Tribunal meeting number 202

Case reference: 72275

Level 2 provider: Syncronized Limited

Type of service: Glamour video subscription service

Level 1 provider: Veoo Ltd; Zamano Solutions Ltd, Fonix Mobile Limited

Network operator: All Mobile Network operators

This case was brought against the Level 2 provider under Paragraph 4.5 of the Code of Practice

Background

The case concerned a glamour video subscription service operating on shortcodes 66255, 88150, 82999, 84506, 80008, and 89225 (the "Service").

The Level 2 provider for the Service was Syncronized Limited (the "Level 2 provider"). The Level 2 provider had been registered with the PSA since 10 February 2012.

The Service was stated to be a glamour video subscription service charged at £3 and £4.50 per week. The Level 2 provider stated that the Service started in August 2014. The Executive noted that on 2 April 2015 the "4 Your Eyes Only" Service changed to the "Lesbian Course" Service from £3.00 per week to £4.50, as shown on the Level 2 provider message logs.

The table below sets out the shortcodes on which the Service operated and the Level 1 providers for each shortcode:

Shortcode	Level 1 provider	Shared shortcode?
66255	Fonix	No
88150	Veoo	Yes
89225	Veoo	Yes
82999	Veoo	Yes
80008	Veoo	No
84506	Zamano	No

In a direction dated 16 February 2016, the Executive asked the Level 2 provider to provide an up to date consumer journey for the Service. The response is set out at **Appendix A.**

Summary of complaints

The Executive received 418 complaints concerning the Service between 5 March 2015 and 15 November 2016.

Complainants variously alleged that the Service and charges incurred were unsolicited.

A sample of complainant accounts is provided below:

> *"I do not lightly subscribe to a service. I definitely would not subscribe to anything like this. I did not previously text STOP as I thought this was a fake number and did not want them to know this was an active number. Only after checking my account did I realise I was actually being charged for this. So today I sent STOP to this number. I do not actually know when the charges started. Is there any way of getting my money back. This is very disconcerting that someone can just take money out of my account like this- so easily."*
>
> *"Consumer has no idea how she got subscribed to the service. Consumer doesn't look up adult content. Consumer doesn't play any games on her phone…"*
>
> *" …I have not subscribed to any premium service. I don't even know what this is about, I din't [sic] even open the texts to see what it was as I thought they were scams…"*
>
> *" I have no idea what this service is and did not opt in for any sms messages to be sent to me. I have now been charged at least £6 for a service I never subscribed to. This is complete fraud…"*

Complainant text message logs

The Executive noted from the majority of the text message logs supplied by the Level 2 provider that:

- there was a high failure rate of chargeable Service messages following the purported consumers' opt-in and;
- the delivery status for Service messages was unclear.

In these logs, failed messages occurred from the date of the complainants' purported opt-in. The failed messages were later followed by successfully delivered chargeable messages. The Executive sent several directions for information regarding this issue to the Level 2 provider.

In light of the high number of failed messages identified by the Executive in the complainants' text message logs and the possible potential explanations offered by the parties in the value chain for the failed messages, on 2 March 2016 the Executive contacted 228 complainants [the total number of complaints received by the PSA about the Service with email addresses at that date] with the following series of questions:

"Is the mobile phone that received the chargeable text messages on contract or pay-as-you-go?

If the mobile phone that was charged is pay-as-you-go, please advise whether you regularly / always had more than £3 credit on your mobile phone?

Please advise whether the mobile phone that received the chargeable messages was regularly switched off and/or had no mobile signal for long periods of time (i.e. for more than several days)?

Please advise whether you transferred your mobile number between mobile telephone companies in the six months before your received the chargeable text messages? If yes, please confirm if you experienced long periods with no signal and/or difficulty in sending and receiving text messages."

In addition, the complainants were sent copies of the promotional material at **Appendix A** and asked whether they recalled viewing and/or interacting with it or a similar service promotion.

As at 12 December 2016, the Executive had received responses to the questionnaire from 59 complainants. Below is a breakdown of the complainant responses:

Question	Response	Comments
Is the mobile phone that received the chargeable text messages on contract or pay-as-you-go?	59 consumers stated they were on contract	N/A
If the mobile phone that was charged is pay-as-you-go, please advise whether you regularly / always had more than £3 credit on your mobile phone?	N/A	N/A
Please advise whether the mobile phone that received the chargeable messages was regularly switched off and/or had no mobile signal for long periods of time (i.e. for more than several days)?	47 consumers advised that their mobile phone was not regularly switched off and/or had no mobile signal for long periods of time 3 Consumers did not respond to this question	• At the time the text message was received- no problems with signal. I always turn off mobile data and wifi when not in use. I deleted the text message first received. However when the second text arrived weeks later I was on holiday in the UK with poor signal. • The Ipad is off unless we are going away with it- could be several weeks at a time

		• Phone was switched off at night • Always on/but I fly long haul so am in different time zones – phone switched off up to 14 hours while on flying duties • Yes it is regularly switched off or without signal • No apart from end of September for about two weeks when I went abroad • Reception is poor in my household however intermittent and would not be without signal for as long as multiple days • Poor signal zone, messages via wifi (TuGo) • Switched off for short periods only
Please advise whether you transferred your mobile number between mobile telephone companies in the six months before your received the chargeable text messages? If yes, please confirm if you experienced long periods with no signal and/or difficulty in sending and receiving text messages	51 consumers advised they had not transferred mobile numbers in the last 6 months 2 consumers did not respond to this question	• The number transferred over without a problem • Yes transferred- no signal difficulties • I took out new contract with EE maybe 6 months before- I was with Orange before • Yes number transferred to a different account with same company o2 in Feb 2015 • Switched from virgin to 3
Please advise if you recall viewing and interacting with the attached, or a similar, promotion?	52 consumers advised they did not recall viewing and interacting with the promotional material supplied by the Executive	• Emails were deleted without opening and I was still charged

	4 consumers did not respond to this question 2 consumers stated they did recall viewing and interacting with the promotional material supplied by the Executive	

The Investigation

In accordance with the transitional arrangements set out at paragraph 1.8 of the PSA 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 12 December 2016 with a deadline for response of 28 December 2016. The Level 2 provider responded on 4 January 2017. Within the Warning Notice the Executive raised the following breaches of the PSA Code of Practice (the"**Code**"):

- Paragraph 4.2.5/4.2.3 – Failure to disclose information (12/13/14th Edition)
- Rule 2.3.3 – Consent to charge (12/13/14th Edition)
- Paragraph 3.1.7 – Inadequate Technical Quality (13/14th Edition)

Having heard the Level 2 provider's oral representations, the Tribunal reached a decision on the breaches raised by the Executive on 15 February 2017.

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, and the Level 2 provider's other evidence submitted in the course of the investigation)
- Correspondence between the Executive and the Fail2 Ban developer
- Complainant questionnaire responses
- Sample complainant message logs
- General Guidance Note 'Privacy and consent to charge' in support of the Code of Practice, 12th Edition and General Guidance Note 'Consent to Charge' in support of the Code of Practice, 13th Edition
- Previous Track 1 procedure documentation

- Service revenue information
- The Warning Notice dated 12 December 2016 and attachments
- Level 2 provider's response to Warning Notice dated 4 January 2017; and
- Post-Warning Notice correspondence from the Level 2 provider, including correspondence relating to an adjournment application, and correspondence from the Level 2 provider dated 15 February 2017 including a log for MSISDN *******8216 showing free messages.

Submissions and Conclusions

Preliminary Issue

On 2 February 2017, the Level 2 provider applied for the case to be adjourned from 15 February 2017 to another Tribunal date, because its Director and its consultant were now unavailable to attend to make oral representations on that date.

When the Executive had sought dates of availability for a re-convened Tribunal on 1 February, the Level 2 provider had indicated its representative would be available on the morning of 15 February.

The Chair of the Tribunal carefully considered the application, together with the Executive's written response. Having done so, the Chair refused the application on 8 February 2017. In reaching that decision, the Chair noted that (a) the unavailability of the Level 2 provider's preferred representative did not preclude it from making representations on the day either directly or in writing or by telephone; (b) given the date of the original hearing, their consultant should have already prepared material for the Level 2 provider's representations on that date; (c) there was no evidence that the factual situation in relation to the hearing on 15 February 2017 – as it might be advanced by and on behalf of the Level 2 provider – had not altered; (d) the hearing would only be taking into account "informal representations"; and (e) there was no evidence that the service provided by the Level 2 provider had ceased, and it appeared that there may be very serious and ongoing consumer harm being occasioned by the operation of the Service. Delaying the proceedings by a further three weeks (as requested by the Level 2 provider)– without the matter being addressed – could contribute to serious ongoing consumer harm in this case.

