Tribunal meeting number:	229
Case reference:	118585
Level 2 provider:	Xplosion Limited
Type of service:	Glamour video subscription service
Level 1 provider:	Dimoco Europe GmbH, Austria
	Dynamic Mobile Billing Limited, Birmingham, UK
Network operator:	All Mobile Network Operators

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

The case concerned adult / glamour video portal subscription services operating under the service names 'SexxyMob', 'Xcite' and 'Xvidland' on PayForIt ("**PFI**") and on shortcode 65065 (used for consumers to send STOP to unsubscribe from the services, and for the sending of free Service initiation and reminder messages) (the "**Services**").

The Level 2 provider for the Services was Xplosion Limited (the "**Level 2 provider**"). The Level 2 provider has been registered with the Phone-paid Services Authority (the "**PSA**") since 27 January 2015.

The Level 1 provider for the Services was Dynamic Mobile Billing Limited ("**DMB**"), formerly Oxygen8 Communications UK Limited.

The Services were stated to be adult / glamour video portal subscription services charged at £4.50 per week.

The Level 2 provider had stated that initial subscribers joined the Services on the following dates:

- SexxyMob – 19 August 2016
- Xcite – 26 August 2016
- Xvidland – 26 August 2016

DMB confirmed that it suspended residual billing for the Services on 13 January 2017.

The Executive issued a request for information ("**RFI**") in relation to the Services on 27 October 2016. In its response to the RFI on 1 November 2016, the Level 2 provider stated the following in relation to Xcite and Xvidland :

"Xcite & Xvidland, -These are both a "video on demand" glamour service. Users can watch videos."

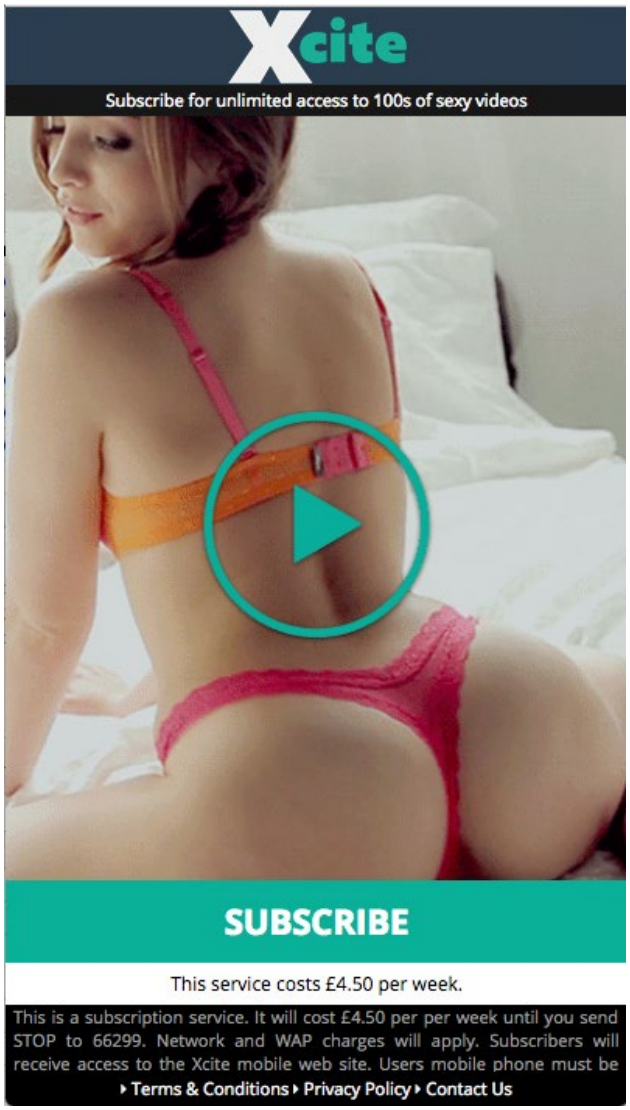
"A user subscribes to watch videos through the Xcite and Xvidland glamour portals. User will have access to this content, until he/she unsubscribes."

In addition to providing the above description of Xcite and Xvidland, the Level 2 provider supplied the following user flow into the above two services:

Xcite user flow

"1) User clicks on banner ad, on mobile site.

1. *User Is brought to landing page, where they click subscribe.*



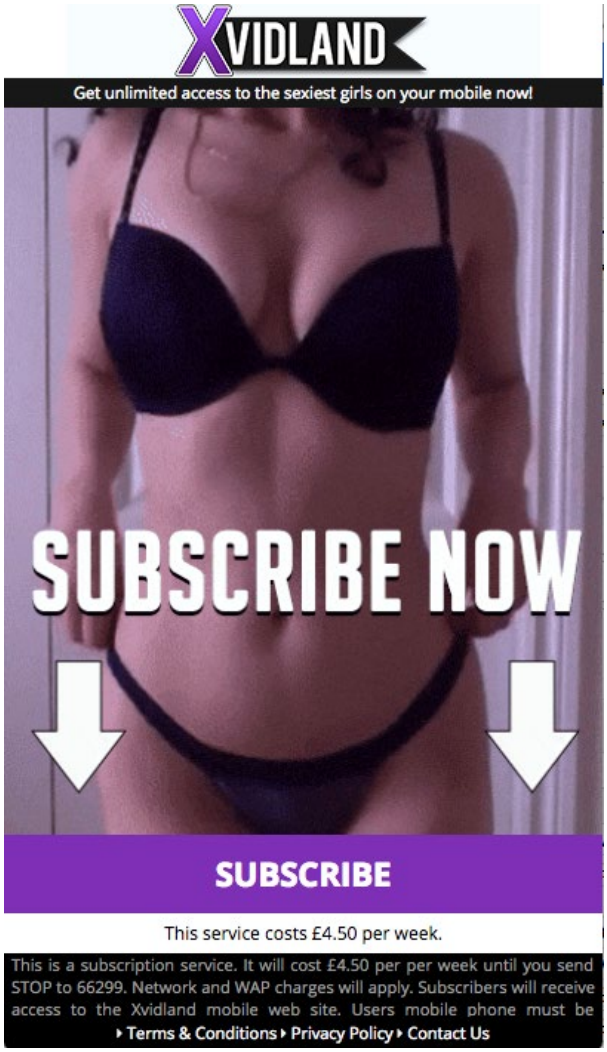
2. *User is brought to PFI Payment page.*

(At the moment Oxygen8 have this switched off, so we are unable to get screenshots. We have requetsed they switch back on to provide screenshots.)" [sic]

Xvidland user flow

"1) *User clicks on banner ad on mobile site.*

2) *User Is brought to Landing page*



3) User is brought to PFI Payment page.

