1 was significantly greater in light of its admitted knowledge of the scams being carried out by certain GP Service users, and its conduct in failing to resolve the issue during either the Informal or Fast-track procedures.

In light of the above, the Executive asserted that a breach of paragraph 5.4.1(a) had occurred.

2. The Information Provider provided an initial response on 10 October 2011 and, following the granting of the Information Provider pass-through, a further response was submitted on 1 November 2011.

The Information Provider regretted that 53 consumers had cause to complain about the GP Service. The Information Provider believed that these complainants were victims of social engineering designed by a small minority of GP Service users to trick unsuspecting consumers into passing redeemable virtual credits for use on the GP Service.

The Information Provider underlined that the Content Provider did not encourage such social engineering in any way and that the perpetrators acted outside the mechanisms provided by the Content Provider for purchasing such credits. The Information Provider further asserted that the perpetrators were not affiliated to or employed or in any way commissioned by the Content Provider to act in this way.

The Information Provider argued that the implication that the Content Provider directly misled consumers by its actions was wholly false, and the Information Provider stated that it welcomed the opportunity to explain why. The Information Provider stated that the Content Provider provided a mobile payment mechanism for purchasing credits and did not encourage, condone and still less facilitate deceptions of the type experienced by the affected consumers. The Information Provider further stated that the payment SMS Payment Method had been subject to extensive correspondence between the Information Provider and the Executive to ensure that it was compliant.

The Information Provider stated that it acknowledged that complainants had reported having been 'misled', 'conned', 'tricked', and 'scammed' into using the service, although it was vital in drawing reasoned conclusions from this investigation that it was understood that the Content Provider, or its providers, were not the protagonists who conned the affected consumers.

The Information Provider said that members of the public signed up to the GP Service to play an online game, many of whom did so without controversy and within the terms and spirit of the game, which contained fantasy and comic-book-type elements.

The Information Provider confirmed that, while it took all complaints seriously, the 53 affected consumers represented just 0.2% of the 24,284 transactions made via the GP Service since September 2010, the time of the first complaint. The Information Provider asserted that the GP Service was a serious online business, with a legitimate payment mechanism which did not pursue illegal channels to increase profit by harming consumers. There was no causal link between the miscreant minority who perpetrated the scams complained of and the management of the GP Service or the Information Provider. The Information Provider conceded that a small minority of the members of the public who signed up to play the game had evidently acted outside the law by using social engineering ('the practice of obtaining confidential information by manipulating or deceiving people') to make other people pay for codes unwittingly.

The Information Provider further stated that, as stated in the Executive's bullet points above, the methods used by the perpetrators to trick affected consumers were by way of false promises. The Information Provider stressed that such promises were in no way commissioned, published, funded or authorised by the Content Provider who could not control false statements made about its service by miscreant users who paid little enough respect to the law, let alone the Content Provider's terms or sound common sense.

The Information Provider further noted the Executive's assertion that complainants had been misled into accessing the GP Service, but it was not the Content Provider or any provider associated with the GP Service who misled the complainants or caused them to be misled.

The Information Provider also commented on the Executive's reference to GP Service users who had misled consumers, but those GP Service users were in themselves consumers, members of the public who had signed up to the GP Service to play the online game. GP Service users were not employed by the Content Provider or in any way encouraged to use social engineering to obtain credits for the game. The Content Provider provided a legitimate mobile billing mechanism via the SMS Payment Method for the purpose of obtaining credits.

The Information Provider commented that it found troubling any implication that the Content Provider and GP Service users were one and the same, acting as a unit to mislead the public. The Information Provider argued that there was no evidence that this was the case and the easy conflation of the Content Provider with a small minority of miscreant players who signed up to use the GP Service was to be avoided.

The Information Provider agreed that service providers are in general responsible for content and promotions, and it acknowledged the wording of paragraph 3.1.1 of the Code; *'whether produced by themselves, information providers or others',* but the Information Provider was of the view that it seemed impractical to expect service providers to control false promises made by those third parties beyond the main facilitating parties on the Web or through instant messaging (as in the supposed use of MSN Chat), or any platform or communications method outside the purview of the Information Provider or the Content Provider.

