

Tribunal meeting number 195 / Case 1

Case reference: 77718
Level 2 provider: Skybytes Ltd (UK)
Type of service: "Glamour Content" glamour video subscription service
Level 1 provider: Zamano Solutions Ltd (Ireland)
Network operator: All Mobile Network operators

THIS CASE WAS BROUGHT AGAINST THE LEVEL 2 PROVIDER UNDER PARAGRAPH 4.5 OF THE CODE**BACKGROUND**

The case concerned a glamour video subscription service operating under the brand name 'Glamour Content' on dedicated shortcode 84507 (the "**Service**").

The Level 2 provider for the Service was Skybytes Limited ("**the Level 2 provider**"). The Level 2 provider had been registered with PhonepayPlus since 17 March 2015.

The Level 1 provider for Service shortcode 84507 was Zamano Solutions Limited ("**Zamano**").

The Service

The Executive understood the Service to be a glamour video subscription service, charged at £4.50 per week. The Executive understood that consumers enter the Service via a wireless application protocol ("**WAP**") opt-in.

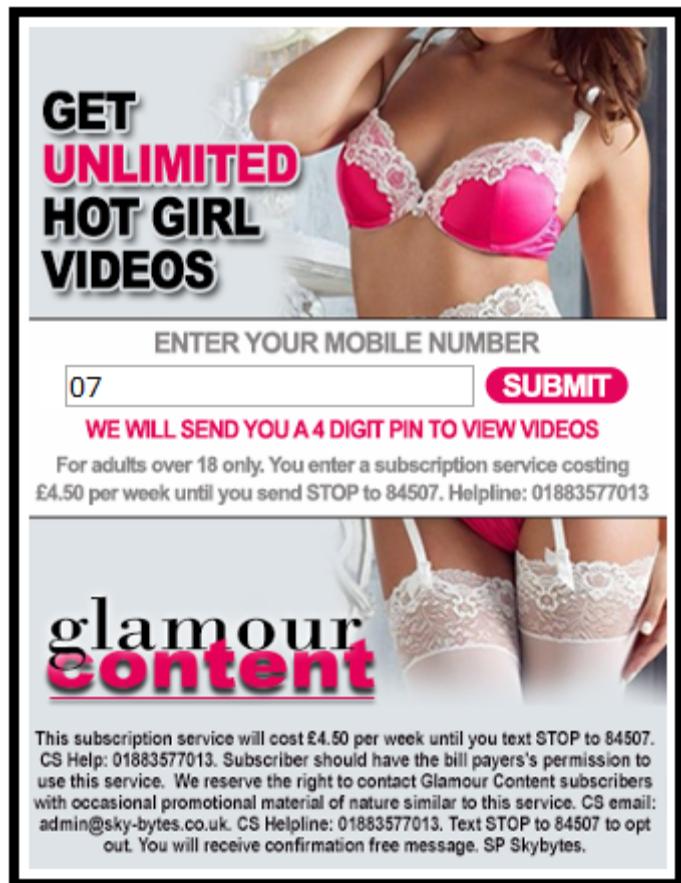
The Level 2 provider had stated that the Service promotion commenced in May 2015. The Service was operational as at 18 August 2016.

The Level 2 provider supplied a document setting out the consumer journey into the Service, extracts of which appear below:

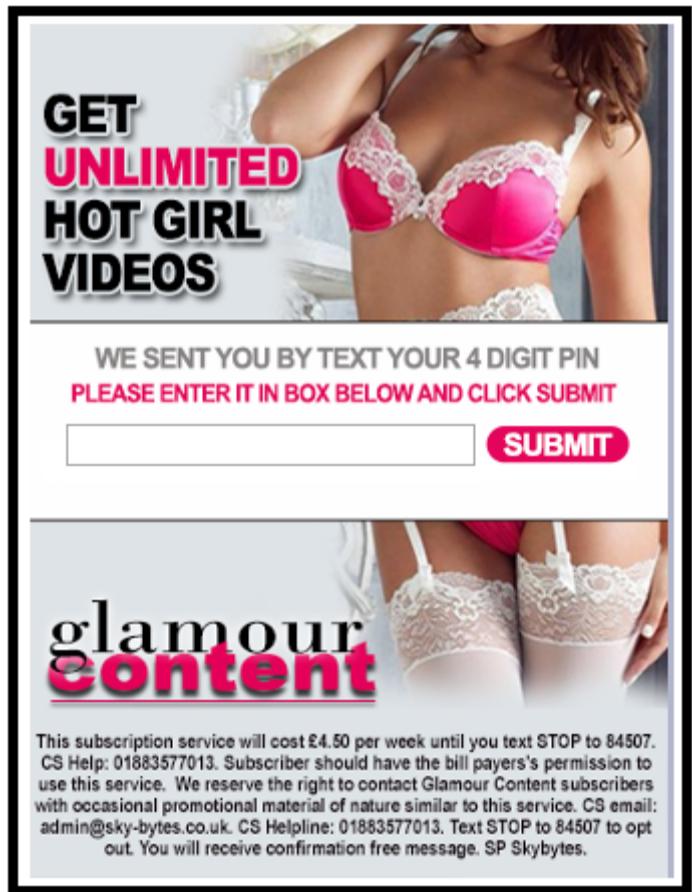
A. Banner ad

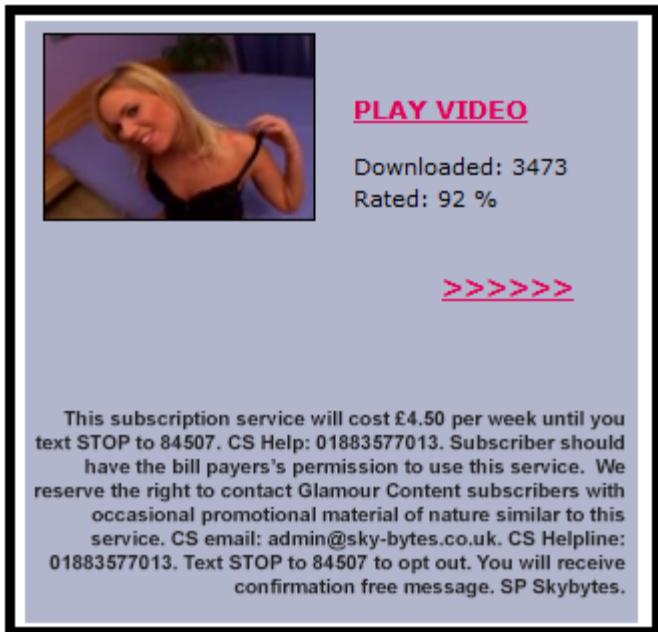


B. Mobile number entry page



C. PIN code entry page



D. Content page

This subscription service will cost £4.50 per week until you text STOP to 84507. CS Help: 01883577013. Subscriber should have the bill payers's permission to use this service. We reserve the right to contact Glamour Content subscribers with occasional promotional material of nature similar to this service. CS email: admin@sky-bytes.co.uk. CS Helpline: 01883577013. Text STOP to 84507 to opt out. You will receive confirmation free message. SP Skybytes.

Summary of complaints

The Executive received 86 complaints concerning the Service between 1 June 2015 and 26 July 2016.

Complainants variously alleged that the Service charges were unsolicited. A sample of complainant accounts is provided below:

"I am being charged 3.75 every week by Glamour Content subscription service on my mobile phone bill. I have never received any message encouraging to sign up to a payable service, neither replied to any suspicious text. Today I have just received my new bill and I am shocked with the amount to pay. I have called my provider but they told me to contact Skybytes as they provide the service. I did so, however nobody answers the telephone. Please could you help me to stop the subscription and get my money back."

"As far as I'm concerned I never signed up for this nor did I misclick anywhere so I have no clue where the subscription came from, there was no info on charges and I just assumed it was spam mail until my bill came through. I have no idea what the content is as I have never clicked on the links for fear of being charged. I feel like I have been massively scammed here! It appears I am billed £4.50 every week and at present the total I have had taken from me is £36. As soon as I noticed the extra charges I called my phone provider."

"I am billed £4.50 each week. I contacted giff gaff, my mobile company and after a long time they found the number that has charging me £4.50 weekly. I did not ask for the service nor do I actually receive anything from them"

"I recently received my mobile bill from TalkTalk and on it were 4 charges of £4.50 for receiving text messages from 84507. I have never signed up to anything to receive this and I believe this to be a fraudulent company that have obtained my number online and have been sending me messages hoping I wouldn't realise I had been charged. I would like this company to be prosecuted for fraud as I certainly haven't agreed to them sending me messages, let alone paying for them to send me them. There's no mention of a charge on the message when I received it and I deleted it as a spam text, not realising I was going to be charged for it. I am absolutely livid that this company can send out messages randomly to people and charge them! This is fraud and it should be stopped immediately."

"I received a text saying "GLAMOUR CONTENT. To stop service text STOP to 84507". I was of course suspicious of this as I had no idea how this company had got my number so I blocked it and, for fear of being charged, did not respond. I checked my bill recently and realised for months i have had an increase of 100% to it! The billing frequency is every week. The total amount billed is currently £98 so far!"

The investigation

In accordance with the transitional arrangements set out at paragraph 1.8 of the PhonepayPlus Code of Practice (14th Edition), the Executive conducted this matter as a Track 2 procedure in accordance with paragraph 4.5 of the Code of Practice (14th Edition).

The Executive sent a Warning Notice to the Level 2 provider on 18 August 2016. Within the Warning Notice the Executive raised the following breach of the PhonepayPlus Code of Practice (the "**Code**"):

- Rule 2.3.3 – Consent to charge

The Level 2 provider responded on 2 September 2016. On 26 October 2016, the Tribunal, having heard informal representations made on behalf of the Level 2 provider, reached a decision on the breach raised by the Executive.

The Tribunal considered the following evidence in full:

- The complainants' accounts;
- Correspondence between the Executive and the Level 2 provider (including directions for information and the Level 2 provider's responses including supporting documentation);
- Correspondence between the Executive and the Level 1 provider;
- Correspondence between the Executive and the Third Party Verifier;
- Complainant message logs from the Level 2 provider;
- PhonepayPlus Guidance on "Privacy and Consent to Charge" (12th Code) and "Consent to Charge" (13th Code)

- The Warning Notice of 18 August 2016 and the Level 2 provider's response of 2 September 2016 plus attachments; and
- An email from the Level 2 provider dated 26 October 2016

PRELIMINARY ISSUE

By email dated 26 October 2016 the Level 2 provider had notified the Executive that the Level 2 provider's representative was at short notice unable to attend the Tribunal to make informal representations, and asked if the Tribunal could be recorded. The Tribunal noted that the determination was to take place via the paper-based procedure, and therefore elected to treat the email as an application for that portion of the proceedings which can properly be disclosed (being oral representations and any queries the Tribunal asked of the Executive) to be recorded, pursuant to the procedure set out at paragraph 151 of the Supporting Procedures.