"(At the moment Oxygen8 have this switched off, so we are unable to get screenshots. We have requetsed they switch back on to provide screenshots.)" [sic]

In addition to the above information provided by the Level 2 provider for Xcite and Xvidland, the Level 2 provider supplied the following description for SexxyMob on 10 March 2017:

"Porn Kingz and SexxyMob are both adult VOD services – the same as Xcite and Xvidland."

On 10 March 2017 the Level 2 provider also supplied the following user flow for SexxyMob:

1) User clicks on banner ad on mobile site

2) User is brought to Landing page.

3) User is brought to PFI Payment Page.

4) User is brought our Content Portal

"

Further to the above service descriptions and user flows for the Services, the Level 2 provider provided full terms and conditions for the Services.

Executive Service monitoring

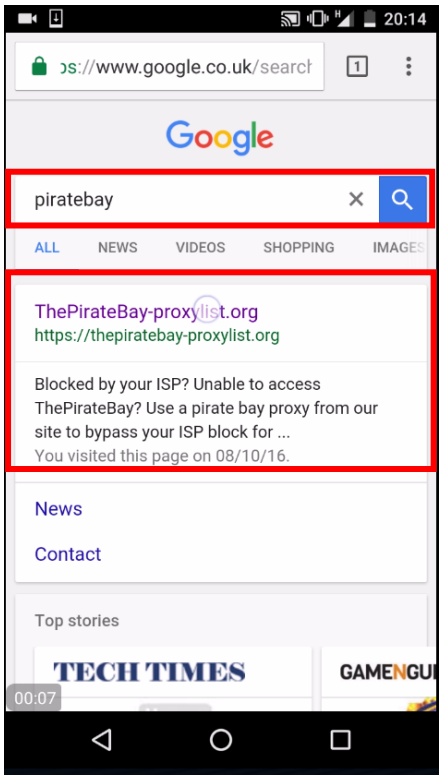
The Executive had monitored the Services on the following dates:

- SexxyMob – 8 October 2016
- Xcite – 16 October 2016
- Xvidland – 16 October 2016

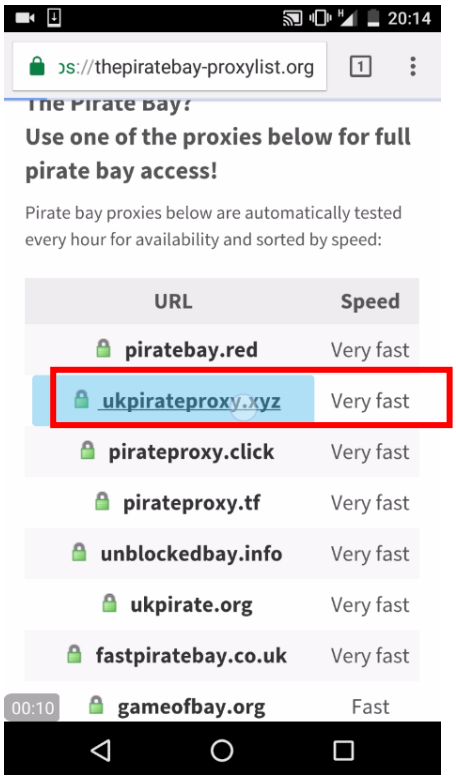
The following are screen shots taken from the monitoring report which demonstrates the user journey as monitored by the Executive:

SexxyMob Monitoring

Screenshot 1

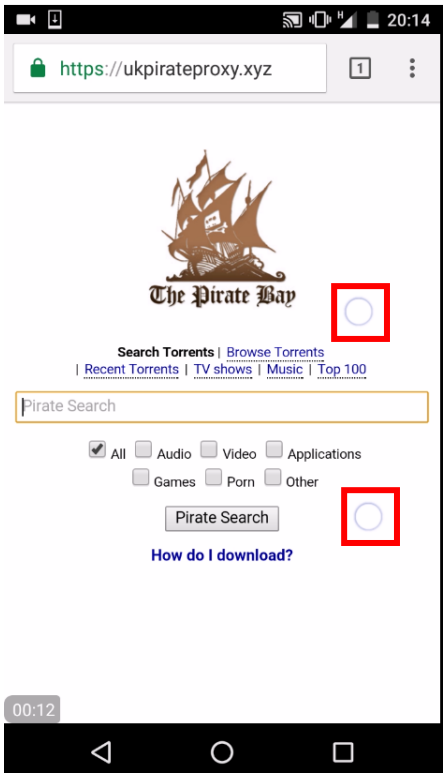


Screenshot 2

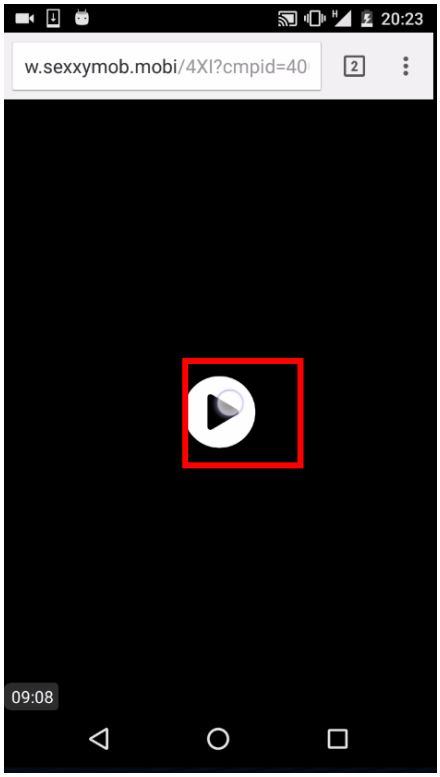


The Executive performed a google search for 'piratebay', as shown in Screenshot 1, and selected '*ukpirateproxy.xyz*', as shown in screenshot 2.