In oral representations on 15 February 2017, the Level 2 provider submitted that the decision by a single Chair not to allow them an adjournment was an apparent legal error, as it did not allow them to have an independent representative for the oral representations. It had appointed an independent representative for the 8 February 2017 but they were informed of a change of date without the opportunity to reach an agreement. It understood the adjournment of the original case was due to strike action. It understood that the effect of this was to deprive it of the chance of having a supporting representative. It acknowledged that it had been advised that it could appoint a new representative but given the short notice and the nature of the Tribunal case, it felt that this was an irrelevant suggestion.

Alleged Breach 1

Rule 2.3.3. - "Consumers must not be charged for premium rate services without their consent. Level 2 providers must be able to provide evidence which establishes that consent."

1. The Executive asserted that the Level 2 provider had breached rule 2.3.3 of the Code because robust evidence of consent to charge was not held for complainants.

   The Executive relied on the content of the PSA Guidance on 'Privacy and consent to charge' (the "Guidance"), correspondence exchanged with the Level 2 provider, complainant accounts (which are referenced in the 'Background' section above), complainant questionnaire responses (which are referenced in the 'Background' section above) and complainant text message logs.

   The Executive noted that the message logs supplied by the Level 2 provider showed that all complainants, for which the Executive had been supplied a message log, had opted-in to the Service via the WAP route.

   The Executive submitted that the Level 2 provider was required to hold robust consent to charge evidence for the WAP opt-ins. The Executive noted that the Guidance makes it clear that all charges must be robustly verifiable. Although Guidance is not binding on providers, where a provider fails to follow Guidance there was an expectation that it would take equivalent alternative steps to ensure that it fulfils PSA's expectations (and compliance with the Code).

   On 2 March 2016, the Executive contacted the Level 2 provider and asked it to provide robust evidence to show opt-ins for a sample of 9 complainants. On 21 March 2016, the Level 2 provider responded to this question. A sample from the response supplied by the Level 2 provider is below:

   ********2847*

   "Opt in:

   Date: 03/10/2014 21:29

   Subscription was activated and user got access to content straight away, even prior to billing attempts commenced.

   Unique PIN: 841edd908 – stored securely in tamperproof database

   3rd party verification: This service was previously been a subject of Track 1 Procedure where we explained that we were using Pinchecked service. We then moved to GVI in October 2014 (which was a prompt action/ remedy) verification since we encountered issues with opt-ins bypassing the Pinchecked channel. This has been fully outlined during Track 1 procedures

between October 2014 and January 2015 and our remedy plan was accepted which resulted in Track 1 being resolved.

Opt in flow:

1. *User accessed banner advertised online.*
2. *User was directed to landing page presenting terms and conditions*
3. *User would enter mobile number into msisdn box*
4. *User would then receive a free text containing a weblink that – once opened would take them into their phone internet browser.*
5. *User would be presented with a 2nd stage landing page asking user to accept terms and conditions should they wish to subscribe to the service.*
6. *Once user clicked on such 'Enter' button, they would automatically be directed to a page (on their mobile internet browser) where content (videos) could be viewed, i.e. they would get instant access to content they wished to view.*
7. *Subscription would commence with join message being sent to users as well*
8. *Usually after 24 hours (but never prior to actual physical acceptance of terms and conditions i.e. clicking on 'enter' button) billing attempts would commence on weekly basis."*

The Executive noted from the complainant message logs that all complainants appeared to have purportedly opted-in to the Service before 7 January 2015, which fell into a period where the Level 2 provider knew it had obtained no robust evidence of consent to charge.

The Executive noted from a previous Track 1 procedure that the Level 2 provider had stated that they were previously using Pinchecked service which was by-passing some subscribers. For this reason, the Level 2 provider said it had moved this service to GoVerifyIt in mid-October 2014. The Executive noted that the Track 1 action plan dated 7 January 2015 included a consent to charge breach for the Level 2 provider's WAP and MO opt-in services.

The Executive submitted that the Level 2 provider charged consumers in the period after 7 January 2015 whilst knowing that it did not have the required robust third party verification of consent to charge in respect of those consumers. At the time the charges were made, the Level 2 provider was aware that it did not hold the required robust third party verification of consent to charge for consumers who opted-in (if in fact they did opt-in) prior to that date.

In response to questioning from the Tribunal, the Executive confirmed it had not received an update from the Level 2 provider in December 2016 on the number of consumers who had been unsubscribed as had been promised.

In response to questioning from the Tribunal about two of the narrative complaints that appeared to identify a different service provider, the Executive noted that the service did appear to be a Syncronized service but it would look into whether they had been attached to the wrong case.

For the reason set out above the Executive asserted that the Level 2 provider did not have consent to charge complainants and was unable to provide evidence which established that consent. Accordingly, the Executive submitted that the Level 2 provider had acted in breach of rule 2.3.3 of the Code.

2. The Level 2 provider admitted the breach in part. The Level 2 provider stated that its evidence of consent to charge did not fall under the definition of 'robustness' outlined by the Code and the main reason for this lack of coherence was a lack of third party record for the Service subscribers under investigation.

   The Level 2 provider stated that its opt-in process was based on a double opt-in scenario acceptable to the regulator and networks, and that the sole difference was that the record of PIN was held internally by the Level 2 provider.

   The Level 2 provider submitted that it had taken all available steps to prevent consumer harm, mitigating any potential fault, including:

   a) Following the Track 1 procedure and additionally successfully completing an external compliance audit, the report of which was supplied to the Executive with full supporting notes;
   b) Changing third party verification partner when it was noted that original provider was not able to assure the robustness of online WAP opt-in;
   c) Implementing various systems to improve the system of message transmission, which was concluded with notable success;
   d) Employing diversified solutions for consumer protection and support (e.g. website forms, Google search engine "one - step access", which meant that if a consumer searches for the shortcode, the first result would take them to its subscription management website where they can opt out and view the Level 2 provider's contact details), and providing a report on this to the Executive;
   e) Issuing refunds to subscribers, and providing a report on this to the Executive (the reimbursement process was still continuously in place);
   f) Proposing a settlement (including charity donations, and an early case settlement which would have saved the consumer hassle and administrative (i.e. public- costs), offering full cooperation to the Executive on numerous occasions during the investigation.
   g) Proactively (i.e. not on the Executive's request, on its own initiative) supplying the Executive with updated reports on remedies applied; and
   h) Taking an active part in industry events and meetings which clearly expressed its involvement in regulatory compliance processes and care for the industry in the broad sense.

In oral representations, the Level 2 provider explained that in 2015 it had sought independent compliance advice and passed an audit. The results of this were given to the Executive and it had further explained that its issue with its service provider was resolved. It had provided a sample of users whose opt-ins had been verified by GoVerifyIt. The Level 2 provider referred to the correspondence with ETX who had confirmed that the type of verification it had introduced was approved by the regulator.

In February 2016, the Level 2 provider had received a preliminary investigation letter, directing it to answer questions regarding the Service operation. It understood this was triggered by consumer complaints which it had in fact already addressed. The opt-ins all pre-dated closed correspondence and the compliance advice. The Level 2 provider's view was that these complaints were potentially made because the consumers had insufficient awareness of how the PRS they had joined worked. It had had no hesitation to refund them, even if the Service had been used. The Level 2 provider stated that the number of these complaints was so insignificant compared to the volume of satisfied Service members.

The Level 2 provider stated that it supported this with several updates to the Service to comply with the law, such as the important directive on distance selling.

The Level 2 provider submitted that the complaints were irrelevant. An industry debrief had indicated to it that consumers were not familiar with the consequences of signing up to PRS; they do not read the terms and conditions and don't opt out promptly because advice on Google says they should not do so. The Level 2 provider clarified that here it was referring to the initial sign in procedure when it provided terms and conditions. The Level 2 provider said that if this caused the end of its business, this would be very disappointing. The Level 2 provider had given consumers every way to terminate the Service and to claim refunds, even if they didn't read the terms and conditions in the first place.

The Level 2 provider submitted that the consumer questionnaire responses had no merit and so asked for these to be removed from the case material.

In response to questioning from the Tribunal about why it had referred to the particular MSISDN it had selected as an example MSISDN for which it had robust verification of consent, the Level 2 provider accepted that the MSISDN in question was not related to a complainant. The Level 2 provider said it could not at that time produce an opt-in for a consumer that complained, as those pre-dated its implementation of full online GVI. The check it had done was a standard one for the Executive's records, to give peace of mind that it does employ a proper verification system, and for future reference.

3. The Tribunal considered the Code and all the evidence before it, including the consumer complaints. The Tribunal noted the Level 2 provider's partial admission of the breach.