The Tribunal noted that the application had been made at a late stage, however based on the Level 2 provider's explanation regarding the circumstances in which the application was made, the Tribunal exercised its discretion to consider the application. The Tribunal understood that the Level 2 provider wished for there to be a further degree of transparency in light of its inability to attend. The Tribunal did have questions for the Executive and so there was material which could be recorded. In the circumstances, the Tribunal agreed that the queries it asked of the Executive, and the answers given, should be recorded.

SUBMISSIONS AND CONCLUSIONS

ALLEGED BREACH 1

Rule 2.3.3 – Consent to charge

"Consumers must not be charged for premium rate services without their consent. Level 2 providers must be able to provide evidence which establishes that consent."

1. The Executive asserted that the Level 2 provider had breached rule 2.3.3 of the Code as evidence provided by the Level 2 provider to establish that complainants who had entered the Service through the WAP opt-in had consented to be charged was not verified by an independent third party. Accordingly, the Level 2 provider had not provided sufficient evidence to establish consumers' consent to be charged.

The Executive noted that Service charges shown in the Level 2 provider's message logs occurred in the period that the PhonepayPlus Code of Practice, 12th Edition was in force, and in the time period after the PhonepayPlus Code of Practice, 13th Edition came into force. Given that rule 2.3.3 was effectively identical in the two versions of the Code that were in force when complainants incurred Service charges, the Executive raised an alleged breach of rule 2.3.3 of the PhonepayPlus Code of Practice, 12th Edition and the PhonepayPlus Code of Practice, 13th Edition.

The Executive relied on correspondence exchanged with the Level 2 provider, correspondence exchanged with ETX (UK) Ltd (the "**Third Party Verifier**"), complainant accounts, (which are referenced in the 'Background' section above), PhonepayPlus General Guidance Note 'Privacy

and consent to charge' in support of the PhonepayPlus Code of Practice, 12th Edition (the "**Code 12 Guidance**"), PhonepayPlus General Guidance Note 'Consent to Charge' in support of the PhonepayPlus Code of Practice, 13th Edition (the "**Code 13 Guidance**") and text message logs.

Code 12 Guidance stated:

"2. What is robust verification of consent to charge?

2.1 Robust verification of consent to charge means that the right of the provider to generate a charge to the consumer's communication bill is properly verifiable (see section 5 below). By 'properly verifiable', we mean a clear audit trail that categorically cannot have been interfered with since the record ... of consent to purchase... was created.

For charges generated by entering a mobile number on a website

For the avoidance of doubt, this section applies to the consent evidence required for services initiated from a web page and where premium SMS is the chosen billing mechanic. This section does not apply to 'web' Payforit.

2.5 Some services are initiated by a consumer entering a mobile number on a website, or a mobile website (i.e. a website browsed on the mobile handset). In recent years, consumers have not appreciated that doing so can result in a charge being generated to their mobile device, or that the entry of their number can be taken as being consent to future marketing by the provider concerned.

2.6 As a result, some consumers have entered a mobile number belonging to someone else (either by mistake or deliberately) and this has generated a charge to a second – unwitting – consumer. Even if there are no chargeable messages, just free marketing messages, the unwitting consumer often feels that their privacy has been invaded (see Part Two for further information around marketing).

2.7 For this reason, we recommend that consumers should always be encouraged to initiate services, or future marketing, with an MO. Failing that:

- All costs should be clearly stated and be proximate and prominent to the field where the consumer is to enter their number;
- After entering the number, a Mobile Terminating message ('MT') should be sent to the consumer. As an example this should state:

"FreeMsg: Your PIN is [e.g. 0911], please delete if received in error"

2.8 An MT message, in these circumstances, should not promote the service itself (e.g. use its name), or give the consumer the option to reply YES to initiate the service. In addition, this method

would require robust systems for verifying any PIN once entered (see paragraph 2.12 below for further details).

2.9 It is more difficult to verify where a charge is generated by a consumer browsing the mobile web, or by using software downloaded to their device. In these circumstances, where the consumer may only have to click on an icon to accept a charge, the MNO has no record of an agreement to purchase, and so robust verification is not possible through an MNO record alone.

2.10 In both of the instances set out above, we would expect providers to be able to robustly verify consent to charge (or to marketing, see Part Two of this General Guidance Note). Factors which can contribute to robustness are:

- An opt-in is PIN-protected (e.g. the consumer must enter their number to receive a unique PIN to their phone, which is then re-entered into a website);
- A record is taken of the opt-in, and data is time-stamped in an appropriately secure web format (e.g. https or VPN);
- Records are taken and maintained by a third-party company which does not derive income from any PRS. We may consider representations that allow a third-party company which receives no direct share of PRS revenue from the transaction, but does make revenue from other PRS, to take and maintain records. It will have to be proven to PhonepayPlus' satisfaction that these records cannot be created without consumer involvement, or tampered with in any way, once created;
- PhonepayPlus is provided with raw opt-in data (i.e. access to records, not an Excel sheet of records which have been transcribed), and real-time access to this opt-in data upon request. This may take the form of giving PhonepayPlus password-protected access to a system of opt-in records;
- Any other evidence which demonstrates that the opt-in cannot be interfered with.

2.11 Providers who are considering using a method of verifying consent to charge, which employs a method that does not involve independent Network operator records of consent, are advised to contact PhonepayPlus before they begin to operate it."