The Information Provider commented that, 'with the best will in the world', the Content Provider and its providers could not monitor and still less edit or censor all communications made by miscreants on open platforms, such as the Web, and even less on private, person-to-person communications, such as instant messaging.

The Information Provider further stated that, even with anecdotal knowledge that MSN Chat had been used by the perpetrators to communicate with their peers or other victims to manipulate them into paying for the GP Service, there was little that the Information Provider or the Content Provider could do to prevent determined perpetrators pursuing these channels to trick unwary consumers.

The Information Provider regretted that the Content Provider appeared uncooperative in its tone during its direct communications with the Executive. The Information Provider's only comment in relation to this was that, in mitigation, the Content Provider felt victimised ('penalized') by the way in which the Executive had appeared to imply that it could control the false promises mentioned in the bullet points above, which lay outside the Content Provider's direct control or influence.

The Information Provider did not consider that the Content Provider had been uncooperative in the context of the changes it had made following contact with the Executive (such as those concerning the implementation of age controls on its main website). Throughout the Information Provider's commercial dealings with the Content Provider, the Information Provider had not found them to be obstructive in a manner that made the Information Provider question the integrity of the GP Service, which was enjoyed without issue by a large number of legitimate users.

The Information Provider conceded that, as regards the notion of tying a GP Service user account to a single MSISDN, which was the Content Provider's main contention in its direct dealings with the Executive, with the benefit of hindsight, it may very well have been at some advantage by imposing this condition on the Content Provider, though the Information Provider felt in the context that this would not have solved the core issue of miscreant users manipulating consumers and there was a question about whether the Information Provider was obliged to follow the Executive's advice or simply give due consideration to it.

The Information Provider commented that questionable users would have been able to create multiple accounts using multiple false email addresses (as it was perfectly easy to do through free email service providers) and obtain an affected consumer's MSISDN by other methods involving the self-same social engineering used to obtain the credits. Given the evident credulity of some of the affected consumers, the Information Provider thought it would be straightforward through the use of multiple accounts to obtain the MSISDN even in the presence of a one-account/one-MSISDN system.

The Information Provider did not believe that the Content Provider had breached paragraph 5.4.1(a) of the Code, given that the service and promotional material under the Content Provider's control were compliant to the best of its knowledge and belief, and that all such materials and communications that were used to make false promises were not authorised, funded, or published by the Content Provider. The Content Provider had no powers to prevent miscreant users from promoting the service in bad faith.

In the absence of any clear mechanism guaranteeing the protection of consumers in a way that could defeat social engineering of the type at the heart of this investigation, the Information Provider was of the opinion that it had done everything it could, in good faith, to honour the Code and that, in conclusion, there was no concerted material breach of the Code.

Following the Executive's granting of an Information Provider pass-through on 17 October 2011, the Information Provider provided a further response to the re-assigned breach letter (dated 25 October 2011) on 1 November 2011.

The Information Provider acknowledged paragraph 11.3.27 of the Code but expressly denied that it had encouraged a minority of rogue GP Service users to "promote" the GP Service directly or indirectly. The Information Provider further acknowledged paragraph 3.1.1 of the Code but expressly denied that it could control "promotion" of the GP Service made by rogue GP Service users who were not authorised to provide any such promotion, however defined.

The Information Provider strongly argued that neither it or the Content Provider had had any control over the so-called "promotion" of the GP Service rendered by rogue GP Service users via methods, such as instant messaging (e.g. MSN Chat), or by social engineering (as defined in the original response) over which the Information Provider had no control.

The Information Provider did not believe, at the time, that the method of having a one-MSISDN/one-account system, as recommended (though never enforced) by the Executive, would have sufficiently curtailed rogue GP Service users; however, the Information Provider was keen to review that recommendation and ensure that the Content Provider sought the approval of the Executive going forward.

The Information Provider further commented that the Executive had "vaguely" referred to "various recommendations" in the plural, though the Information Provider asserted that it was not aware of questioning any substantial recommendations aside from the one centred on providing a "one-MSISDN/one-account" mechanism, which the Information Provider was happy to review now that it was aware of the strength of the Executive's views on that issue. It said the GP Service was enjoyed without issue by many young adults, and rogue users represented a very small minority of the total user base.