The Tribunal noted the Level 2 provider's submission that the consumer questionnaire responses should not be admitted as evidence. The Tribunal considered that, in the context of the allegations and the Level 2 provider's admission, it was not necessary to accord any weight to the consumer questionnaire response.

The Tribunal noted the Executive's evidence that logs showed all complainants as opting in to the Service before 7 January 2015, which fell into a period where the Level 2 provider knew it had obtained no robust evidence of consent to charge. The Tribunal noted the Executive's evidence that the Level 2 provider charged such consumers in the period after 7 January 2015. The Tribunal considered that, at the time charges were made, the Level 2 provider was aware that it did not hold the required robust third party verification of consent to charge for consumers for whom logs showed they opted-in prior to that date.

The Tribunal noted that the Level 2 provider had queried whether the Executive had verified the Level 2 provider's evidence submitted, such as evidence that it did hold robust evidence of consent for a sample of consumers, with the Level 1 provider. The Tribunal noted that, even if the Executive had verified such evidence with the Level 1 provider, it would not have contradicted the Executive's case since the sample did not include complainants.

The Tribunal was satisfied that the Level 2 provider had not provided robust evidence that consumers had given their consent to charge. Accordingly, the Tribunal upheld a breach of rule 2.3.3 of the Code.

Decision: UPHELD

Alleged Breach 2

Paragraph 4.2.5 of Code 13 and Paragraph 4.2.3 of Code 14

"A party must not fail to disclose to PhonepayPlus when requested any information that is reasonably likely to have a regulatory benefit in an investigation." (4.2.5)

"Where a direction is made pursuant to paragraph 4.2.1 a party must not fail to disclose to the Phone-paid Services Authority, when requested any information that is reasonably likely to have a regulatory benefit in an investigation." (4.2.3)

1. The Executive submitted that it had requested information from the Level 2 provider, which had not been supplied and was likely to have a regulatory benefit to the investigation. The Executive therefore asserted that paragraph 4.2.5 of Code 13 and paragraph 4.2.3 of Code 14 had been breached.

   The Executive noted that, due to concerns over potential irregularities with logs provided by the Level 2 provider, in a direction dated 16 February 2016, the Executive asked the Level 2 provider to provide its reasons for the high failure rate of chargeable service messages. The Level 2 provider explained that this was due to "an error in

technical database resulting from server settings that were by default too restrictive blacklisting Level 1 IP addresses." The Level 2 provider stated that in order to rectify this issue "the automated script CRONTAB was run to enable successful connect between Syncronized and Level 1 systems".

On the 2 March 2016, the Executive requested several pieces of information from the Level 2 provider. On 11 March 2016 the Level 2 provider provided a response in relation to the questions regarding CRONTAB, which is attached at **Appendix B.**

Based on the directions issued by the Executive and the responses that were received from the Level 2 provider, the Executive submitted that the following information was not provided:

- The exact date upon which CRONTAB was implemented
- The date on which the Level 2 provider detected the 'error in technical database'
- Documentary evidence relating to the identification or correction of the technical fault by the Level 2 provider
- Any evidence from the Level 2 provider's technical team in relation to the technical fault
- Evidence of the service message it stated had been sent to subscribers once the problem had been detected
- Evidence of the explanation it had provided to consumers once the technical error had been detected

The Level 2 provider had asserted that once CRONTAB was implemented, it was then able to run a 'successful connecting between Syncronized and Level 1 systems.' The Executive asserted that without the key information above, it was unable to establish the exact dates on which message failures began and were rectified. Therefore the Executive was unable to understand any of the solutions put forward by the Level 2 provider. The Executive noted that, despite the Level 2 provider's assurances that "most importantly we managed to overcome it and implement a solution to remedy the issue" in logs provided by the provider in response to requests made by the Executive as recently as 15 November 2016, a similar pattern of failed messages was still seen to be occurring.

Further to this, on 2 April 2016 the Executive asked for documentary evidence to show its network settings before and after the error was identified.

On 13 April, the Level 2 provider responded with "internal server network settings" for before and after the error was identified, as set out at **Appendix C.**

The Executive noted that the files provided were neither dated nor verified in any way. Further research conducted by the Executive revealed that this was one of many files or logs which could have been provided to demonstrate network settings.

The Executive noted that this was the first time the Level 2 provider mentioned Fail2ban. Once it had been established that Fail2ban was the purported cause of the technical error in the Level 2 provider database, the Executive carried out independent research to understand the mechanics of the software Fail2ban where it instructed the services of an independent developer (the "Developer"). The Developer concluded that without key pieces of information regarding Fail2ban (as outlined in the questions put to the Level 2 provider in **Appendix B**), he was unable to provide a conclusive response as to the plausibility of messages failing due to the Fail2ban software.

Based on the correspondence with the Developer, the Executive asked a series of questions to the Level 2 provider. The questions asked by the Executive and the responses given by the Level 2 provider on 5 May 2016 are attached at **Appendix B.**

The Executive asserted that the following information was not provided:

- A definitive answer as to whether Fail2ban was responsible for the failure of ALL messages between the Level 1 provider and the Level 2 provider, prior to the initial billing as shown in the message logs for complainants
- Details of the configurations of Fail2Ban
- The date range for each configuration of the Fail2Ban log
- Monitored Fail2ban log files or any Fail2Ban log files
- Confirmation as to whether Fail2Ban had been downloaded separately or as a standalone installation
- Confirmation as to which firewall solution had been running underneath Fail2ban

The Executive noted that it had asked the Level 2 provider on three separate occasions to provide the following information: 'Please confirm who Syncronized Ltd used as their hosting provider at the time the fail2ban error occurred.' The Level 2 provider failed to provide a response to this question. The Executive understood that should this information have been available, it would have potentially been able to correspond with the hosting provider in relation to this.

In response to questioning from the Tribunal regarding whether or not the Fail2ban log file could be unavailable, the Executive stated that it understood from the Developer that the log file, and the system configurations, could be over-written. However the Executive noted that it had not been provided with the latest log file in any event.

In response to questioning from the Tribunal, the Executive stated that it understood that there was no need to pay or sign up for Fail2Ban as it was free open source software.

In response to questioning from the Tribunal, the Executive stated that its understanding was that a provider would usually need to contract with and pay for a hosting provider, and would expect a provider to hold some correspondence with its hosting provider.

The Executive, in response to questioning from the Tribunal, clarified that its understanding was that other files such as the Fail2Ban log could also have been provided to it.

The Executive had sent directions to the Level 2 provider on 27 April 2016, 16 June 2016, 27 July 2016, 6 September 2016 and 29 September 2016. The Executive submitted that at each stage the Level 2 provider failed to provide sufficient information to allow further analysis of its claims regarding the high failure rate and therefore substantiate their explanation that it was caused by a technical error. The Executive submitted that this failure resulted in the Executive being unable to evaluate as to whether Fail2Ban may have been the cause of the constant failure of messages to particular MSISDNs. The Executive regarded the actions of the Level 2 provider as causing a regulatory detriment to the investigation carried out in that the Executive was unable to conduct further enquiries in relation to these matters. Due to the inconsistencies of the Level 2 provider's responses and the lack of evidence provided, the Executive submitted that the assertions made around Fail2Ban could not be substantiated. It is for the reasons above that the Executive asserted the Level 2 provider was in breach of paragraph 4.2.5 of Code 13 and paragraph 4.2.3 of Code 14.

2. The Level 2 provider denied the alleged breach. The Level 2 provider stated that it could not have provided more exhaustive or detailed answers to the extensive and at times repeated questions that came from the Executive (e.g. the Crontab System Report including explanatory notes, images, graphs, diagrams). Moreover it supplied a technical (even historic) background as an additional aid designed to help the Executive get a full picture of issues and solutions.

   The Level 2 provider stated that it had supported its statements on remedial actions undertaken with evidence (e.g. delivery receipts and screenshots from Level 1 provider interfaces), which could not be more accurate.

   The Level 2 provider submitted that the allegation that information was not provided to the Executive was not legitimate, as the Executive had made a subjective list whereas the details involved had been supplied to the Executive, even if under different labels.

   The Level 2 provider submitted that the allegation of breach seemed to be an outcome of insufficient understanding / misinterpretation of evidence provided by the Level 2 provider to the Executive. The Level 2 provider submitted that, for instance, even details on IPs from log files were coherent with the Level 1 providers' information.

In oral representations, the Level 2 provider submitted that the questions from the Executive were elaborate and detailed and it had tried to answer them all in full. The Executive had included questions about affiliate marketing which were irrelevant as they did not use this.

The Level 2 provider submitted that it had in fact provided too much information as some of it could infringe their company's confidentiality, but it had thought this was the right thing to do.