On 6 July 2015, the Executive contacted the Level 2 provider and directed it to provide evidence of when and how a sample of five complainant mobile telephone numbers were opted in to receive the Service. On 14 July 2015 in response to the Executive's direction the Level 2 provider stated:

"Opt in process has been presented in A-D step by step journey case study. It is complex yet straightforward method allowing interaction with full range of service facilities only upon verification of unique pin-code sent to mobile number. Every aspect of user journey is based on conscious consent and desire for enjoying premium video content that is offered by our service."

On 23 July 2015 the Executive contacted the Level 2 provider and directed it to provide evidence of how it had robustly verified consent to charge, and to provide the name of any third party it used for this and a copy of the signed contract between both parties. The Level 2 provider responded on 31 July 2015 stating:

"I hope my reply would clarify the way our service is providing a verifiable verification for consent of charge. Opt in is 'PIN' protected which means the consumer must enter their number to receive a unique PIN to their phone. Such PIN is then re-entered into a website form and is stored with relating time stamp. These details are available on request – they are not eligible for making any changes thereto though after they record of such opt in is taken."

"We understand that it is necessary to protect consumers from becoming members of chargeable mobile or online services without their consent therefore we implemented this 2 step opt in process so that it is not only to enter mobile number and expect premium membership to commence because such method is vulnerable to interference, e.g. mobile number could be provided by someone else than bill payer. Taking into account such possibilities there is another secure step set up and this is where unique PIN is coming into action."

On 18 May 2016 the Executive contacted the Level 2 provider and directed it to provide the identity of the third party company who verified their PIN opt-in. On 26 May the Level 2 provider stated:

"As far as the verifying 3rd party is concerned, we initiated a cooperation with company ETX however integration between our message flow and ETX verification specifications has been very complicated therefore we utilise it on trial basis for chosen marketing campaigns which is letting us to learn how to implement the ETX methodology into our flow and integrate these two together."

"In addition but if we wish to be exact – most of all we trust that our secure opt in flow recordings that we hold internally would be sufficient to provide a tamper proof record of subscribers consent to charge. I am keen to get a report on the details for this internal method and system, should you wish to review it for your due diligence and comfort that opt in records are robust and held in secure data storage."

On 31 May 2016 the Executive contacted the Level 2 provider and directed it to provide robustly verifiable evidence of consent to charge for a sample of 20 complainant mobile phone numbers and provide the Executive with real time access to their opt-in data. On 10 June 2016 the Level 2 provider supplied opt-in data. An example of the evidence supplied by the Level 2 provider appears at **Appendix B**.

Upon review of the information supplied by the Level 2 provider the Executive stated that it was unclear as to how the information supplied demonstrated evidence of consent to charge complainants. In an attempt to verify whether the above information demonstrated that the Level 2 provider held robust evidence of consent to charge, the Executive directed the Level 2 provider to supply the following information:

- I. A clear explanatory note of the information contained in the submitted opt-in information and how this information demonstrated robust evidence of consumer opt-into the Service.

II.A request that the Level 2 provider supply to the Executive real time access to its Service messaging system (which may have taken the form of giving PhonepayPlus password protected access to its Service message logging system).

On 29 June 2016 the Level 2 provider provided the following response to the Executive's enquiries:

I. "I hope that below example would sufficiently (and efficiently) provide you with answer:

MSISDN ***595**

Mobile user was browsing internet on their phone and the nature of their search was linked with service nature i.e. erotic entertainment. Mobile user decided to focus attention on our advertisement in a form of banner that was displaying on their screen.

Mobile user made a decision to check what is behind the banner and hit the ad by clicking on it ('tapping' on it physically in a case of smartphones) and was taken to a service website. It was presenting all possible and available terms and conditions of service, its price and prominent guide on how to leave the service. Contact details for customer line were available without a need to scroll down the screen at any point.

*Mobile user found the service interesting and was willing to spend specified amount (£4.50) which is not significant for a good quality service they can enjoy in private on mobile handset. Mobile user entered a number into special form and received a subscription access pin (**Subscription PIN**) within WAP (free) message. Such pin was solely assigned to this user, no one else.*

*Mobile user was continuously interested in joining the service and entered (hit) the WAP link and was given an opportunity to review terms of service again. Mobile user was happy to proceed and eager to join the subscription and clicked on confirmation button which could only happen if done with consent. Clicking on confirmation button delivered an acknowledgement to our database and we welcomed mobile user as a member. This action was recorded by our system and assigned a secure time stamp (**Verified Subscription Timestamp**). This was confirmed by welcome message sent to mobile user."*

II. "Consent to charge proofs are kept in offline archive to avoid external/ post-date interference as advised in our earlier correspondence.

The secure system has been designed to prohibit potential interference therefore login attempt performed by user with limited admin privileges would be treated as a system threat aiming to tamper with securely stored records."

In response to questioning by the Tribunal, the Executive confirmed that it had not been provided with real time access to AdminX, despite its request. The Executive noted that the Level 2 provider's stated reason for this was a risk of compromising the security of the system (even though PhonepayPlus was a regulator). The Executive stated that its position on the robustness of this

system might possibly have been different if it had been provided with such access, as then the Executive could've checked its system.

The Executive had contacted the Third Party Verifier on 15 June 2016, with the same sample of 20 complainant mobile phone numbers supplied to the Level 2 provider, and requested that the Third Party Verifier confirm when the Level 2 provider started using their opt-in verification, and whether it had records of Service opt-in for the complainant mobile telephone numbers. The Executive noted that on 17 June 2016 the Third Party Verifier stated "they are a client since 1st May 2015" and "we don't have any record of these MSISDNs in our database".