Screenshot 3

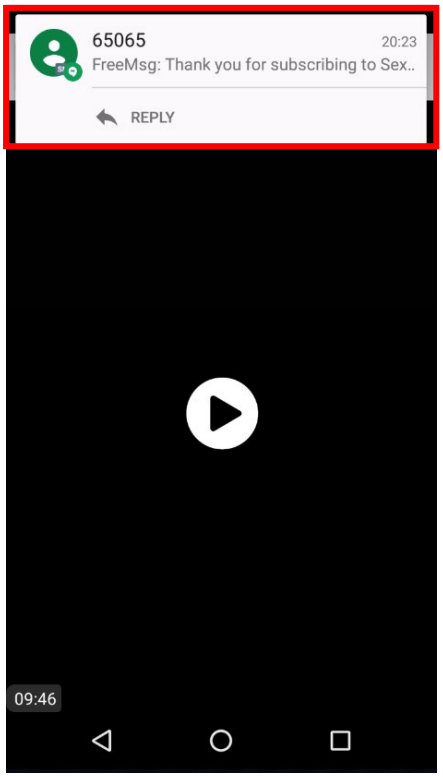


Screenshot 4

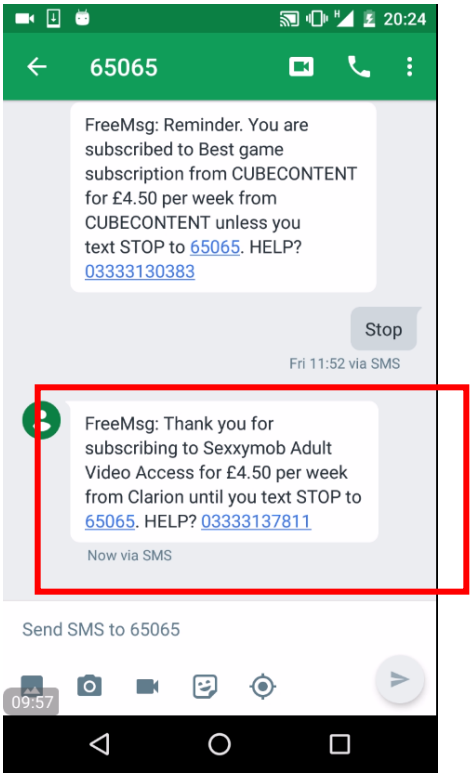


Upon attempting to zoom in on Screenshot 3 the Executive was presented with the screen as shown in Screenshot 4, which appeared to include a video play icon.

Screenshot 5



Screenshot 6



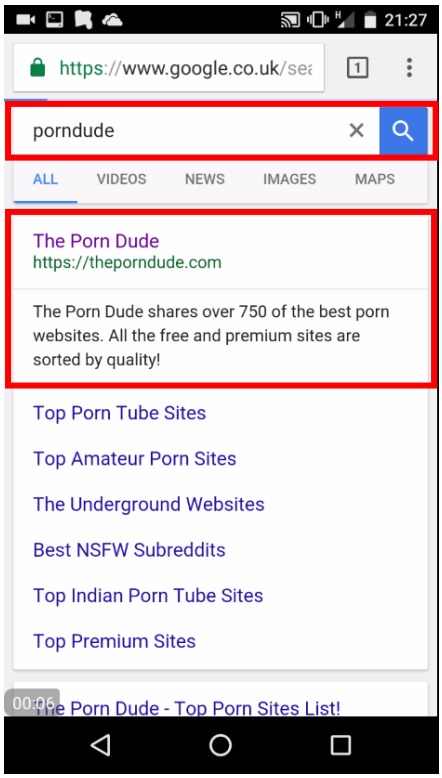
The Executive clicked on the video play icon displayed in Screenshot 4 and received the following free SexxyMob initiation message from shortcode 65065 (the Service ignition message has also been highlighted in Screenshots 5 and 6 above):

"FreeMsg: Thank you for subscribing to SexxyMob Adult Video Access for £4.50 per week from Clarion until you text STOP to 65065. HELP? 03333137811"

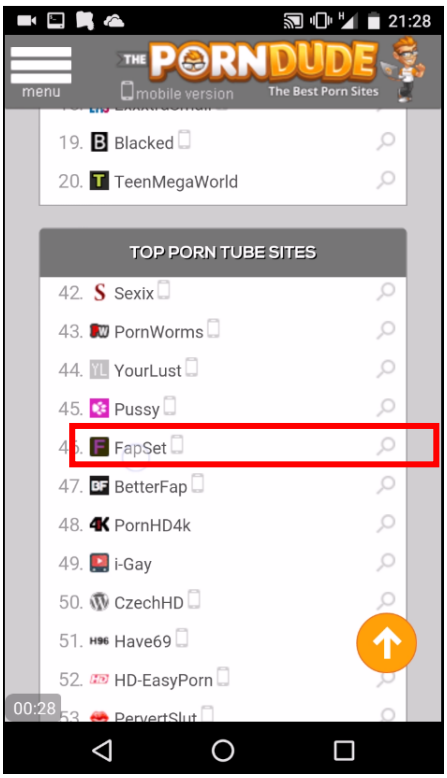
In addition to the receipt of the SexxyMob initiation message, the Executive incurred a £4.50 SexxyMob charge.