The Level 2 provider submitted that it first made a proposal to deal with this matter informally in February 2016. The Level 2 provider submitted that it would have saved time if the Executive had accepted this offer, but it had been rejected based on a claim that the Level 2 provider hadn't answered all questions. The Level 2 provider submitted that the Executive's positon was based on a lack of knowledge of how advertising agencies and marketing worked, despite its efforts to explain. To its disappointment, its explanation as to why it was not able to release details of the websites were not verified, despite the fact that it would have been straightforward to verify that this was not the way blind networks worked with any advertising network. The Level 2 provider submitted that this had been detrimental to it.

The Level 2 provider referred to the reply rejecting this offer and seeking more answers from the Level 2 provider. The Level 2 provider stated that it had attempted to provide more details, and it had pushed for its marketing team to provide examples of places where its adverts were found. The Level 2 provider stated that it had also provided an exhaustive example of the processes worked, using two example advertising agencies. It had provided proof that its promotional materials were approved by the PSA and Advertising Standards Authority. It had explained it did not use affiliate marketing for promotions. It had elaborated on the technical issues- it had explained that it had problems with an incompatible API certification and how it had overcome this issue. It had provided proof from the Level 1 provider portal to show a message and delivery receipt. The Level 2 provider queried whether this information had been verified or checked with the Level 1 provider, and queried what other information was required for it to prove the validity of messages.

The Level 2 provider stated that it had provided proof of refunds issued to consumers. The Level 2 provider believed this information had been ignored when the interim warning notice was determined. The Level 2 provider noted that the consultation issued by PSA in November 2015 at section 2.2.8, had stated that "providers will be able to challenge the decision to withhold… for provider's representations to carry any weight, they should provide evidence of any refunds given to date." The Level 2 provider was asked if it had exercised its right to have a review of the withhold imposed, and it confirmed it had not. It had taken the view that its evidence submitted in response to the interim warning notice had not been taken into account, and so had found it difficult to proceed further.

The Level 2 provider referred to the records it had enclosed of use of its MSISDN lookup tool, showing an example of specific subscribers and their experience, providing proof from the Level 1 provider that messages were delivered to these consumers. Again, the Level 2 provider queried if this had been verified with the Level 1 provider. The Level 2 provider submitted that their evidence hadn't been taken into account because it didn't fit with the Executive's case.

The Level 2 provider submitted that on 6 April 2016 it had replied to another letter, providing code as had been requested plus some information in layman's terms. On 24 April 2016, the Level 2 provider had offered a settlement, which included ending subscriptions for the users required by PSA, a compliance audit to prove it was adhering to the opt-in procedure, and a charity donation. The Level 2 provider stated that unfortunately this proposal had been rejected. The Level 2 provider had then received repeated requests for information, which prolonged the case, though it had tried to answer the questions. The Level 2 provider submitted that this was a challenge and noted that their IT team found the questions irrelevant at most times. The Level 2 provider submitted that the specific file location referred to by the Executive was not in existence or correct, and that the further questions regarding the hosting provider were irrelevant. The Level 2 provider stated that it didn't see how answering this question would have any importance to the case, and the aim of this was unknown to it. The Level 2 provider submitted that despite having answered questions, often with confidential information, the questions were now duplicating each other.

The Level 2 provider referred to the question about "who initiated messages" and stated that having a basic knowledge of how this worked, it was highly difficult to understand why such a question would be placed in an official letter.

The Level 2 provider referred to the correspondence with the Developer and noted that their analysis did not contradict the Level 2 provider's position, and in fact it confirmed that there were an entire set of scenarios which could affect message delivery. It also confirmed that if this one software issue was causing failures, and affected only a minor number of subscribers, it could have gone unnoticed for a long time. The Level 2 provider noted that the Executive hadn't submitted that the technical scenarios it had referred to were impossible – the Developer had stated that the scenario could have happened, due to the nature and flexibility of the settings of Fail2ban.

The Level 2 provider submitted that it was a matter of common sense that there was no factual grounds on which to say it had provided inappropriate information to the regulator.

The Level 2 provider noted that in July 2016 it had pro-actively contacted the Executive with an update on its remedy plan, including its new sufficient system for subscriber management. Following industry discussions, this had been designed to correct consumer awareness. The second part of the plan was technical, including a complete server move. Unfortunately, after this the Executive had still issued an interim warning notice. In response to the interim warning notice it had listed 14 points which, in light of

the Code, meant the interim warning notice had procedural errors and was in breach of the Code. The Level 2 provider queried why the legal issues it had raised at the interim stage in response to the interim warning notice had not been added to the final case annexes submitted to the Tribunal. The Level 2 provider was asked whether it had submitted these issues in response to the Warning Notice, and it acknowledged that it had not done so.

The Level 2 provider had issued the Executive with a planned progress update, but this was ignored and the Level 2 provider received a Warning Notice in December 2016, which had suggested a higher fine than the amount withheld, as if all its attempts to satisfy the Executive had gone unnoticed.

The Level 2 provider submitted that the burden of proof for the breach of paragraph 4.2.3/4.2.5 was not passed.

In response to questioning from the Tribunal about why it had not provided details of its hosting provider, the Level 2 provider stated that at the time it was asked, it did not find that question, and certain others, relevant. The Level 2 provider did not think it had said that it could not provide this information without its IT team, although it noted that the lack of current income due to the withhold had forced it to let its major development team go. The Level 2 provider said it regarded its hosting provider as its server provider, which had nothing in common with the technical issue it had experienced as it was software-based. Although the Executive had come back to it on this question four times the Level 2 provider still believed it had fully cooperated, as it had never gotten an explanation of why this information was valid to the case.

In response to questioning from the Tribunal about whether it had referred its serious allegation that the Executive had sought to prolong the investigation in order to increase the fine imposed, the Level 2 provider stated that it got this impression after so many months of exchanging information and cooperating, but then still received interim and final warning notices. The Level 2 provider confirmed that it had not made any complaints outside the PSA and would rather keep it confidential; whether it later pursued this allegation would depend on the outcome of this hearing, and whether the Tribunal took into account all its evidence, and the outcome was not prejudicial and was fair.

3. The Tribunal considered the Code and all the evidence before it.

The Tribunal noted that the Level 2 provider had failed to provide the following information when requested:

- The exact date upon which CRONTAB was implemented
- The date on which the Level 2 provider detected the 'error in technical database'

- Documentary evidence relating to the identification or correction of the technical fault by the Level 2 provider
- Any evidence from the Level 2 provider's technical team in relation to the technical fault
- Evidence of the service message it stated had been sent to subscribers once the problem had been detected
- Evidence of the explanation it had provided to consumers once the technical error had been detected
- A definitive answer as to whether Fail2ban was responsible for the failure of ALL messages between the Level 1 provider and the Level 2 provider, prior to the initial billing as shown in the message logs for complainants
- Details of the configurations of Fail2Ban
- The date range for each configuration of the Fail2Ban log
- Monitored Fail2ban log files or any Fail2Ban log files
- Confirmation as to whether Fail2Ban had been downloaded separately or as a standalone installation
- Confirmation as to which firewall solution had been running underneath Fail2ban

The Tribunal noted the Level 2 provider's submissions that some of the questions were not intelligible, such as the question as to whether the Level 1 or Level 2 provider initiated the messaging protocol. However, the Tribunal considered that the requests for the above information were adequately clear.

The Tribunal noted that the Level 2 provider had submitted that the Level 2 provider had taken the view that certain questions were not relevant to the investigation. The Tribunal commented that it was not for providers to make this determination, and select which questions they were willing to answer. The Level 2 provider had provided further information as set out in its above submissions, including information which had not been specifically requested, but this did not relieve it of its obligations to comply with a direction requiring the provision of specific information.

The Tribunal considered it was possible that some of the older logs and configurations requested may have been overwritten. However this did not relieve the Level 2 provider of its responsibility to provide what information it could.

The Tribunal considered the Executive's case on why the information would have been of regulatory benefit to the investigation. The Tribunal noted the Level 2 provider's submission that the Developer had stated that it was possible that Fail2ban had caused the pattern of message failures seen. However, the Tribunal considered it was clear that the Developer's view was that this was a theoretical possibility only, and that they were

not able to provide a definitive view on whether Fail2ban had in fact caused the failures without further information, which the Executive had requested from the Level 2 provider but the Level 2 provider had not supplied. In relation to the identity of the hosting provider, the Tribunal considered this information could have assisted the Executive to correspond with the provider regarding whether the Fail2ban errors had occurred as described. The Tribunal considered that the Level 2 provider had failed to provide sufficient information to allow further analysis of its claims regarding the high failure rate, and therefore substantiate their explanation that this was caused by this technical error.