The Executive noted the Third Party Verifier was unable to provide verification that a sample of 20 complainants had opted into the Service and consented to the Service charges. The Executive submitted that the data relating to the WAP opt-in for the individual complainants had not been held by a third party, nor was there any evidence that it was held in a way which meant it categorically could not have been tampered with since creation.

The Executive noted that the Code 12 Guidance and Code 13 Guidance made it clear that all charges must be robustly verifiable. However, the Executive submitted that the Level 2 provider in the relevant period did not utilise the Third Party Verifier's robust verification process. The Executive submitted that although Guidance was not binding on providers, where a provider fails to follow Guidance there was an expectation that it will take equivalent alternative steps to ensure that it fulfils PhonepayPlus' expectations (and compliance with the Code).

The Executive therefore submitted that the Level 2 provider did not have sufficiently robust systems in place to provide evidence of consent to charge, and so asserted that it had breached rule 2.3.3 of the Code.

2. The Level 2 provider admitted the breach in part. The Level 2 provider submitted the following.

It considered the allegation of breach of the Code was made as a result of the Executive's confusion. The Level 2 provider stated that it was not its intention to state that it had PINs stored by a third party so that Executive had to verify that information with Goverifyit. The Level 2 provider asserted that it had stated on a number of occasions that it had complied with current requirements in the best available way and using most efficient method. The Level 2 provider submitted that, unfortunately, the Goverifyit add-on implemented to its service flow was not efficient in a sense that it caused a page to load for long time, making potential subscribers simply go away to another service or advertisement. It stated that it had experienced these delays many times upon trial campaigns and its impression had been that it was an issue at its end that needed further development.

The Level 2 provider stated that it was using internal PIN verification and storage in the meanwhile, which served well over time. The Level 2 provider believed that its internal system for subscription verification was a state of art project and was always flawless when it came to verifying consumer mobile numbers entered on a website and interaction initiated by users via a WAP link containing

a secure pass-key for subscription (i.e. each subscriber could be verified with a positive outcome). The Level 2 provider submitted that it was an alternative step it undertook to ensure it fulfilled PhonepayPlus expectations.

The Level 2 provider stated that it had encountered a percentage of consumers who were not particularly satisfied with the Service and these had been refunded even if they used the Service and its content, as a goodwill gesture. The Level 2 provider stated that it was discontented to learn that complaints were a factor that initiated an investigation into the Service. The Level 2 provider stated that its Customer Services department made its best efforts to always explain how the Service and billing mechanisms operate. The Level 2 provider asserted that consumers who initially complained to the Executive were simply not aware of what they wish to achieve and to what kind of Service they subscribed, and submitted that although this sounded unlikely, from its experience this was very often the case. The Level 2 provider asserted that users browsed the internet, encountered its advertisement, took a decision to join the Service, and see prominent pricing information but their brain does not transfer the information to the correct part of their brain. The Level 2 provider asserted that if they don't have to take out cash from their pocket physically, they don't consider it as transaction and it simply leads to an act of denial at a later date when they check their bill. The Level 2 provider asserted that they tend to ignore monthly reminder messages, regarding them as spam, when they dispose of a memory of joining a premium rate service. The Level 2 provider asserted that, even if we analyse a double opt in subscription process like the one it operated when users had to physically click on a URL embodied in a text message and again click on an acceptance box, if they don't want to remember that action, they remove it from their memory just because it was a mobile phone transaction. The Level 2 provider asserted that it knew of these instances from experience as reports from its Customer Services department were indicating this was the case on a majority of occasions where a complaint was raised.

The Level 2 provider asserted that it had provided full consumer journey experience to the Executive and wished for it to be presented with its response for the attention of the Panel. Firstly, the Level 2 provider asserted that its advertisements were only targeted at mobile users who were happily browsing internet on their phone and the nature of their search was linked with specific nature, i.e. erotic entertainment. The Level 2 provider asserted that the mobile user decides to focus attention on its advertisement in a form of banner that was displayed on their screen. The Level 2 provider submitted that no reasonable consumer could expect to receive a good quality service for free. The Level 2 provider asserted that consumers may claim they expected this, but compared the situation to going to a big brand high street shop expecting free wardrobe from the current collection - they might get a free sample, but if they want a full size product, they have to pay for it. The Level 2 provider stated that it had tested several sample bonuses that could attract users, like 24-hour free service or even 7 days free. The Level 2 provider asserted that in every instance where a consumer logged a complaint saying they were not aware of charge or did not give consent to charge, this was not legitimate and untrue, and submitted this arose from consumers' instinct of denial. The Level 2 provider asserted that it was patient, understood human nature and followed a policy where every consumer was treated with attention to a claim and every claimant is issued with refund, even if a small bonus as a goodwill gesture. The Level 2 provider

asserted that they may then come back and join the Service again (noting that addictions is a separate subject).

The Level 2 provider asserted that a mobile user made a decision to check what is behind the banner and hit the ad by clicking on it ('tapping' on it physically in a case of smartphones) and was then taken to a service website. The Level 2 provider asserted that it presented all possible and available terms and conditions of service, its price and a prominent guide on how to leave the Service. The Level 2 provider asserted that contact details for the customer line were available without a need to scroll down the screen at any point.

The Level 2 provider asserted that mobile users found the service interesting and were willing to spend the specified amount (£4.50) which was not significant for a good quality service they can enjoy in private on a mobile handset. The Level 2 provider asserted that mobile users entered a number into a special form and received a subscription access PIN (subscription PIN) within a WAP (free) message. Such PIN was solely assigned to this user.