Xcite Monitoring

Screenshot 1

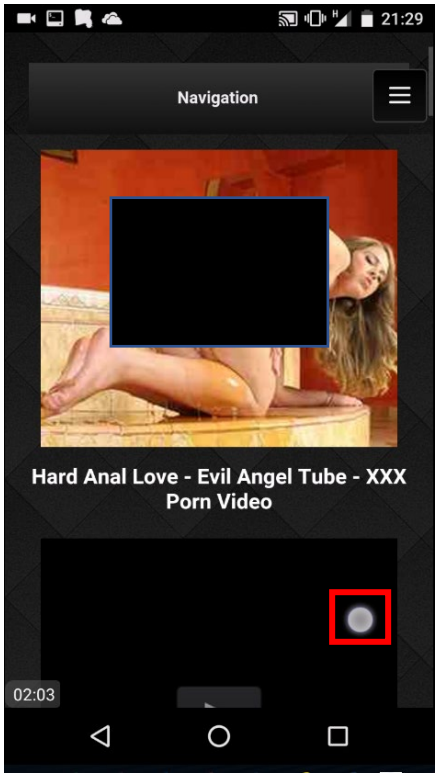


Screenshot 2

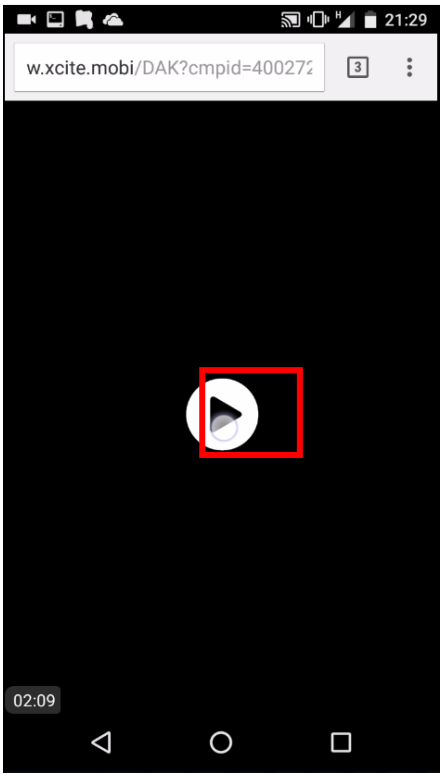


The Executive performed a google search for 'porndude', as shown in Screenshot 1, and selected '*FapSet*', as shown in screenshot 2.

Screenshot 3

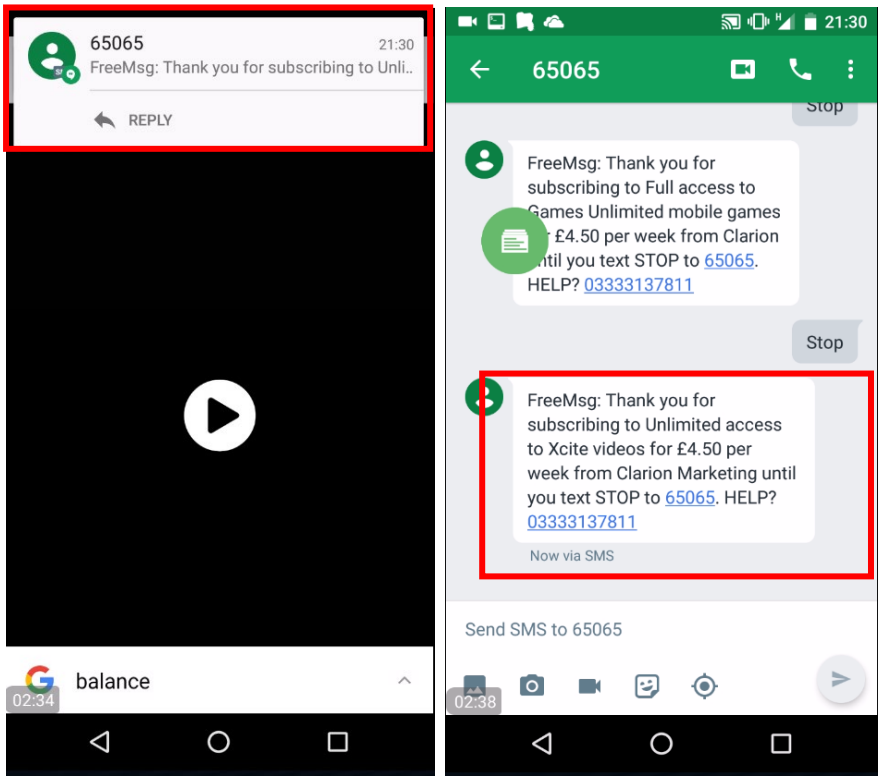


Screenshot 4



Upon attempting to scroll down on Screenshot 3 the Executive was presented with the screen as shown in Screenshot 4, which appeared to include a video play icon.

Screenshot 5 **Screenshot 6**



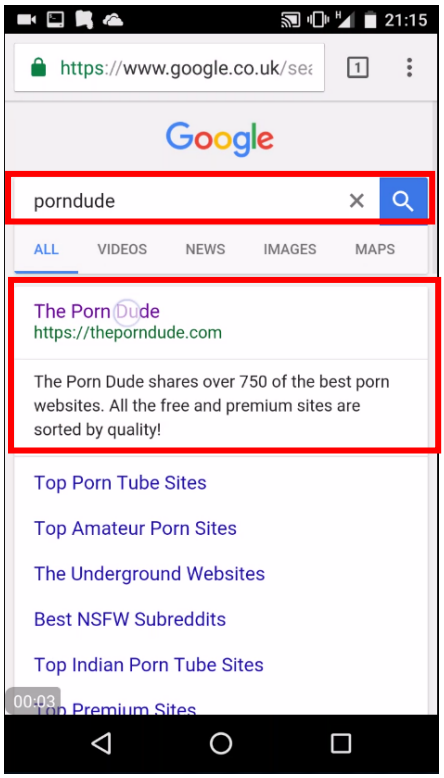
The Executive had clicked on the video play icon displayed in Screenshot 4 and received the following free Xcite initiation message from shortcode 65065 (the Service ignition message has also been highlighted in Screenshots 5 and 6 above):

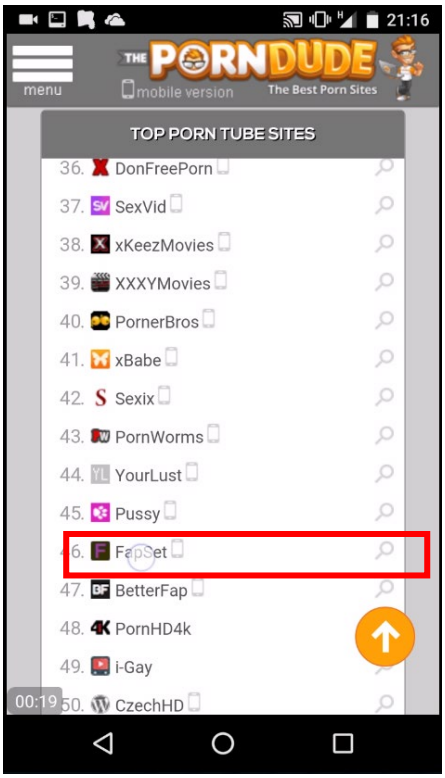
"FreeMsg: Thank you for subscribing to Unlimited access to Xcite videos for £4.50 per week from Clarion Marketing until you text STOP to 65065. HELP? 03333137811"

In addition to the receipt of the Xcite initiation message, the Executive incurred a £4.50 Xcite charge.