The Tribunal was satisfied that, having been formally directed to do so by the Executive, the Level 2 provider had failed to provide information which was reasonably likely to have had a regulatory benefit in an investigation. Accordingly, the Tribunal upheld a breach of paragraph 4.2.5 of the 13th Code and paragraph 4.2.3 of the 14th Code.

Decision: UPHELD

Alleged Breach 3

Paragraph 3.1.7. - "All…Level 2 providers must…use all reasonable endeavours in the context of their roles to ensure that all of the premium rate services with which they are involved are of adequate technical quality, including the mechanisms used to deliver services to and enable exit from services by consumers."

1. The Executive asserted that the Level 2 provider had breached paragraph 3.1.7 of the Code as it did not take all reasonable endeavours to ensure that the Service was of an adequate technical quality based on its logs showing the widespread and consistent message transmission failures.

   The Executive relied on correspondence exchanged with the Level 2 provider, text message logs and the PSA guidance.

   Code 13 and 14 Guidance states:

   "9. Technical Quality

   9.1 All providers of services offered via a mobile-based payment mechanic should ensure their services are compatible with each technical network platform and/ or handset on which they are promoted. Where this is not possible, consumers with incompatible devices should be prevented from purchasing the service in question."

   Due to concerns over potential irregularities with logs provided by the Level 2 provider, in a direction dated 16 February 2016, the Executive asked the Level 2 provider to provide its reasons for a high failure rate of chargeable service messages. The Level 2 provider explained that this was due to "an error in technical database resulting from server settings that were by default too restrictive blacklisting Level 1 IP addresses."

The Executive noted that the Level 2 provider had stated that it has taken measures such as the implementation of CRONTAB as detailed above, as well as sending separate documents to the Executive outlining measures it had taken to solve problems it had encountered in the past. However the Executive noted that the Level 2 provider is required to "use all reasonable endeavours in the context of their roles to ensure that all of the premium rate services with which they are involved are of adequate technical quality, including the mechanisms used to deliver services to and enable exit from services by consumers."

The Executive noted that on review of the most recent message logs supplied by the Level 2 provider, the message failures shown continued up until mid-2016, showing that the measures taken by the Level 2 provider to rectify the problem had not been successful. The Executive submitted that the Level 2 provider could have taken further steps including better technical measures, and unsubscribing all affected consumers to the Service and then re-subscribing them to the Service using a robustly verifiable opt-in method.

The Executive referred to an example message log showing the extended period of time over which the purported message failures occurred. The Executive noted that the message log listed the message failures continuing from 19 October 2014 to 17 July 2016. The Executive relied on previous correspondence from the Level 2 provider stating that messages listed as 'SENT' and 'ACCEPTED' and 'FAILED' had not received a positive message delivery receipt / response had not been received from its aggregator, meaning that the messages had not been received by consumers. The Executive noted that if messages were consistently failing, consumers were deprived of the ability to opt out of the service and faced the risk of distress as a result of the length of time between their first chargeable message and alleged opt-in.

The Executive relied on further examples of message logs supplied by the Level 2 provider which contained failed chargeable Service messages for an extended period of time.

The Tribunal asked the Executive whether it understood the Level 2 provider's evidence of the MSISDN lookup tool's use as meaning that they had pro-actively contacted consumers to ask if they wanted continue their subscriptions. The Executive stated that, having checked the evidence against the logs, it wasn't clear how consumers would have understood this was what was happening. The Executive's understanding was that the messages' content was simply a unique URL, which led to the Level 2 provider's log-in page if it was clicked. However the Executive's view was that consumers may very well not have clicked on such a link if it was sent to them by text.

The Executive submitted that the Level 2 provider had an obligation to ensure that the Service worked correctly in order for it to operate fairly and according to the Service terms and conditions and the requirement of the Phone-paid Services Authority. In light of the reasons set out above, the Executive submitted that the Level 2 provider had acted in breach of paragraph 3.1.7 of the Code.

2. The Level 2 provider denied the alleged breach. The Level 2 provider submitted that it had taken steps to minimise the impact of message transmission irregularities. These were extensive long term technical development projects, followed by the ultimate measure of last resort i.e. migration of the server to a new provider. The Level 2 provider submitted that technical issues had been limited to zero after all these undertakings, and the process was assisted by additional procedures focused on consumer protection and support.

   In oral representations, the Level 2 provider submitted that this breach was added to increase the monetary fine the Executive could impose – it was highly difficult to claim that the Level 2 provider did not have technical facilities of sufficient quality.

   In response to questioning from the Tribunal, the Level 2 provider explained that it had a standard system in place that would notify it if a specific irregularity was in place. The volume of message failures were not outside the standard value it noted each month. The Level 2 provider said it was possible that the specific problem went unnoticed. The Level 2 provider said there was no alarming rate of failures.

   The Tribunal noted that in November 2016 the Level 2 provider had stated it had found 7000 consumers who had received only "failed/sent" messages, and queried whether this would be considered a high failure rate. The Level 2 provider stated that this was not, when compared to the total amount of subscribers and messages sent. The Level 2 provider did not have the total number of failed messages to these 7000 subscribers available at the date of the hearing. The Level 2 provider stated that it had implemented remedies to re-verify subscriptions for users and provided a sample to the Executive. The Tribunal queried if the Level 2 provider had supplied an update on this to the Executive in December as promised. The Level 2 provider had not, but it confirmed that it had now stopped all subscriptions and traffic until the Tribunal decision.

   In response to questioning from the Tribunal about MSISDN *******8216 (which had received over a year of failed messages before being successfully billed when the shortcode changed in July 2016) the Level 2 provider was not able to confirm whether the consumer had received a message confirming there had been a migration, with details of the pricing and how to opt-out. The Level 2 provider then provided a log showing "freemsgs" sent to the consumer.

3. The Tribunal considered the Code and all the evidence before it, including the consumer complaints.

The Tribunal noted that the Developer had stated that the issue with Fail2ban could go undetected; however in this case the Level 2 provider had been put on notice of the issue at an early stage, including by being passed complaints from the Executive. The Tribunal noted the Level 2 provider's submission that the volume of message failures was not unusual for a premium rate service. The Tribunal considered that, whilst this may be true, the Level 2 provider's logs showed that all messages to certain consumers were failing, rather than message failures being dispersed randomly amongst its consumer base. In light of this, the provider was under an obligation to pro-actively investigate and take all reasonable endeavours to ensure that the issues were resolved promptly.

The Tribunal considered the evidence of endeavours the Level 2 provider had taken to rectify the issue. The Tribunal noted that the logs indicated these measures had not been successful in resolving the issues. The Tribunal noted that the Level 2 provider had identified steps it could take to mitigate the harm in April 2016 but had not implemented these until after September 2016 (by which point interim measures had been imposed in respect of the investigation). The Tribunal considered that, in light of the Track 1 action plan, these were in fact measures it should have considered implementing in January 2015. The Tribunal did not consider that the measures taken by the Level 2 provider represented all reasonable endeavours in the context of their role.

The Tribunal considered whether the breach represented duplication of the harm which was addressed by the breach of rule 2.3.3. which had been upheld. The Tribunal considered that if messages were consistently failing, consumers were deprived of a proper opportunity to opt out of the Service, and also faced the risk of distress as a result of the length of time between their first chargeable message and apparent opt in. The Tribunal noted that there was no obvious given warning to consumers when the Service was migrated to a new shortcode and successful billing commenced for the first time. The Tribunal noted that the delay between the opt-in date shown on the logs and the first successful billing was in some cases over a year.

Decision: UPHELD

SANCTIONS

Representations on sanctions made by the Executive

The Executive submitted that if breaches were upheld, the following sanctions were appropriate:

- a requirement that the Level 2 provider remedy the breach by ensuring that (a) 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 and (b) it takes all reasonable steps to show message failures are rectified promptly
- a formal reprimand
- a fine of £650,000
- a bar to access to all number ranges associated with the Services which it currently operates and any subscription Service until it has sought and implemented (a) compliance advice on consent to charge and (b) remedied the apparent breaches; 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 the PSA that such refunds have been made.

The Level 2 provider submitted that, if breaches were upheld:

- The recommended sanctions of remedy the breach, a formal reprimand, a bar, and general refunds were appropriate;

- The Level 2 provider noted that it had wished to avoid further prolonged investigation and to avoid such delay, it offered a settlement on 26 April 2016 stating it was willing to terminate any subscription that was not satisfactory to Executive in the scope of robustness and was affected by irregularities in message transmission. It was also suggested that the Level 2 provider was willing to be a subject of an external audit to confirm that it utilises robust third party verification system (i.e. no breaches to the Code occur). It also confirmed that the refund process continued and made a charity donation offer with sincere willingness to fulfil such offer. Unfortunately, the Level 2 provider noted that the offer was rejected and the case proceedings continued for nine months more. The Level 2 provider submitted that, had the settlement been agreed, the case could have been successfully closed in April / May 2016. The Level 2 provider stated that it was under the impression that the prolonged investigation was aimed at allowing the Level 2 provider to continue service charges for a further nine months to collect more money through a very high inadequate monetary fine which was aimed at eliminating the Level 2 provider from the market (and business in general), and submitted that this was not acceptable and was by all means unfair. The Level 2 provider therefore disputed the imposition of a fine.