The Level 2 provider asserted that if a mobile user was continuously interested in joining the Service and entered (hit) the WAP link, the user was given an opportunity to review terms of service again. If a mobile user was happy to proceed and eager to join the subscription, they clicked on the confirmation button which could only happen if done with consent. Clicking on confirmation button delivered an acknowledgement to its database and it welcomed the mobile user as a member. The Level 2 provider asserted that this action was recorded by its system and assigned a secure time stamp (Verified Subscription Timestamp). This was confirmed by a welcome message sent to the mobile user.

The Level 2 provider asserted that the above consumer journey could not have been more complex but all these measures were taken to make sure users would not just accidentally click on a screen and join the unwanted service. The Level 2 provider underlined that users expressly granted their consent to subscribe to the Service via two positive actions and lack of negative action at a final stage which also counted towards a full picture. The Level 2 provider explained that the first positive and physical action was to enter their mobile number into a website. The second action was a compilation of small steps, i.e. to open the text message from inbox, to click on an interactive link, to get redirected to the mobile browser screen, to read terms of service and ultimately – to physically confirm acceptance of terms by clicking on ENTER section, using a human finger to touch the screen in the correct place with appropriate pressure adequate for handset settings. The Level 2 provider submitted that consumer harm did not occur in any instance. The Level 2 provider asserted that the Executive is bound by firm Code rules that have restricted interpretation, therefore to acknowledge its continuous and ever-standing offer of cooperation, it was ready to admit the breach in part, in that not all requirements of Guidance were met. The Level 2 provider asserted that this failure was however not due to bad will or negligence. The Level 2 provider asserted that it had trusted that its Service opt in method was satisfactory because users were providing it with positive feedback on many occasions.

The Level 2 provider listed differences and similarities between the third party verification system and its "AdminX" verification for consent to charge:

DIFFERENCES:

- A. Admin X – pin enclosed within free wap text
Third Party – pin enclosed within free sms text
- B. AdminX – user simply clicks on interactive link wap message and page on mobile browser opened
Third Party – user has to remember the pin or copy it onto handset clipboard
- C. AdminX – consent to charge is obtained once user again confirms acceptance of Terms and Conditions and click on accept press button on the service page. Clicking on text message link does not initiate the subscription at all, and it believed this is where the Executive got confused. For subscription to commence, there needs to be another action from a user – a physical press on phone screen in a designated space, which is an equivalent to second stage of a double opt in process required by Code of Practice.
Third Party – user has to type in pin into box
- D. AdminX – record of date, time and pin is stored in offline database, which means it cannot be accessed online (i.e. cannot be hacked) and details cannot be changed or interfered with in any way.
Third Party - record of date, time and pin is stored in a database, which it trusted according to contract cannot be changed or interfered with in any way

SIMILARITIES:

- A. AdminX – message with pin is free of charge
Third Party – message with pin is free of charge
 - B. AdminX – double opt in process in place to avoid accidental or unwanted subscription
Third Party - double opt in process in place to avoid accidental or unwanted subscription
 - C. AdminX – mobile number must be entered on website and verified with user's handset
Third Party - mobile number must be entered on website and verified with user's handset
 - D. AdminX – consent of charge is obtained only once 2-step opt in process is accomplished
Third Party - consent of charge is obtained only once 2-step opt in process is accomplished
 - E. AdminX – opt in records are kept in safe tamper proof place
Third Party - opt in records are kept in safe tamper proof place
3. The Tribunal considered the Code and all the evidence before it. The Tribunal noted that the Level 2 provider had admitted the breach in part, but not in full.

The Tribunal considered that the Level 2 provider had not made it adequately clear what process it had been using to opt-in consumers, and the description of the process had not been consistent throughout the course of correspondence. The Tribunal noted that the Level 2 provider referred to a second message which contained a PIN; however the evidence indicated that this was not a number which a consumer was required to type into another website as part of the opt-in process. The evidence indicated that a consumer merely had to click on the link included in that message to send them to a website from where the Service could be accessed. The Tribunal considered that this system did not accord with the recommendations made in the Guidance that opt-ins were PIN-protected, or that records were taken and maintained by a third-party company which did not derive income from any PRS. The Tribunal did not consider that it had been demonstrated that the records of opt-in could not be tampered with after they were created. The Tribunal considered that the "AdminX" system did not provide robustly verifiable evidence of consumer consent to be charged. The Tribunal considered that the system may have been considered sufficient to provide such evidence had direct access to the raw opt-in data been provided to the Executive.

The Tribunal considered the Level 2 provider's submissions that it had developed its own system for verifying consent to charge, and had trusted that this method was satisfactory. The Tribunal also noted that the Level 2 provider had asked the case investigator in an email of 23 May 2016 to provide it with assurance that it was dealing with consumers correctly. The Tribunal commented that providers were required to pro-actively take steps to comply with the Code. The Tribunal accepted that the Level 2 provider was not obliged by the Code to use a third party to verify consent to charge records, but commented that the Level 2 provider could have taken compliance advice if it was unsure of what it had to do to comply with the Code, and that providers who were not using independent Network operator records were encouraged to do this by the Guidance (as set out above).

The Tribunal was concerned that the Level 2 provider's response which referred to consumers' "instinct of denial" and "addictions", and indicated that third party verification had not been implemented because the Level 2 provider had found it to be "too slow", indicated it had not taken seriously its obligations to ensure that it held evidence which established consumers' consent to be charged.

The Tribunal considered the complainants' accounts that they had not consented to Service charges, and the evidence regarding their opt-in to the Service. The Tribunal noted that no explanation had been provided for why records showed that a number of the complainants had opted into the Service at exactly 4pm on Christmas Day 2015. The Tribunal noted that a significant number of complaints had indicated that they had found it difficult to obtain a refund promptly.