The Information Provider stated that it did not believe that any promotions authorised by or otherwise within the control of the Content Provider had the effect of encouraging or facilitating rogue users to trick consumers into using the GP Service. There was no causal link between such GP Service promotions and the fraud committed by rogue users. To suggest that such rogue users were "promoting" the GP Service by inventing fake campaigns (e.g. for "sex cams" or "ringtones") designed to trick consumers into using the GP Service was to wrongly imply that the Content Provider facilitated or otherwise encouraged such "promotions", which was denied.

The Information Provider did not believe that rogue GP Service users could be said to have "promoted" the GP Service, as defined by the Code, given that rogue GP Service users were illegitimately encouraging use of the GP Service without the authorisation or backing of either the Information Provider or the Content Provider.

The Information Provider commented further that the Executive had singularly failed to explain how it or the Content Provider encouraged such fraud, or why it would wish to do so, given the success of the GP Service through legitimate means. Neither the Information Provider nor the Content Provider had sufficient powers to prevent rogue users from contacting unfortunate consumers through instant messaging or other off-site methods outside the direct control of the Content Provider

3. The Tribunal considered the evidence and, in particular, the responses of the Information Provider and concluded that, notwithstanding its lack of direct involvement in the scams that had been alerted to PhonepayPlus by 53 complainants, the Information Provider was responsible for misleading consumers for the following reasons:

- The enticements used by rogue GP Service users to trick members of the public into accessing the SMS Payment Method to obtain GP Service credit fell within the definition of 'promotion' under paragraph 11.3.27 of the Code, given that a promotion was widely defined as, *"anything where the intent or effect is, either directly or indirectly, to encourage the use of premium rate services".*

- Under paragraph 3.1.1 of the Code, *"Service Providers are responsible for ensuring that the content and promotion of all of their premium rate services (whether produced by themselves, information provider <u>or others</u>) comply with all relevant provisions".* [Emphasis added]

- The Tribunal noted a previous case against another party (case ref: 700486), in which a Tribunal had upheld a breach of paragraph 5.4.1(a) of the Code under circumstances that were similar to the present case whereby a premium rate service had been promoted by a third party.

The Tribunal confirmed that the requirement to comply with paragraph 5.4.1(a) of the Code had fallen to the Information Provider as a result of the successful application for an Information Provider pass-through which was granted by the Executive on 17

October 2011. Taking these factors into consideration, the Tribunal considered that the Information Provider was, at the very least, in technical breach of paragraph 5.4.1(a) of the Code.

The Tribunal noted that the Information Provider knew as early as 5 January 2010 (by virtue of its postings on www.whocallsme.com) that MSN Chat requests were being made by rogue GP Service users to unsuspecting consumers in order to fraudulently obtain GP Service credits via the SMS Payment Method. This posting pre-dated all but one of the 53 complaints received by PhonepayPlus in relation to the GP Service. The Tribunal further noted that, notwithstanding its knowledge as set out above, the Information Provider failed to implement any mechanisms (whether recommended by the Executive or the Information Provider itself) which would have potentially reduced the number of consumers being misled.

Accordingly, the Tribunal upheld a breach of paragraph 5.4.1(a) of the Code.

Decision: UPHELD

ALLEGED BREACH TWO

Paragraph 5.8 (Contact Information)

"For any promotion, the identity and contact details in the UK of either the service provider or information provider, where not otherwise obvious, must be clearly stated. The customer service phone number required in paragraph 3.3.5 must also be clearly stated unless reasonable steps have been taken to bring it to the attention of the user or it is otherwise obvious and easily available to the user".