Initial overall assessment

The Tribunal's initial assessment of the breaches 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 breach had a clear and highly detrimental impact directly on consumers
- The nature of the breaches, and the scale of harm caused to consumers was likely to severely damage consumer confidence in premium rate services; and
- Consumers had incurred an unnecessary cost.

Paragraph 4.2.3/4.2.5 – Failure to provide information

The initial assessment of paragraph 4.2.3/4.2.5 of the Code was **very serious.** In determining the initial assessment for this breach of the Code the Tribunal applied the following criteria:

- The provider had deliberately and without good reasons provided a limited response to directions to provide information;
- The nature of the breaches was likely to severely damage consumer confidence in premium rate services; and
- The breach demonstrated fundamental non-compliance with the Code

Paragraph 3.1.7 – Inadequate technical quality

The initial assessment of paragraph 3.1.7. of the Code was **serious.** In determining the initial assessment for this breach of the Code the Tribunal applied the following criteria:

- The breach had a clear and damaging detrimental impact or potential impact on consumers;
- The nature of breach meant the Service would have damaged consumer confidence in premium rate services;
- The cost incurred by consumers may have been higher, and the Service had the potential to generate higher revenues, as a result of the breach; and
- Noting the length of message failures extended over a year in some cases, the Service had been operated in such a way that demonstrated a degree of recklessness regarding non-compliance with the Code.

Final overall assessment

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

- The Level 2 provider had been subject to two previous Track 2 procedures in January 2013 and November 2014, each of which contained findings regarding consent to charge breaches. The Level 2 provider had also been subject to a Track 1 procedure since those adjudications. The last Track 2 procedure contained a warning that "if the Level 2 provider fails to demonstrate that it has robust verifiable evidence of consumers' consent to charge in the future, it should expect to receive a significant penalty." The

Tribunal attached particular weight to this aggravating factor, and commented that the Level 2 provider appeared to have treated past fines as a cost of doing business.

- The Level 2 provider had caused unnecessary delay to the progression of the investigation by its approach to responding to 4.2.1 directions, including several requests for extensions in relation to seven out of ten 4.2.1 directions, whilst continuing to operate the Service without taking adequate remedial action in this period.

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

- The Level 2 provider had made a partial admission of the breach of Code rule 2.3.3.
- There was some evidence that the Level 2 provider had made some pro-active refunds to affected consumers.

The Tribunal noted the Level 2 provider's submission that it had taken steps to remedy the breaches; however the Tribunal noted that such steps were pursuant to its obligations under paragraph 3.1.7 which it had not fulfilled. The fact that some steps had been taken were reflected in the Tribunal's assessment of the seriousness of that breach.

The Tribunal had noted that the Level 2 provider's allegations that the Executive had acted so as to prolong the breach and had done so in order to maximise any potential fine (as a result of higher service revenue having been accrued). Having reviewed the correspondence, the Tribunal was of the view that, if the investigation had been prolonged, this was as a result of the Level 2 provider's actions in failing to provide requested information and in consistently requesting time extensions for each such request. The Executive had not indicated that the Level 2 provider should continue to generate revenue by operating the Service as it was – this was a choice made by the Level 2 provider. Regarding the "settlement proposal" made in April 2016, the Tribunal commented that:

- The Level 2 provider was obliged to pro-actively take any action it had identified as necessary to comply with the Code's required outcomes. It was not appropriate for a provider to offer to take such action only if the Executive agreed to end its investigation;
- The Executive could not be expected to end any investigation through a settlement where it reasonably believed that the Level 2 provider had failed to fully cooperate with its requests for information; and
- In any event, the Executive did not have the power at the time to settle cases in this way save via the Track 1 procedure, which the Tribunal considered would have been manifestly inappropriate given the facts of the case and the provider's compliance history.

The Level 2 provider's evidenced revenue in relation to the Service in the period from March 2015 to October 2016 was in the range of Band 1 (£1,000,000 +).

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

Having regard to all the circumstances of the case, including the high service revenue generated and compliance history of the provider, and having found that the Level 2 provider had been knowingly involved in a series of breaches and/or a serious breach of the Code, the Tribunal decided to impose the following sanctions:

- a formal reprimand;
- a fine of £600,000 (being £250,000 in respect of the breach of rule 2.3.3, £250,000 in respect of the breach of paragraph 4.2.3/4.25, and £100,000 in respect of the breach of paragraph 3.1.7);
- a prohibition on the Level 2 provider from providing, or having any involvement in, any premium rate service for a period of three years from the date of publication of this decision, or until compliance with sanctions, whichever was later;
- a requirement that the Level 2 provider seeks prior permission for the operation of any premium rate service for a period of 24 months after the expiry of the prohibition; and
- a requirement that the Level 2 provider must refund all complainants who claim a refund, within 28 days, for the full amount spent by them on the Service, save where there is good cause to believe that such claims are not valid, and provide evidence to Phone-paid Services Authority that such refunds have been made.

In imposing a fine of £100,000 in respect of breach of paragraph 3.1.7, the Tribunal took into account that a degree of harm addressed by that breach was also addressed by the breach of rule 2.3.3.

Administrative charge recommendation: 100%

The decision of a previous Tribunal on 4 August 2016 to impose interim measures is attached at Appendix D.

Appendix A

Syncronized service – consumer journey:

1. Below advert is fully acceptable under the Code of Practise and has been accepted by ASA Copy Advice Service

    a) It contains clear basis of charging

    b) It presents age restriction

    c) It presents Helpline

    d) It presents method of exit

    e) It presents Service Provider name

http://lesbiancourse.com/advertising1/

2. Landing page No 1

a) Clicking on above banner takes user to a landing page with MSISDN enter form

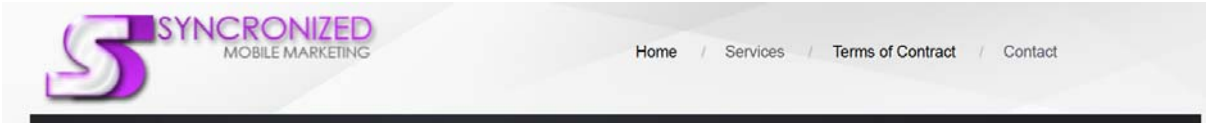
b) Landing page is hosted by external party – ETX

c) Pricing on the page is prominent and placed prior to MSISDN call 2 action form. We even inform users that service costs excludes regular network carrier charges for internet connection and this pro-active guidance has been qualified by independent compliance advisors as a 'forerunner', setting new standards in transparency of service Terms and Conditions.

d) Pricing is also stand alone as has been embodied into Submit Button

e) Landing page includes 14 day cancellation disclaimer and in addition, an information for user that Terms of Contract are available on Service Provider website. These 2 parts of Terms have been introduced after consultations with Level 1 Providers and external legal advisors (Monitoring Compliance Partners) especially with respect to MCP Regulatory Update – Complaint Handling; CCR issued on 14th October 2015. This document sets out guidance and clarifies rules of distance selling and their applicability for premium SMS subscriptions, with attention to the following essential points:

- Provide the contract in a durable form



Terms of Contract

Our Subscription services cost £4.50 per week until you send STOP to 84506 (excluding your network operators standard network charges). You can cancel subscription within 14 days at no charge.

Images are compatible with colour wap enabled phones and mobile browsers Android and iOS.

You must have the bill payers permission. To stop text stop to 84506. We reserve the right to contact individuals with occasional promotional material of similar nature that we may think you would have an interest in. You can stop promotional material by texting NO INFO to 84506. Service Provided by Syncronized Ltd. Helpline: 02476998420 or text stop at any time to cancel this service.

You can also email us at marta@syncronized.co.uk in case you have any question regarding services and their operation.

