THE CODE COMPLIANCE PANEL OF PHONEPAYPLUS

TRIBUNAL DECISION

Thursday 19 March 2009 TRIBUNAL SITTING No. 23 / CASE 1
CASE REFERENCE: 768557/CB

Information provider & area:	Vision SMS Limited, Glasgow
Service provider & area:	mBlox Limited, London
Type of service:	Virtual Chat Service
Service title:	SMS Chat
Service number:	81313
Cost:	£1.50 per message received
Network operator:	Mobile Networks
Number of complainants:	30

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

BACKGROUND

The PhonepayPlus Executive ("the Executive") received 30 complaints relating to a text chat service operated by the information provider on shortcode 81313. The service appeared to be marketed by promotional text messages sent to mobile numbers, details of which had been purchased from a third party. The complaints centred on the receipt of unsolicited text messages; complainants stated that they had not consented to receive the marketing material sent to them. Consequently, the sending of these text messages appeared to the Executive to have contravened the requirements of the Privacy and Electronic Communications Regulations 2003.

The Executive therefore raised the following potential breach under the PhonepayPlus Code of Practice 11th Edition (amended April 2008) ("the Code"):

- Paragraph 5.2 - Legality

(i) The Service

The service operated as a text chat service which appeared to be marketed by free promotional messages being sent to mobile numbers which had been purchased from a third party data provider. The service operated from 23 July 2008 and the shortcode was, according to the service provider, suspended on 09 October 2008 due to payment arrears.

The promotional messages sent to recipients provided them with the opportunity to access the service by responding with a keyword and also an option to stop receiving messages by replying 'STOP'.

Two promotional messages appeared to have been sent as follows:

Free Msg:Cathy, 44, housewife looking for no strings fun.Age/looks not important. Txt CATHY to 81313 to get str8 thru. Msgs 150p rcvd. SP vsms. STOP 2 stop. 0116603316

Free Msg:Kirsty, 19, nurse looking 4 no strings fun.Age/looks not important. Txt KIRSTY to 81313 to get str8 thru. Msgs 150p rcvd. SP vsms. STOP 2 stop. 0116603316

The service operated on a £1.50 short code billing tariff for messages received from the service once users had responded to promotions with the keywords.

(iii) <u>Complaint Investigation</u>

Standard Procedure

The Executive initially conducted this matter as a standard procedure investigation against the service provider in accordance with paragraph 8.5 of the Code but it subsequently accepted the service provider's request to deal with its information provider client directly.

On 3rd October 2008 the Executive sent a preliminary investigation letter to the service provider requesting information under paragraph 8.3.3 of the Code. The Executive received a response dated 23rd October 2008 from the service provider which contained additional information provided by the information provider.

On 24th October 2008 the Executive sent a second letter to the service provider requesting further information as to how consumers had specifically consented to receive marketing from Vision SMS. On 6th November 2008, the Executive received a response by email from the service provider.

The Executive carried out an investigation into the evidence that had been provided by the service provider with regard to complainant opt–in methods and issued a formal breach letter dated 7th November 2008 to the service provider, raising a breach of paragraph 5.2 of the Code.

On 14th November 2008 the Executive accepted undertaking forms signed by both the service and information provider and re-issued the formal breach letter directly to the information provider. The Executive received a response from the information provider dated 24th November 2008 containing further information which purported to show that complainants had opted-in to receive promotional SMS messages. This evidence came in the form of (a) a list of mobile phone numbers which had allegedly clicked on a WAP link to visit an adult movie WAP site, (b) a screen shot from the website climaxtoys.co.uk and (c) screen shots taken from the website sextoys.co.uk. The latter included a paragraph at the end of the registration section which informed users that their personal information might be shared with selected third parties for marketing purposes and enabled them to opt-out of data sharing by ticking a box.

The Executive then visited the website sextoys.co.uk and took some screen shots of the registration page which showed that the page in question did not actually contain the paragraph regarding personal information sharing for third party marketing purposes, nor an opt out tick box. The Executive then contacted the Managing Director of the company which operated the website sextoys.co.uk on 27th November 2008 and asked him to comment on the screen shots that had been provided to the Executive by the information provider and the screen shots the Executive had taken directly from the website. The Managing Director confirmed that the screen shots provided by the Executive were correct and that the website had not appeared in the manner that the information provider's screen shots suggested. In addition to this he said that his company had never shared users' information with third parties.