1. The Executive noted that neither the game website nor the three messages received from the SMS Payment Method contained any contact details for the Service Provider. The Information Provider's contact details and its customer service phone number were not available to users on the GP Service website itself but were located on the Information Provider's website (txtnation.com) which could be viewed by following a hyperlink which was embedded within the Terms of Service accessible from the GP Service login page on the GP Service website. Furthermore, to locate this link, the user was required to scroll down to the bottom of the page to point 22 of the Terms of Service (the last point within these Terms). The hyperlink was contained within the text under point 22. It was only after the link had been opened that the consumer had access to the Information Provider's contact details and contact number. Point 22 of the terms of service document stated the following:

   "You must understand that payments are processed by our service provider txtNation [linked] *who can be contacted* here [linked]*. Any problem with a purchase should be brought to their attention".*

   It was noted that, on the first page of the Terms of Service, a disclaimer was presented in bold red text (as below). The disclaimer made it clear that the Content Provider was not responsible for any failure to deliver goods (such as virtual credits). The Executive asserted that the content of this disclaimer could deter the consumer from scrolling down to read the remainder of the Terms of Service in order to find out above the existence of the Information Provider and access the hyperlink to their website. The disclaimer stated:

"We will not be held responsible for any failure to deliver goods ordered by you or any delay in delivering goods ordered by you, the cause of which is any event or circumstance beyond our reasonable control".

The Executive asserted that, given the location of the Information Provider's identity and contact details as set out above, they were not otherwise obvious, and accordingly, these details should have been clearly stated to the user (which the Executive asserted they were not).

The Executive asserted that, given the location of the customer service phone number as set out above, the Information Provider's contact information had not been clearly stated and reasonable steps had not been taken to bring it to the attention of the user. The contact information was also not otherwise obvious or easily available to the user.

In the response submitted by the Information Provider on 10 October 2011, it stated that their contact details and support number were available on the payment window under the 'mEnable' brand.

In its original monitoring, the Executive said it was specifically looking for the Service Provider's and/or the Information Provider's details. It did not notice the details referred to by the Information Provider in its response.

When re-accessing the service on 21 October 2011, the Executive found that, in order to locate these details, a user would be required to register with the service, login, and click 'buy credits'. Clicking this link resulted in the appearance of the first 'mEnable' payment screen, which provided consumers with all the keywords and shortcodes required to make purchases using the SMS Payment Method.

Next to the keyword and shortcode detail was a link (in orange) entitled, *'pay in another way/country'.* When clicked, this resulted in a second 'mEnable' payment screen, which the Executive noted opened not as a full window, but as a small page on top of the first 'mEnable' screen (**Appendix A1**). Although the hyperlinks to the contact details were on this page, these were not visible when the page opened, as they required the user to scroll down and across, or to maximise the screen.

As such, the Executive asserted that, for the promotion of this service, the identity and contact details of the Information Provider were not clearly stated, nor were they otherwise obvious. With regard to the customer service number, it too was not clearly stated, or otherwise obvious and easily available to the user, and no reasonable steps had been taken by the Information Provider to bring it to the attention of the user.

In light of the above, the Executive asserted that a breach of paragraph 5.8 had occurred.

2. The Information Provider provided its original response on 10 October 2011. The Information Provider stated that, to the best of its knowledge and belief, it had not been asked previously to change the contact details on the GP Service, despite the long history of communications between it and PhonepayPlus. The Information Provider did however confirm that it was reviewing the clarity and placement of the contact details to ensure they were optimised for ready access by consumers. The Information Provider further confirmed that is had no issues ensuring improvements were brought in this area.

   By way of clarification, the Information Provider confirmed that its contact details and support number were, and always had been, displayed on the payment window

provided by txtNation (under its 'mENABLE' brand) for use by the Content Provider. When users of the GP Service made payment for credits by mobile phone via the prompts on the payment window, the support details for the Information Provider were clear.

In addition, the Information Provider further stated that, since August 2011, changes had been made to the wording of the text messages sent to end users to ensure clarity, and to advise consumers of the risks of sharing the credits with others:

"Thank you for purchasing credits from Gangster Paradise. If [you] *have any problems, please log into gangparadise.com and access GP* [Gangster Paradise] *Support. Your password is:"* [all end users received this billed message]

"This is a premium billing message from gangparadise.com Do not give out your pin code / password. It will arrive shortly." [end users requiring two or three billed messages receive this message]

"If you need assistance with this billed message please visit http://sd.txtnation.com/enduser*"* [end users requiring three billed messages receive this message]

The Information Provider further argued that, where third parties had defrauded affected consumers, they did so without reference to the GP Service website or other support as far as they were able, claiming, for example, that the consumer needed to use the service due to a family emergency. The Information Provider stated that it was in the interests of the perpetrators to ensure that affected consumers did not see the GP Service website, which was in the nature of the dupe. However, the message terminating (MT) messages above did go some way to ensuring consumers were empowered to seek appropriate help in cases where they had been defrauded.