- Provide a 14 day refund facility unless the Consumer has purchased digital content that is delivered immediately and has been advised (and they consented) that the contract cancellation period does not apply.

f) Helpline is clear and prominent and has been a subject to continuous monitoring carried out by both Level 1 Providers, in addition it passed the examination of outside review

g) Page content meets all requirements of telecommunications laws

3. Landing page No 2

a) Once MSISDN is entered into form and verified, a Pin is sent to users' handset

b) User is redirected into next page with PIN form

c) PIN message: *Free Msg: Here is your PIN for subscription service: [pin]. Enter it now. Enjoy! Ignore if sent in error.*

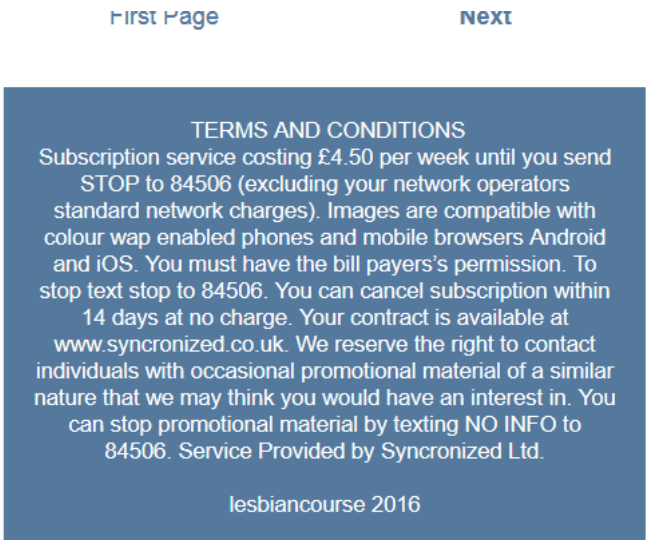
4. Subscription confirmation message

a) Once PIN send back by User via website form is verified, subscription have a green light to commence

b) Standard subscription confirmation message: *FreeMsg: U have subscribed to Lesbian Course, £4.50 per week until you send STOP to 84506. Help? 02476998420. SP Syncronized*

5. Content access and weekly billing

a) Terms and Conditions on Content page:



b) Videos are accessible to user via above service website and via weekly premium SMS message

c) Standard premium message: *#WAP_LINK# Help? 02476998420 or marta@syncronized.co.uk Send STOP* to 84506 to exit (#WAP_LINK# is a uniquely customised URL that is transformed into accessible service site URL for each subscriber, i.e. User would receive actual hyperlink via SMS message)

6. Monthly reminder message

a) Every calendar month, subscribers receive a reminder message at no cost to make sure they are aware of ongoing subscription and are reminded of opt out method should there be such desire from their end

b) Standard reminder message: *FreeMsg: Reminder: You are subscribed to Lesbian Course for £4.50 per week until you send STOP to 84506. Help? 02476998420 or marta@syncronized.co.uk*

7. Opt out methods:

a) SMS STOP to short code 84506

b) Opt out request logged with Support Team via:

- Telephone 02476998420
- Email marta@syncronized.co.uk
- Website opt out form

Contact Syncronized

*Your Name

*Your Email

*Tel Number

*Mobile Number

*Your Message

Additional Information

Send Message

- **Post**

Contact Details

SYNCRONIZED LTD
THE MERIDIAN 4 COPTHALL HOUSE
STATION SQUARE
COVENTRY
ENGLAND
CV1 2FL

Appendix B

Provider response dated 11 March 2016

i. Please specify the exact date on which CRONTAB was implemented.

SYNCRONIZED:

Implementation of CRONTAB monitoring has been a long term complex process initiated back in 4th quarter of year 2014 and has been gradually applied and activated throughout Level 2 databases to eliminate connectivity and transmission interferences.

ii. You have stated 'we identified a reason as an error in technical database resulting from server settings that were by default too restrictive blacklisting Level 1 IP addresses.' Please confirm the date on which this error was identified, and provide copies of any correspondence relating to this discovery.

SYNCRONIZED:

This error has been identified internally and the process of reaching conclusion was complex since it involved technical interferences of various reasons:

- We were aware and by experience we expected that certain percentage of messages are always likely to fail. We have been running premium services for several years and never on single accountable month would we note a 100 percent of messages delivered to users handsets. A leeway for failed delivery (resulting in profit lower than expected) has been applied to all our budget, cash flow and profit estimate reports. Therefore to actually evaluate that the profit is lower than expected, it must have been analysed throughout months. Should a premium profit was zero for particular month (or even single week) we would have been instantly alarmed by statistics. However when it was only a small percentage of messages that were failing due to specified technical reasons and majority of traffic was performing in positive way, and when consumers were satisfied, for these all reasons it was not a particular day that a problem was discovered. It was a result of various factors and most importantly we managed to overcome it and implement a solution to remedy the issue.

- Additionally, certain amount of service messages were logged with unsuccessful status however it was only once we updated our server to be capable of recording combined delivery statuses received from each Level 1 providers API. As we specified in section 6 below, each Level 1 provider had their own API specifications and they contradicted each other.

iii. You have also stated that 'as soon as the discrepancies in communication between Syncronized and Level 1 provider were discovered, the subscriber would receive a free of charge message with service details so that users have an option to opt out and review the service they subscribed to' Please provide evidence to show this message was sent to consumers.

SYNCRONIZED:

Please see sample mobile number that received such message and supporting evidence provided by Level 1 provider. This clearly proves that we have made all efforts to made user aware of the subscription and to provide a review of terms and conditions and to provide them with opt out option should they decide so. This consumer indeed decided to opt out from the service and contacted PhonepayPlus to request a stop. This request was forwarded to us on 23 June 2015, was followed up by our Support Team and in addition to explain server aspects, we offered a good gesture refund which was accepted with satisfaction and refund was sent to user by PayPal (transaction ID is available upon request) on 26 June 2015. This example confirms our best efforts to remedy any potential consumer harm and most of all, successful efforts because we provided high standard of Customer Support to all affected consumers and refunds were issued to apologise for inconvenience caused.

*******5425

Response dated 5 May 2016

1. Please clarify whether it is Syncronized Ltd's position that fail2ban was responsible for the failure of ALL messages between the Level 1 provider and Syncronized Ltd prior to the initial billing, as shown in the message logs for the complainants?

Yes, users in question were affected by this technical occurrence.

2. Please also answer the following questions:

a. Please provide full copies of all the fail2ban configuration(s) which was set both before and after you identified the issues with messages not being received by the Level 1 provider(s), which includes every configuration which affected any IP address.

As has been explained in our previous correspondence, it is not possible to retrieve such data since this software records only most recently saved configuration, i.e. it overwrites the settings. Please note we have put strongest efforts to provide exhausting answers engaging our Technical Team. As far as the nature of the issue is concerned it was not required to make a copy or record of historic credentials simply because the changes and updated were implemented as they were found to be necessary. I am not sure how to explain it better other than this way, the measures were applied where appropriate to serve the purpose and solve any arising problem/ blockage to solve the issue.

b. Please identify for each configuration the date range for which the configuration was in force, and which server connections each configuration related to.

As per above, the software and system would not record specific time ranges because it would simply over-write the script to fit the purpose to enable reinstating of message transmission.

When Fail2Ban blocks an IP address, the ban is typically applied for 600 seconds (10 minutes). There may be many instances where addresses have been banned and removed before our technical team could react and manually un-ban or whitelist these addresses.

This is a dynamic system and in most cases it can be relied upon to manage the blocking of suspicious IP addresses automatically.

We wish to emphasize the fact that misconfigurations caused intermittent transmission issues and it is not a common practise to store server logs for banned IP addresses or misconfigurations because such records occupy server space. Furthermore it is necessary to understand that keeping incorrect problematic data in the system is reckless as it may interfere with correct records. To sum up, since the software works intuitively and adjusts settings for connections in the background, once a setting is overwritten, it is not a practise to record the earlier configuration, let alone it would be impossible and not reasonable from database maintenance point of view.

c. Additionally, please supply the entire /etc/fail2ban configuration(s) and excerpts from the corresponding monitored log files which were picked up by fail2ban as well as the entire fail2ban.log file(s) showing the IP addresses which were banned at any given period by the fail2ban application.

According to information outlined above, these details were not stored, nevertheless as a result of very in depth search throughout handwrite/ draft notes we managed to find few examples of IP addresses:

54.78.19.37

54.247.27.69

Response to request on 16 June 2016

1. With regard to your response to our request to supply the fail2ban.log file for your system, you should inform your technical representative(s) that it can be located and exported from the following location: /var/bin/fail2ban.log

This file is created by default in this location by the system in order for users to identify suspicious activity and decide appropriate action. The Executive can think of no good reason why the creation of this file should have been disabled or moved.

Please therefore supply this log. If you are unable to do so please specify the reason as to why.

Reply: I consulted the above questions and it appears that the location provided does not exist and it ought to be /var/log/fail2ban.log instead. I am not certain why such discrepancy occurred.

Our server uses a standard tool called logrotate - this means every week the log files are compressed and a new one is created. Our logrotate keeps 4 backups, so we only have logs for the previous month. This means that the fail2ban.log file will contain no information relevant to the investigation.