The Executive therefore sent an addendum to the breach letter to the information provider on 24th December 2008 which included the new evidence which suggested the screen shot for sextoys.co.uk provided by the information provider was not accurate. The Executive received an emailed response to the addendum from a consultant retained on behalf of the information provider, within which a meeting with the Executive was requested.

Between 26th January 2009 and 12th February 2009, the Executive attempted to make contact directly with the data supplier whom the information provider had named as the supplier of the opt-in evidence. On 11th February 2009 a response was received from the data supplier stating that it had not been involved in the data provided to the information provider.

On 28th January 2009, during a meeting with the Executive, the information provider's consultant provided copies of email correspondence between it and the data supplier which purported to show that the data supplier had provided the mobile numbers used by the information provider for this service but had in turn been supplied with the data by a third party. The Executive sent an email dated 3rd February 2009 to the information provider requesting further evidence to substantiate the information provider's claim that a third party had apparently supplied the data supplier with the opt-in data.

On 9th February 2009, the Executive received two separate responses from the information provider confirming that the third party company had provided them (following a direct request) with the screenshot of the website sextoys.co.uk which had contained the additional paragraph on personal information sharing for third party marketing purposes and the opt out tick box. On 10th February and 26th February 2009 the Executive attempted to contact the third party company to ask questions relating to the data provided to the information provider, but received no response.

On 17th February 2009, the Executive received an email from the information provider showing an email dated 24 Nov 2008 which appeared to be from the third party company which had provided the information provider's consultant with opt-in evidence. The Executive also received an email from the information provider's consultant setting out the problems it was experiencing with the data supplier and the third party company and requesting an opportunity to make informal representations before the Tribunal.

The Tribunal made a decision on the breaches raised by the Executive on 19 March 2009 having heard informal representations from the information provider and its consultant.

SUBMISSIONS AND CONCLUSIONS

ALLEGED BREACH ONE
LEGALITY (Paragraph 5.2)

"Services and promotional material must comply with the law. They must not contain anything which is in breach of the law, nor omit anything which the law requires. Services and promotional material must not facilitate or encourage anything which is in any way unlawful."

Under Regulation 22 of the Privacy and Electronic Communications (EC Directive) Regulations 2003, it is an offence to send unsolicited promotions using electronic mail (including text messages) for direct marketing purposes, unless (1) the recipient has specifically consented to receiving such promotions. This is sometimes called 'a hard opt in', or (2) the recipient's details were obtained whilst purchasing a similar or related product or service to that now being promoted and the recipient was given the opportunity, when his details were collected, to opt out (without charge) of receiving further communications, and is given the same opportunity in each subsequent communication. This is sometimes called a 'soft opt-in'.

1. The Executive's position was the information provider could not rely on a "soft opt in" because this did not apply where the recipient's details had been provided by a third party, as in this case. It stated that since the information provider must be relying on a "hard opt in", Regulation 22(2) required that consumers must have specifically consented to receiving the promotional material from the information provider and therefore the information provider should have been able to provide evidence that consumers had specifically consented to receive the type of promotional material they had been sent.

   The Executive had received 30 complaints about the 'SMS Chat' service from members of the public and all complainants had stated that the SMS messages that they had been sent were unsolicited.

   The Executive reviewed the initial evidence provided by the information provider, which consisted of (a) a list of mobile phone numbers which were alleged to have clicked on a WAP link in order to visit an adult movie WAP site, (b) a list of IP addresses (with corresponding mobile phone numbers) associated with users who were alleged to have visited the website sextoys.co.uk (c) and screen shots of the websites climaxtoys.co.uk and sextoys.co.uk, all of which had been allegedly used by users to indicate their consent to receiving marketing from third parties. The Executive stated that the evidence which had been provided had failed to show that the necessary specific consents had been obtained from the complainants.

   In an addendum, the Executive raised further concerns regarding additional evidence supplied by the information provider which was intended to show that consumers had consented to receive the marketing messages via provision of a 'hard opt-in' i.e. by giving their specific consent. These concerns related specifically to the sextoys.co.uk website screen shots provided to the Executive within the information provider's response dated 24th November 2009. On the screen shots there was a paragraph which presented a tick box that appeared to enable users to tick the box so as to opt out of further marketing:

   'We may share your personal information with selected third party marketing companies, who may wish to contact you with related offers and services of an adult nature (Over 18's) by electronic communication including but not limited to (SMS Email). To opt-out of third party marketing please click here [ ]'

   The Executive challenged this evidence and the process of registration given by the information provider on the basis of: 1) the Executive's monitoring of the website which showed that the paragraph had not been included on the sextoys.co.uk website; and 2) the confirmation of the company which owned and operated the website that it had never and would never sell/provide

users' data to third parties, and that the screenshot provided by the information provider was not a true reflection of the webpage and must have been fabricated .