Legitimate consumers signing up to the GP Service were asked to agree with the terms, and they were expected to read those terms prior to signing up to ensure they understood what recourse they had to solve any issues arising from their use of the service.

The Information Provider stated that it was happy to work with the Content Provider to make all relevant contact details clearer, though it underlined that consumers signing up to the GP Service (whether or not they later bought credits) did confirm that they had read the Terms of Service, and the length of such terms was not an adequate reason for not reading them.

Where consumers were duped into using the GP Service by third parties outside the direct control of the Content Provider, the contact details were largely bypassed, as was the nature of the manipulation, notwithstanding the text messages above. The Information Provider was of the opinion that it was positive that consumers left in that position contacted PhonepayPlus or the provider via the regulator's online Number Checker to seek help in these cases.

The Information Provider believed that it did not breach or cause or allow the Content Provider to breach paragraph 5.8 of the Code and that, as regards contact details, reasonable steps had been taken to bring these contact details to the attention of the user. Notwithstanding this assertion, the Information Provider confirmed that it was happy to make further improvements.

Following the Executive's granting of an Information Provider pass-through on 17 October 2011, the Information Provider provided a further response to the re-assigned breach letter (dated 25 October 2011) on 1 November 2011.

The Information Provider confirmed that it was free for users to sign up to the GP Service and, only at the point where they wished to pay for GP Service credits, did they have cause to access the payment options and the contact details from the relevant link on the payment window.

With respect to the Executive's account of the 'mENABLE' payment window, the Information Provider stated that it was at a loss as to why the window had opened without sufficient screen estate to show the entire payment page and why the web browser's menu and icons were displayed (it said ordinarily, the window would open without this part of the window's interface, allowing the full payment page to be rendered without the use of scroll bars). The Information Provider acknowledged that, in the Executive's screenshot, it was evident that the browser's menu was pushing down the payment page, rendering part of it accessible only by scrolling).

The Information Provider asserted that, to be clear, under ordinary operating conditions, the payment window opened in either a "pop-up" window that was proportionate to the page (so that the full content of that page was rendered in full view to the consumer), or in a new browser "tab" (so that the full content was similarly fully rendered), depending on the settings of the individual web browser software.

The Information Provider submitted its own screenshot of the payment window as it should have been displayed (**Appendix A2**). The Information Provider stated that, under different operating systems and/or web browser configurations, together with any software installed by the consumers on their PCs (including but not limited to browser 'add-ons' or 'plugins'), it was possible that windows may not always open or be proportioned or styled as intended by the publisher (the publisher in this case being the Information Provider).

The Information Provider did not therefore consider the Executive's screenshot to be a fair reflection, either of how the Information Provider intended the window to be displayed or of how most consumers experienced that window and the payment page therein.

The Information Provider asserted that any allegation that it had intended to obfuscate its contact details, or to otherwise avoid supporting consumers by rendering the window smaller than required to display the payment page in full, would be expressly denied. The Information Provider further stated that, in circumstances where a web browser window did not open as intended, the Information Provider believed that consumers would know how to manually resize the window using their cursor and input device or else use the 'maximise' button to render the window full-screen. Users of Windows or other operating systems would therefore understand how to resize a window as part of their basic day-to-day use of their PCs, without requiring any advanced technical knowledge.

The Information Provider further stated that it provided regular support to consumers of the service and had no record of complaints regarding the accessibility of its contact details, which were eminently accessible on the payment page. The GP Service itself had a number of links to FAQs, their own contact page, and all new members of the GP Service were sent a message on the GP Service website with links to help information.