Consequently, for the reasons advanced by the Executive, the Tribunal was satisfied that the Level 2 provider had not provided evidence which established consumers' consent to be charged for the Service. Accordingly, the Tribunal upheld a breach of rule 2.3.3 of the Code.

Decision: UPHELD

SANCTIONS

Representations on sanctions made by the parties

1. The Executive, based on its view that the alleged breach was “very serious” submitted that the following sanctions were appropriate:

- a formal reprimand;
- a requirement that the Level 2 provider remedy the breach by ensuring that it has robust verification of each consumer’s consent to be charged before making any further charge to the consumer, including for existing subscribers to the Service;
- a fine of £150,000; and
- a requirement that the Level 2 provider must refund all consumers who claim a refund, for the full amount spent by them on the Service, within 28 days of their claim, save where there is good cause to believe that such claims are not valid, and provide evidence to PhonepayPlus that such refunds have been made.

In response to questioning by the Tribunal, the Executive stated that it did not consider the Level 2 provider’s offer sufficient to remedy the breach, as it did not ensure that robustly verifiable consent to charge evidence would be held for existing consumers before they incurred further charges. If the Tribunal did not use the Executive’s wording, this would not prevent existing subscribers being charged without the Level 2 provider holding such evidence. The Executive did not consider the monthly reminder message sufficient for the purposes of evidencing consent, as it submitted that consumers did not always check these. The Executive submitted that the Level 2 provider’s suggested remedy was not sufficient to remedy the breach for existing subscribers; it should be asked to go back and re-subscribe existing subscribers for whom it did not have robust verification.

2. In response, the Level 2 provider submitted that a remedy the breach sanction was not necessary as it considered having a robust internal system was, just the same, satisfactory to obtain consent to charge. The Level 2 provider considered this was a very punitive measure and not regarded as a remedy to the alleged breach as it required a physical action from a subscriber who had already expressed a will to be subscribed. Repeated requests to subscribe would make the service operation non-transparent as this option was not a part of the original and initial terms and conditions of the service. The Level 2 provider submitted that a monthly reminder was a sufficient and mandatory method of reminding consumers about their subscription.

In relation to refunds, it stated that remedy was already in place and it had provided the Executive with evidence on 6th June. The Level 2 provider stated it was not sure on the implications of a formal reprimand and was taking legal advice on this. The Level 2 provider submitted that the recommended fine was too high as not supported by most recent adjudications. The Level 2 provider did not make any specific representations about the severity rating of the alleged breaches.

Taking into account all mitigating factors, the Level 2 provider had submitted that the below sanctions would be appropriate:

- formal reprimand;
- continued refunds for users who claim a refund where there is a reasonable grounds for such a claim;
- independent compliance advice to confirm the Level 2 provider operated a fully compliant service as instructed; and
- a monetary fine of £85,000

Initial overall assessment

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

Rule 2.3.3 – Consent to charge

The initial assessment of rule 2.3.3 of the Code was **very serious**. In determining the initial assessment for this breach of the Code the Tribunal applied the following criteria:

- The Level 2 provider charged consumers but was unable to provide robustly verifiable evidence of consent to charge;
- The case had a clear and highly detrimental impact on consumers; and
- The nature of the breach was likely to severely damage consumer confidence in premium rate services

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

Final overall assessment

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

- The provider had failed to follow Guidance or take alternative steps which, had they done so, would have avoided breaches occurring, and the importance of doing so in relation to evidence of consent to charge had been highlighted by numerous previous adjudications of the Tribunal; and
- There was evidence that the provider had failed to provide adequate customer service to consumers, including that consumers had undue difficulties in communicating with the provider, and difficulties in obtaining promised refunds promptly.

The Tribunal did not find any mitigating factors. The Tribunal did not consider that steps taken to avoid breach of the Code in relation to future subscribers which were taken after receipt of an Interim Warning Notice constituted prompt action to rectify the breach. Given the Tribunal's findings regarding the standard

of customer service the Tribunal did not find that provision of refunds had been pro-active. The Tribunal did not consider that the level of cooperation with the Executive was beyond that which was to be expected.

The Level 2 provider's evidenced revenue in relation to the Service in the period from May 2015 to August 2016 was in the range of Band 2 (£500,000 to £999,999).

Having taken into account the circumstances of the case, the Tribunal concluded that the seriousness of the case should be regarded overall as **very serious**.

Sanctions imposed

The Tribunal noted the submissions of the Executive and the Level 2 provider regarding the wording of the remedy the breach sanction. The Tribunal noted that the Level 2 provider's evidence was that consumers tend to ignore monthly reminder messages, regarding them as spam. The Tribunal did not consider that wording the sanction in the way proposed by the Executive would be unfair to the provider in the circumstances of the case, as any user who genuinely enjoyed the Service and wished to continue to receive it would be likely to confirm their wish to be subscribed to the Service if they were invited to do so.

The Tribunal noted the Executive and the Level 2 provider's submissions regarding a fine. In making its own determination as to the appropriate level of fine, the Tribunal took into account the seriousness of the case, other sanctions which it intended to impose, and the fact that the number of complaints and relevant service revenue may have been lower had the Executive progressed the case more quickly between July 2015 and May 2016.

The Tribunal chose not to impose a compliance advice or compliance audit sanction but commented that the Level 2 provider may wish to voluntarily seek advice or an audit.