Xvidland Monitoring

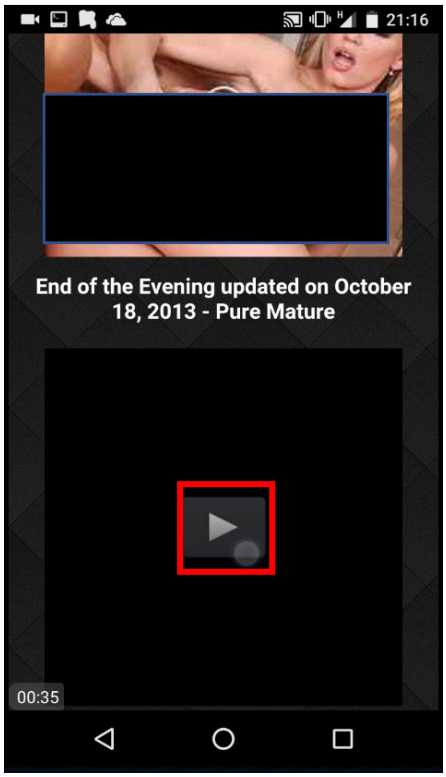
Screenshot 1 ***Screenshot 2***



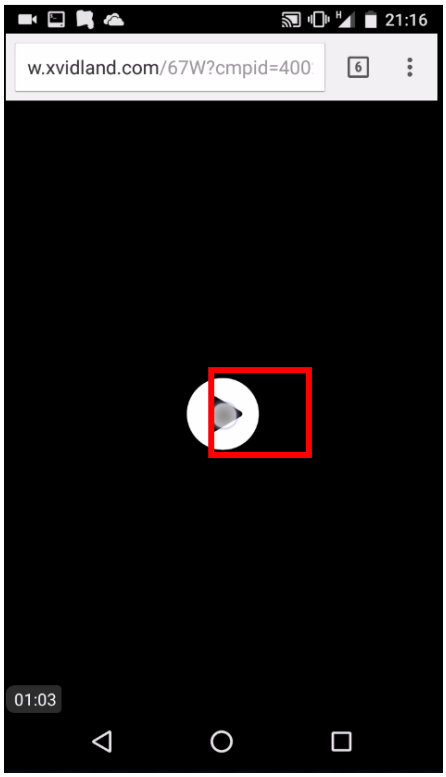


The Executive performed a google search for 'porndude', as shown in Screenshot 1, and selected '*FapSet*', as shown in screenshot 2.

Screenshot 3

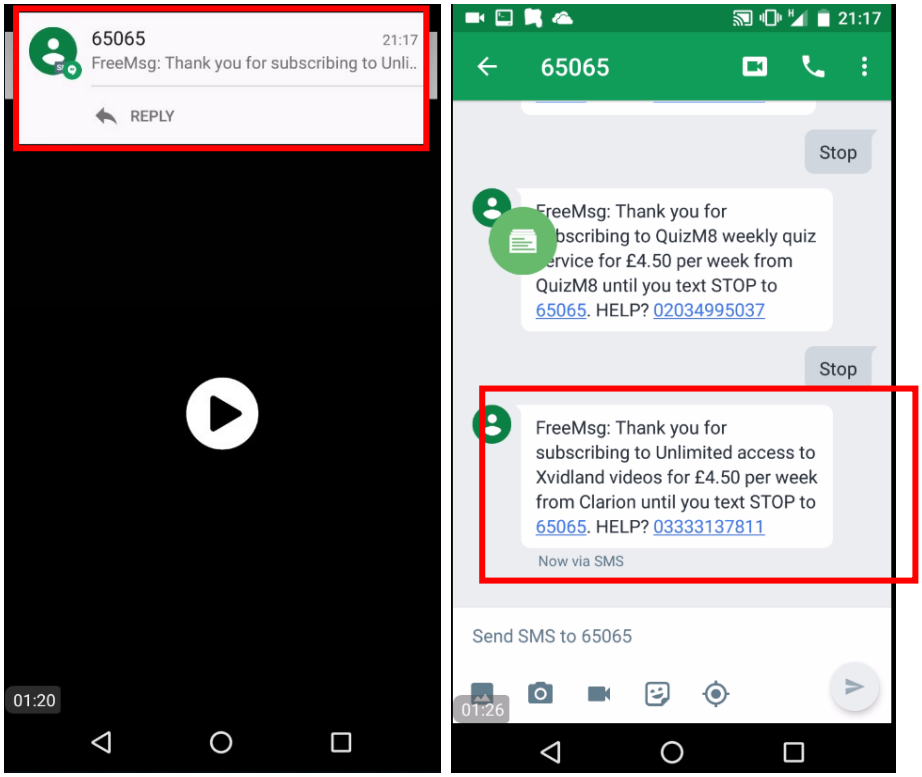


Screenshot 4



Upon attempting to view the video in Screenshot 3 the Executive was presented with the screen as shown in Screenshot 4, which appeared to include a video play icon.