The Information Provider believed that, under paragraph 5.8 of the Code, its contact details were, *"easily available to the user",* from the link on the window used to make a payment for GP Service credits. The Information Provider therefore argued that an isolated issue with the Executive's browser window was not sufficient to claim that the window appeared likewise on the PCs of the majority of consumers using the GP Service. The Information Provider did not believe that any GP Service user had difficulty in contacting either the Content Provider or the Information Provider when attempting to remedy any issue they had experienced during their use of the GP Service.

3. The Tribunal considered the evidence and concluded, with respect to the messages received during use of the SMS Payment Method, that Message 1 and Message 3 were not promotions under paragraph 11.3.27 of the Code, as neither had the intent or effect of encouraging the use of premium rate services. Message 1 and Message 3 were not therefore subject to a potential breach under paragraph 5.8 of the Code.

   Message 2 was a promotion, as it had the effect of encouraging the recipient to pay for more credits using their landline. The Tribunal concluded that, as Message 2 contained neither the identity nor the contact details for the Information Provider, the information was neither obvious nor clearly stated.

   The Tribunal concluded that the location of the Information Provider's identity within item 22 of the GP Service Terms of Service was neither obvious nor clearly stated. The Tribunal further concluded that, as the Information Provider's contact details were not actually provided within the GP Service Terms of Service, but were located only after clicking the link within item 22 thereof, these contact details were equally neither obvious nor clearly stated.

   The Tribunal further concluded that, as the customer service phone number required in accordance with paragraph 3.5.5 of the Code was absent from Message 2, reasonable steps should have been taken to bring it to the attention of the user. Alternatively, it ought to have been otherwise obvious and easily available to the user.

   The Tribunal considered the Information Provider's arguments with regard to the accessibility of its contact details, together with the customer support number, on its payment window. The Tribunal considered that the requirement to navigate through a number of links to reach this information meant that the identity and contact details of the Information Provider were in neither obvious nor clearly stated, and no reasonable steps had been taken to bring the customer support number to the attention of the user or make it otherwise obvious and easily accessible.

   The Tribunal accordingly upheld a breach of paragraph 5.8 of the Code.

Decision: UPHELD

SANCTIONS

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

In determining the sanctions appropriate for the case, the Tribunal took into account the following aggravating factors:

- The Information Provider's behaviour was negligent by virtue of the fact that the Information Provider was fully aware that innocent consumers were being misled into

their service, yet failed to implement any of the Executive's recommendations or make any suggestions of its own, which could have potentially prevented or limited consumer harm.

- The cost paid by individual consumers was high – one consumer had incurred charges of £750 and numerous other consumers had incurred charges of over £100.

- Promotion of the GP Service had been harmful to some minors – 11 of the complaints received by PhonepayPlus were in relation to access of the SMS Payment Method by minors. Both the Service Provider and the Information Provider were aware of this.

- The Information Provider had failed to implement compliance advice or taken notice of any recommendations by the Executive during the Informal and Fast-track procedures.

- The relevant breach history of the Information Provider.

The Tribunal considered the following mitigating factors:

- The Information Provider's argument that the breach was caused by a third party (other than the Information Provider) in circumstances that were beyond its control. However, the Tribunal considered that, because the Information Provider was on notice of the problems being caused by third parties, it had a duty of care to act to prevent or minimise those problems, which it had refused or failed to do, which meant it would not treat this as a mitigating factor.

- The Information Provider confirmed that some partial refunds were offered to complainants for unused credit, and the complainant whose mobile had been linked to 10 usernames was eventually provided with a full refund.

The revenue in relation to the GP Service was in the high range of Band 2 (£250,000 - £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 **significant**.

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

- A Formal Reprimand;

- A fine of £65,000 (comprising £50,000 for the breaches upheld and £15,000 for the relevant breach history).

The Tribunal commented that it expected claims for refunds to be paid by the Information Provider for the full amount spent by complainants, except where there is good cause to believe that such claims are not valid.

The Tribunal further recommended that the Information Provider take steps (including seeking and implementing compliance advice) to eliminate the risk of consumers being misled in the future and safeguard against any further breaches of the Code.