Please note fail2ban logs are only generated for internal use to help with regular maintenance and security of the server. Despite my willing to assist with your investigation it is impossible to provide the file.

Response to request on 19 September 2016

1. Please supply full details of Fail2ban configuration settings, particularly those which you state caused the over-zealous blocking of communication between yourselves and the L1 provider and thus caused bulk message failure.

Syncronized: Due to server migration these configuration settings are no longer accessible. Settings of this nature would not be available whatsoever as advised by Tech because they are being removed every time new configuration is implemented. In conclusion, with all willing to help Executive, this data is not accessible.

2. Were these set by your Technical Dept. or were the default configuration settings of the installation accepted?

Syncronized: It is impossible at this point in time to compare default and custom settings. IP addresses are never put by default so these details used to be added by Tech.

3. Which version of fail2ban was being used when the incorrect "banning" was occurring?

Syncronized: It was a standard version of fail2ban.

4. Please supply "ANY" available log files produced by fail2ban. (One would assume that some of these would be kept as there were problems with the system and these would have helped diagnose the problem).

Syncronized: The usual and recommended procedure advises not to keep incorrect settings logs in case they affect remedied and 'cured' code. Syncronized provided example logs to Executive earlier this year.

5. Was the installation part of a Linux distribution?

Syncronized: In is standard available version it is a recommended software.

6. Was the installation downloaded separately as a standalone installation?

Syncronized: Due to server migration these details are no longer accessible.

7. Was the installation supplied as part of a server package by your hosting company?

Syncronized: No.

8. What communication protocol/service(s) are used between yourselves and the L1 provider?

Syncronized: Http connection.

9. Is connection between yourselves and the L1 initiated by yourselves or does the L1 establish a connection and then receive messages from you?

Syncronized: The nature of this question is not clear, if Executive asks about how message chain works, then yes – the message is initiated by Syncronized after all, it is Syncronized who wishes to send a message to subscriber to provide content access, collect contract charge or remind about subscription.

10. What is the name of the software used for communicating with L1 servers?

Syncronized: Http protocol.

11. Which Firewall solution was being used beneath Fail2ban.

Syncronized: It used to be both packet filters and stateful inspection type.

Appendix C

Internal server network settings before this error was identified

```
# Fail2Ban configuration file.
#
# This file was composed for Debian systems from the original one
# provided now under /usr/share/doc/fail2ban/examples/jail.conf
# for additional examples.
#
# Comments: use '#' for comment lines and ';' for inline comments
#
# To avoid merges during upgrades DO NOT MODIFY THIS FILE

# and rather provide your changes in /etc/fail2ban/jail.local
#
# The DEFAULT allows a global definition of the options. They can be overridden
# in each jail afterwards.
[DEFAULT]
# "ignoreip" can be an IP address, a CIDR mask or a DNS host. Fail2ban will not
# ban a host which matches an address in this list. Several addresses can be
# defined using space separator.
ignoreip = 127.0.0.1/8
```

Internal server network settings after this error was identified:

```
# Fail2Ban configuration file.
#
# This file was composed for Debian systems from the original one
# provided now under /usr/share/doc/fail2ban/examples/jail.conf
# for additional examples.
#
# Comments: use '#' for comment lines and ';' for inline comments
#
# To avoid merges during upgrades DO NOT MODIFY THIS FILE
```

```
# and rather provide your changes in /etc/fail2ban/jail.local
#
# The DEFAULT allows a global definition of the options. They can be overridden
# in each jail afterwards.
[DEFAULT]
# "ignoreip" can be an IP address, a CIDR mask or a DNS host. Fail2ban will not
# ban a host which matches an address in this list. Several addresses can be
# defined using space separator.
ignoreip = 127.0.0.1/8 52.19.105.85 54.228.242.71 54.154.185.30 54.74.18.32 54.78.51.224 176.34.161.57 54.194.146.155 54.194.13.190
```

Appendix D

Application for interim measures pursuant to Code of Practice paragraph 4.6

Case ref:	72275
Service:	"4 Your Eyes Only" glamour video subscription service
Level 2 provider:	Syncronized Ltd
Level 1 provider:	Zamano Ltd; Veoo Ltd
Cost:	£3 per week and £4.50 per week
Shortcodes:	80008, 82999, 89225, 88150, 84506 and 66255

Tribunal number: **189**

Adjudication

- The Tribunal has paid full regard to the material supplied by the Executive. In respect of the material submitted by the Executive, the Tribunal noted in particular:

  a) 341 complaints had been received about the Service after the last procedure against the Level 2 provider, the latest being on 12 July 2016.
  b) There was a history of previous enforcement action against the Level 2 provider for charging consumers without having robust evidence of their consent.
  c) The nature of the apparent breaches referred to by the Executive, including their submission on the veracity of message logs provided by the Level 2 provider.
  d) The information in the Debt Collection Withhold Assessment

- The Tribunal has paid full regard to the representations provided by the Level 2 provider. In respect of the material submitted by the Level 2 provider, the Tribunal noted in particular:

  a) The Level 2 provider's submission that complainants had opted in before the Track 1 procedure, and so it did not hold sufficient evidence of consent for those complainants.
  b) The Level 2 provider's submission that it had had technical problems resulting in delays to billing complainants, which was why complaints were now being received. The Tribunal considered that the explanation of why this had happened and why it was affecting complainants in the way shown for the period in question was unclear; the Tribunal considered that the Level 2 provider may in due course provide sufficient evidence to support its explanation that the pattern shown was explained by the operation of a firewall, but considered that until this was done there were legitimate concerns regarding the accuracy of the logs.
  c) The Level 2 provider's submission that the matter was addressed by a previous Track 1 procedure. The Tribunal noted that the action plan clearly stated that the Executive may initiate a Track 2 procedure if the issues previously identified were not rectified,

and in any event, noted that the complainants had been charged in the period post-dating the Track 1 procedure.

d) The Level 2 provider's representations that it was unclear what allegations they had to face as "paragraph 4.2.4" was not present in the current 14th edition of the Code of Practice. The Tribunal considered that this submission had no merit as the text of the Code provision was set out in the Interim Warning Notice, and related to the Code in force at the time of the conduct in question, and it was plain from the context of the Level 2 provider's response that they understood the nature of the Executive's concerns.

e) The Level 2 provider's representations that it was unfair that they had not previously received notice that the case was allocated to Track 2. The Tribunal noted that the investigation in this case had commenced during the period when the 13th Code of Practice was in force and was continuing in the current period when the 14th Code of Practice was in force. Allocation to a Track remained an internal process handled by the Executive. The Tribunal noted that the Executive had written to the Level 2 provider on 18 February 2016 and made it clear that the Executive was conducting investigations into the Level 2 provider's conduct, and in previous enforcement actions it had been made clear that a Track 2 procedure might be initiated in future if issues previously identified were not rectified. The Tribunal considered that the Level 2 provider had not suffered any prejudice by not being separately and specifically notified of allocation to Track 2, as the Interim Warning Notice had provided an explanation of the Executive's concerns, and given the Level 2 provider an opportunity to respond before any measures were taken.

f) The Level 2 provider's submission that in light of procedural errors by the Executive it needed to seek legal advice and would not be able to do so if the withhold was imposed. The Tribunal considered that the Level 2 provider had not supplied any evidence to support this assertion.

g) The Level 2 provider had stated that it had provided refunds and referred to a spreadsheet setting out refunds provided up to 8 October 2015. However the Tribunal also noted that this evidence did not address more recent complaints, and also noted that some complainants mentioned refunds not being given when promised, and issues with contacting the Level 2 provider, and so was concerned that the refund system was not working as well as it should do.

- The Tribunal has paid regard to the Supporting Procedures, including the factors set out at paragraph 80 and paragraph 91.

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

6) At first appearance (and subject to evidence, arguments or information being later supplied and/or tested), there does appear to be sufficient evidence that could support a breach of Code of Practice rule 2.3.3 and Code of Practice (13th edition) paragraph 4.2.4.

7) 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 lack of up-to-date published filed accounts

ii) that a notice of dissolution had been recently filed at Companies House, (although dissolution had since been cancelled)
iii) the Level 2 provider's most recent published balance figures
iv) the Level 2 provider's compliance history
v) the potential seriousness of the breaches, and service revenue, which could result in a higher level of fine.

8) The Tribunal is satisfied that PhonepayPlus has made reasonable endeavours to notify the Level 2 provider of its initial findings and the proposed interim measures.

9) The Tribunal considers that the measures set out below are appropriate and proportionate to take in the circumstances of this case.

10) Accordingly, the Tribunal hereby directs that:

a) PhonepayPlus is authorised to direct a withhold of up to £276,000**.**

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.

ROBIN CALLENDER SMITH
4 AUGUST 2016