Screenshot 5 **Screenshot 6**



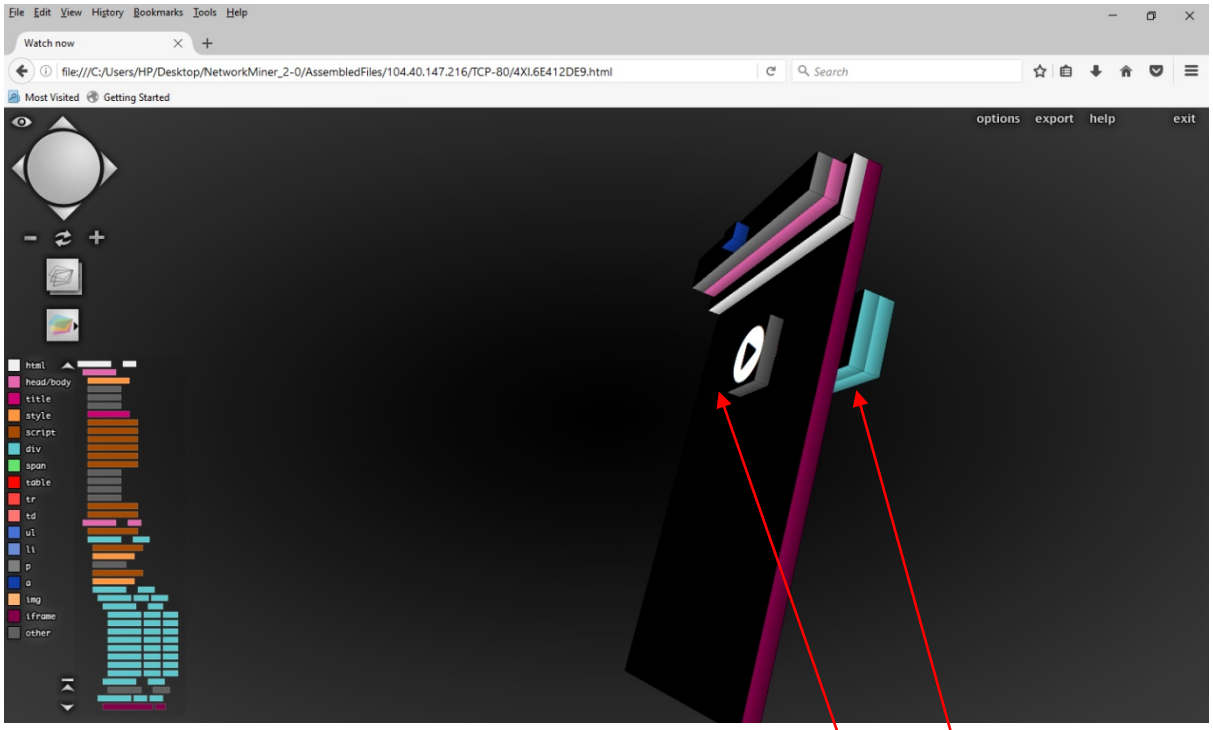
The Executive had clicked on the video play icon displayed in Screenshot 4 and received the following free Xvidland initiation message from shortcode 65065 (the Service ignition message has also been highlighted in Screenshots 5 and 6 above):

"*FreeMsg: Thank you for subscribing to Unlimited access to Xvidland videos for £4.50 per week from Clarion until you text STOP to 65065. HELP? 03333137811*"

In addition to the receipt of the Xvidland initiation message, the Executive incurred a £4.50 Xvidland charge.

The Executive's understanding from the above monitoring of the Services is that, when the Executive arrived at Screenshot 4 in the monitoring journeys it had arrived at the Services PFI payment page, however, an 'iFrame' had been placed over the PFI payment pages, which obscured the Services payment and terms and conditions information. This process is known as "iFraming".

The Executive, in its full monitoring report provided the following visual representation of how 'iFraming' work:



The Executive's monitoring report explained that, by clicking on the video play icon on the iFrame (as shown in monitoring Screenshot 4), a visitor to the 'iFramed' PFI webpage would have inadvertently clicked to accept a Service charge confirmation hidden behind the iFrame. This use of 'iFraming' in this way is known as 'click-jacking'.

Summary of complaints

The Executive had received 82 complaints concerning the Services since 30 August 2016. Complainants variously alleged that the Service charges were unsolicited. A sample of complainant accounts is provided below:

FreeMsg: Reminder. You are subscribed to Sexxymob Adult Video Access for £4.50 per week from Clarion unless you text STOP to 65065. HELP? 03333137811
I never activate such thing . It pop up on my phone while browsing the net . Recieve a message . It said press stop to cancel it i did thinking that was the end until i saw my phone bill this month
Have you contacted the Service Provider: Yes

I have contacted my service provider (T-Mobile via EE), who have stated that this is a service, video, games or digital content that I have paid for. They stated that upon review of the bill, it has been charged by www.payforit.org, which I cannot recall visiting.
I do not purchase anything through my phone ever so cannot see how this has been charged. I understand that I may have visited a website that is capable of taking my details.
Have you contacted the Service Provider: Yes

i was browsing a news website when a pop a pornographic pop-up message popped up, i attempted to click the x in the corner of the pop and as i did this i received the above message saying i had been billed £4.50 this the 2nd time this has happened!

I don't know what the supposed service is for or how they got my details.
They have text twice now and they seem to be on a 7 day rotation
£10 has been added to my bill up to now.

I am unsure on the service being offered as I did not knowingly subscribe to anything. I received the 1st message on 12.10.2016 and called the number given on 13.10.2016 to cancel. i then received another message on 20.10.2016 and again called to cancel and that time spoke to an advisor who emailed confirming as much. i then received another message on 28.10.2016 and called again.

Interim measures in place

On 3 May 2017 the Code Adjudication Panel ("**CAP**") had imposed interim measures, namely a withhold of Service revenue.

On 3 August 2017 the Level 2 provider's solicitors submitted an application to review the use of interim measures.

On 4 August 2017 the CAP considered the Level 2 provider's application to review the imposition of interim measures, along with an interim consent order. The CAP determined that it was appropriate to remove the interim measures imposed by the CAP of 3 May 2017, as detailed in the interim consent order. At the date of the substantive Tribunal hearing, there were, therefore, no interim measures in place in respect of the Service.

Preliminary issue

On the morning of the hearing, but before deliberations had begun on this case, the Tribunal received correspondence from the Level 2 provider's solicitors (letter dated 21.8.18 and Extracts from the Claimant's Grounds for Judicial Review against the imposition of Interim Measures on 3rd May 2018; paragraphs 52-60, 77, 97-101 and PSA's response by email dated 21.9.18).

It referred to an exchange between the Level 2 provider's solicitors and the Executive in relation to potential prejudice that may be caused by the inclusion of pornographic material, from a third-party affiliate website, which featured in the Executive's monitoring of the Service.