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

- a formal reprimand;
- a fine of £135,000;
- a requirement that the Level 2 provider remedy the breaches by ensuring that it holds robust verification of each consumer's consent to be charged before making any further charge to the consumer, including for existing subscribers to the Service; and
- a requirement that the Level 2 provider must refund all consumers who claim a refund, for the full amount spent by them on the Service, within 28 days of their claim, save where there is good cause to believe that such claims are not valid, and provide evidence to PhonepayPlus that such refunds have been made.

Administrative charge recommendation:

100%

The decision of a previous Tribunal on 28 July 2016 to impose interim measures is attached at Appendix A

APPENDIX A

Application for interim measures pursuant to Code of Practice paragraph 4.6

Case ref: 77718
Service: 'Glamour Content' glamour video subscription service
Level 2 provider: Skybytes Limited
Level 1 provider: Zamano
Cost: £4.50 per week
Shortcode: 84507
Shortcode to send 'STOP' if different

Tribunal number: 188

Adjudication

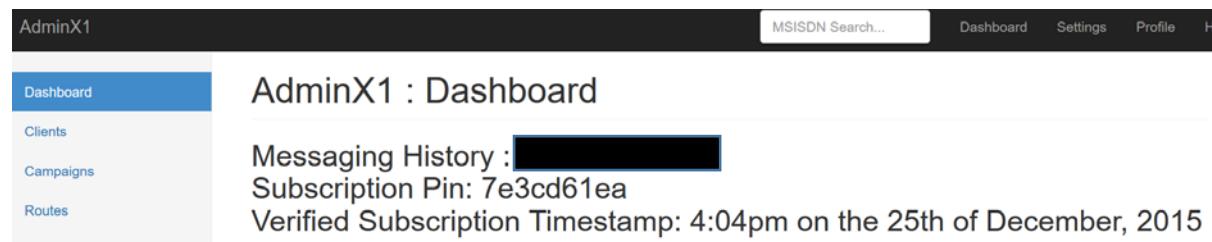
- The Tribunal has paid full regard to the material supplied by the Executive and the Level 2 provider
- In respect of the material submitted by the Executive, the Tribunal noted in particular the consistency of the complaints, and the correspondence with ETX (UK) Limited, appear to give support to a case that there was a lack of third party evidence of consent to charge for the complainants.
- The Tribunal has paid full regard to the representations provided by the Level 2 provider (relevant party). In respect of this material the Tribunal noted in particular that:
 - a) No cogent and robust evidence of consent to charge for the complainants had been provided in their response to the Notice;
 - b) Submissions had been made on potential mitigating factors, including subsequent implementation of GVI and providing refunds to complainants. The Tribunal paid regard to these submissions, and noted that this evidence was of limited significance in that it related to one recent opt-in which was not an opt-in relating to any one of the complainants who was the subject of the current Application;
 - c) Although there may not have been any legal requirement to file accounts with Companies House, the Level 2 provider had not supplied credible evidence of its current financial situation to the Executive; the Interim Warning Notice makes specific reference to this type of material.
- The Tribunal has paid regard to the Supporting Procedures, including the factors set out at paragraph 80 and 91.

Having considered the evidence before it, the Tribunal has made the following determinations:

- 1) At first appearance (and subject to evidence, arguments or information being later supplied and/or tested), there appears to be sufficient evidence that could support a breach of the Code of Practice Rule 2.3.3.

- 2) The Tribunal considers that the Level 2 provider will not be able or willing to pay such refunds, administrative charges and/or financial penalties that may be imposed by a Tribunal in due course. The Tribunal notes in particular:
 - a) the Executive's comments in its Debt Collection Withhold Assessment regarding:
 - i) the Level 2 provider's date of incorporation, and lack of published filed accounts or any profit or balance figures
 - ii) the potential seriousness of the breach, and service revenue, which could result in a higher level of fine; and
 - b) The Level 2 provider's failure to supply evidence to establish that it would be able to pay any sanctions imposed (as estimated by the Executive).
- 3) The Tribunal is satisfied that PhonepayPlus has made reasonable endeavours to notify the relevant party of its initial findings and the proposed interim measures.
- 4) The Tribunal considers that the measures set out below are appropriate and proportionate to take in the circumstances of this case. The Tribunal takes into account in particular the revenue generated by the service, the sanctions imposed in previous similar cases, and the lack of information supplied by the Level 2 provider regarding its financial position.
- 5) Accordingly, the Tribunal hereby directs that:
 - a) PhonepayPlus is authorised to direct a withhold of up to £167,000.
 - b) The sums directed to be withheld may be allocated and re-allocated between any Network operators or Level 1 providers for the Service as the Executive sees fit from time to time, provided that the total sum withheld by all providers does not exceed the maximum sum authorised in this decision.
 - c) The Executive is given discretion to vary the total directed to be withheld downwards in the event that it is provided with alternative security which is, in its view, sufficient to ensure that such refunds, administrative charges and/or financial penalties as it estimates a CAT may impose in due course are paid.
 - d) Such interim measures are to be revoked upon the case being re-allocated to Track 1 or otherwise discontinued without sanction.

**Mohammed Khamisa QC
28 July 2016**

APPENDIX B - Level 2 provider's evidence of consent

The screenshot shows the AdminX1 dashboard interface. The left sidebar has four items: Dashboard (which is selected and highlighted in blue), Clients, Campaigns, and Routes. The main content area is titled "AdminX1 : Dashboard". It displays the following information:
Messaging History : [REDACTED]
Subscription Pin: 7e3cd61ea
Verified Subscription Timestamp: 4:04pm on the 25th of December, 2015