In the absence of any evidence to show specific consumer consent for the purposes of Regulation 22(2) of the Regulations, the Executive considered that a breach of paragraph 5.2 had occurred.

2. The information provider initially stated that it had provided relevant evidence during the preliminary investigation and expressed some disappointment that the information it had provided did not satisfy the Executive sufficiently. It stated that had the Executive requested the additional screenshot information it would have happily supplied it and would do so in a separate email that day. The information provider also listed a number of points which it wished the Tribunal to take into account as mitigating factors. The points included submissions that; the Code did not specify what constituted an acceptable opt-in, upholding the breach would almost appear to be a victimisation of its small business despite the introduction of strong compliance processes, and that consumers had not been charged a single penny for the texts they had received as part of this service.

Following receipt of the addendum, including the additional evidence provided by owner of sextoys.co.uk, the information provider provided an interim response stating that it was visibly shocked and upset by the contents of the addendum and supporting evidence. It stated that the marketing list was sold to it in the summer of 2008 by the data supplier, who as part of the agreement retained responsibility for the supply of any verification opt-in information. The information provider stated that the data supplier made it aware last year that the services of a third party company were used to supply the opt in information which PhonepayPlus had requested. The information provider understood it was this company which was responsible for producing the evidence from the sextoys.co.uk website. The information provider said it had played no part in the fabrication of the evidence.

The information provider subsequently requested a meeting with the Executive to discuss the evidence. At the meeting it presented the Executive with a significant quantity of correspondence relating to the information provider's attempts to obtain evidence of consumer opt-in from the data supplier that had supplied the marketing data list.

The information provider also stated (and restated during informal representations made to the Tribunal) that assurances had been made to a previous Tribunal that new measures had been introduced to ensure it had adequate opt ins before it sent out marketing communications, so as to prevent consumers receiving unsolicited promotional material. It emphasised that this incident occurred prior to the new measures being introduced. It stated that lessons had been learnt as accepted in the previous case and confirmed that the measures were working and that marketing data was not being purchased where opt-in verification could not be supplied prior to purchase of the marketing data lists. However, the information provider accepted the evidence that, on this occasion, marketing messages had been issued contrary to the Regulations and that the promotion was therefore in breach of paragraph 5.2 of the Code.

3. The Tribunal considered the evidence and found that, on the balance of probabilities, the opt-in evidence had been fabricated (and it noted this was accepted by the information provider). The Tribunal found that there was no evidence to suggest that the information provider had itself been involved in the fabrication of the website screen shot supplied as evidence. However, the Tribunal concluded that, had the information provider exercised proper due diligence with regard to the opt-in data received prior to sending the promotional messages, it would have established for itself that the evidence had been fabricated. The Tribunal considered the other evidence in relation to consumer opt-ins and found that there was no other satisfactory evidence of consumers having given specific consent to receive marketing communications. The Tribunal therefore decided to uphold a breach of paragraph 5.2 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 factor:

- The information provider was negligent in not carrying out checks on the data it had purchased prior to commencement of marketing.

The Tribunal noted that the information provider had a relevant breach history but decided not to consider this as an aggravating factor in this instance, as the current case arose out of an incident which occurred at the same time as the breach in the previous case, and before new compliance measures had been put in place.

There were no apparent mitigating factors for the Tribunal to consider. However, the Tribunal noted that following the previous case the information provider had put into effect compliance arrangements (e.g. appointment of a compliance officer) which if adhered to successfully should prevent future breaches of this kind.

Having taken into account the aggravating factor, and the number of complaints received in this case, the Tribunal concluded that the seriousness of the case should be regarded overall as **significant**.

The Tribunal therefore decided to impose the following sanctions:

- A formal reprimand; and
- A £1,000 fine.

The Tribunal did not impose an additional fine in respect of the information provider's breach history, in view of the information provider's current compliance activity. The Tribunal stated that if future cases were brought to PhonepayPlus involving services which demonstrated a failure in the new compliance structure, it would be open to the Executive to recommend that future Tribunals take into account the fact that there was no additional fine imposed for breach history in this case.