The Tribunal considered the correspondence and came to the following decisions:

1. There was no prejudice caused to the Level 2 provider in the Tribunal viewing the entirety of the Executive's monitoring journey and the accompanying screenshots. The Tribunal considered that it would have been inappropriate for the video or screenshots to have been edited in any way as this would have impacted on their evidential value

and could open up arguments in relation to continuity. The Tribunal, made up of professional panel members, was quite capable of identifying irrelevant information and putting it to one side when making decisions. The nature of the photography had no impact on the fact finding.

2. The Tribunal read the extracts from the judicial review application and where appropriate, considered them in its decision making on the substantive case.

Apparent breaches of the Code

The Executive submitted that the Service breached the Phone-paid Services Authority (the "**PSA**") Code of Practice 14th Edition (the "**Code**") and in particular the following Code provisions:

- Rule 2.3.3 – Consent to charge
- Rule 2.2.1 – Transparency and pricing
- Rule 2.3.1 – Fair and equitable treatment
- Paragraph 3.4.14 (a) – Service registration

Alleged breach 1

Rule 2.3.3 of the Code

"Consumers must not be charged for PRS 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 consumers could be unwittingly subscribed to the Services and therefore be charged without their consent.

The Executive relied on complaints received stating that unsolicited charges had been incurred, the content of the PSA Guidance on Consent to Charge (the "**Consent to Charge Guidance**") and the PSA Guidance on Promoting PRSs (the "**Promoting PRS Guidance**").

The Consent to Charge Guidance states:

"1. Why is the capability to verify your right to charge important?

1.1 *PRSs allow a charge to be generated to a consumer's phone bill, whether pre-paid or post-paid as part of a contract with an originating network, directly and remotely. A major concern then is that they can be charged without having requested or consented to any purchase.*

1.2 *It is important to understand the need for transparency when establishing any consent to charge a consumer via PRS payment. The key service information necessary to comply with Rule 2.2.4 of the Phone-paid Services Authority's Code of Practice must be presented clearly and with suitable proximity and prominence. This is to ensure any action on the consumers part reflects a genuine intention to consent to the charges triggered by the action."*

The Promoting PRS Guidance states:

"2. Setting out key information and promoting transparently

***2.1** There is a vast range of different types of PRS. Each of these may need to give slightly different information to a consumer within their promotions, in order to ensure consumers have all the information they would reasonably need before purchasing.*

***2.2** In addition, there are a range of different types of promotional material, ranging from promotions that are self-contained (such as a print-based advert, inviting a consumer to call or text an access number), to promotions that have a number of components that lead a consumer toward a purchase. An example of this would be a text message with a link to a mobile website, where the consumer subsequently makes purchases using a secure payment method. In this latter case, there would be a number of steps between the first promotion and a purchase. This results in a number of stages at which a provider can act to ensure consumers were aware of all information necessary to make a decision to purchase, prior to any purchase.*

***2.3** Because of this complexity, the Phone-paid Services Authority recommends that providers familiarise themselves with the entire contents of this Guidance and especially the parts relevant to the promotional mechanics they use. However, as a basic starting point, the following information is considered key to a consumer's decision to purchase any PRS, and so should be included in promotional mechanics for any PRS:*

- *Cost*
- *Brand information*
- *Product or service information*
- *How it is delivered or used*
- *How it is paid for – one off payment, recurring charges, etc.*
- *How to get help where necessary"*

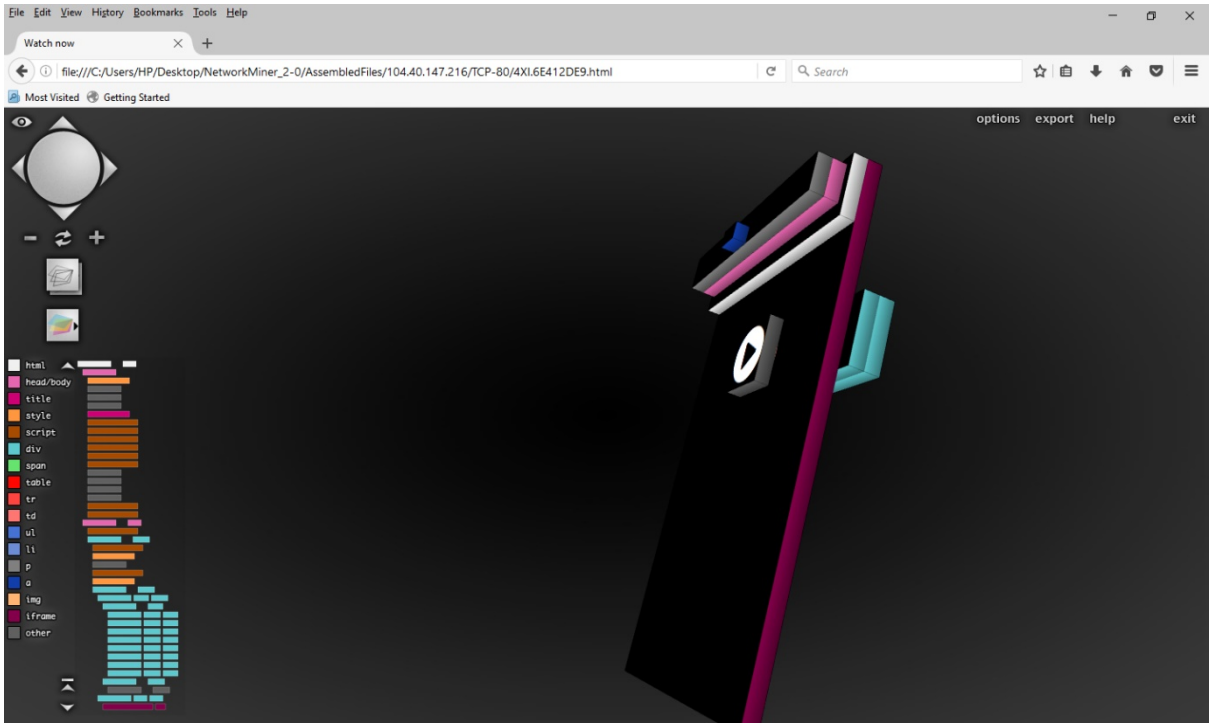
The monitoring journeys performed by the Executive on 8 October 2016 and 16 October 2016 showed that the Services were promoted via a website that aggregated online entertainment media and software (in respect of SexxyMob), and an adult website that aggregated links to other adult websites (in respect of Xcite and Xvidland), as shown in Screenshot 2. After selecting an option from the aggregated list of websites, the Executive arrived at one of the websites listed in Screenshot 3 of the monitoring journeys.

The Executive noted that no information on the Services, or the Level 2 provider, had been provided during the monitoring journeys. After clicking a link within Screenshot 3 in the monitoring journeys, the Executive was presented with a screen which appeared to be black with a video play icon located in the centre of the screen.

The Executive noted that at this point in the monitoring journeys (Screenshot 4) the monitoring handset had been directed to the domain, sexxymob.mobi, xcite.mobi and xvidland.com in the monitoring journeys for SexxyMob, Xcite and Xvidland, respectively. Further, the Executive noted that Screenshot 4 lacked any information on the Services, or

information on the Level 2 provider, as required in the Code.

By clicking on the video play icon displayed in Screenshot 4, a visitor to the Services websites was inadvertently clicking to agree to premium rate charges on the underlying PFI payment page which was obscured by the iFrame puporting to show a video play icon.



The Executive's monitoring showed that clicking on the video play icon in Screenshot 4 resulted in a charge without the provision of any Service information prior to the commencement of that charge.

During the course of the investigation, the Executive directed DMB to supply HTTP header information and SQL databases for subscribers, which contained information on the flow into the Services that consumers followed prior to incurring premium rate charges. The Executive had then performed an analysis to determine the number of subscribers whose journeys to the Services mirrored the journeys performed in the Executive's monitoring. The analysis of the Service subscriber HTTP header information and SQL databases indicated that 7944 subscribers incurred premium rate charges after interacting with the same URLs on which the iFrame was hosted in the Executive's monitoring.

The Executive noted that the monitoring journey captured by the Executive did not follow the method of entry described by the Level 2 provider, in which a conusmer was requried to enter their mobile number to subscribe to the Service.

The purpose of requiring a consumer to interact with a PFI page, if implemented, was to ensure that a consumer knowingly initiated a subscription to a PRS through their actions. However, in the journeys captured by the Executive, the action that initiated the premium rate subscription was an attempt by the consumer to view what purported to be a free video, and not an acceptance of the charges for a PRS. At no point during the journeys was the consumer alerted

to the fact that they were engaging with a PRS or given the choice as to whether they wished to subscribe to the Service. A consumer would only have become aware that a subscription to the Service had been initiated when they received a confirmation text message on their handset. By this point the consumer would have already been charged.

The Executive noted that the Level 2 provider had contracts in place with the audit houses Empello Ltd ("**Empello**") and MCP Insight Ltd (formerly Monitoring & Compliance Partners Limited) ("**MCP**") to provide monitoring of the Level 2 provider's PRSs, including the Service subject to this investigation.

In relation to the monitoring performed by Empello and MCP, the Level 2 provider stated in its submission received by the Executive on 20 January 2017:

*"We engaged the services of both MCP and Empello to provide us with monitoring of our services. We engaged Empello on 8th August 2016 and MCP on 15th August 2016. Neither monitoring company discovered any evidence of non-complaint activity for our services. There were no spikes in traffic, and no spike in conversion rates for these services. I am attaching a report from Empello ["**Example Empello Monitoring Report**"], who discover our offer 14 times in the market. On none of these 14 times did they discover any non-compliance. MCP have not responded to our request for information before the deadline of 5pm on 20th January."*

The Executive noted that the Example Empello Monitoring Report contains four screen shots relating to the 'Porn Kingz' PRS operated by the Level 2 provider, apparently monitored on 15 October 2016 at 20:31.

On 22 September 2017 the Level 2 provider supplied links to the 14 instances in which it stated that Empello had discovered its PRSs in the market. The Executive noted that Empello had not opted-in to the Level 2 provider's services in any of the monitoring journeys. In addition, the PFI payment page, which was the subject of iFraming captured in the Executive's monitoring, had not been captured in eight of the 14 monitoring journeys.

The Executive also noted that in three of Empello's monitoring journeys, the time displayed while on the PFI payment page was 11:13, despite the monitoring journeys apparently being performed at different times.

In addition to the above, the Executive noted that the Example Empello Monitoring Report was timed at occurring at the same time as one of Empello's monitoring journeys on 15 October 2016 at 20:31, however, the Executive was concerned that the screen shots within the two documents differ, and that the time stated on the monitoring handset differs.

Further, the Executive noted from Empello's email to the Level 2 provider dated 24 July 2017 that the software used by Empello did not always capture the entire journey performed by Empello.

In relation to monitoring performed by MCP on the Level 2 provider's PRSs, the Level 2 provider had provided an email from MCP advising that it had not found the Level 2 provider's

services in general advertising. There was, therefore, no MCP monitoring of the Level 2 provider's PRSs at all.

The Executive submitted that its monitoring was more reliable than that undertaken by Empello and MCP for the following reasons:

- Empello had accepted that its software did not capture entire monitoring journeys in all instances
- Empello had not opted into the Level 2 provider's PRSs when performing its monitoring
- There were discrepancies between the screen shots supplied by the Level 2 provider, purporting to be of monitoring by Empello, and the monitoring journey said to have been performed by Empello
- Screen shots of monitoring journeys performed by Empello appeared to have been re-used
- There was a complete lack of any monitoring by MCP, despite the Service being promoted, as demonstrated by the Executive's monitoring and the large number of affected consumers.

The Executive's position was that, as the iFraming exploit was hosted on the Services' website, the Level 2 provider must have been aware of it. The Executive noted the Level 2 provider's explanation for the 'iFraming' of its Service payment page:

"*Xplosion shares our servers with at least 379 other websites. We also provide access to our servers via FTP and Host and Post….There would be many avenues for a rogue affiliate, hacker, or advertising partner to access and compromise the Xplosion payment pages*".
The Executive submitted that, merely sharing a server with other websites would not in itself allow third-parties to compromise the Service payment page. Further, the Level 2 provider had supplied no evidence that its servers were compromised at the time the iFraming exploit was implemented.

The Executive's monitoring indicated that a consumer could trigger a subscription to the Service through the act of trying to view a free video. The Executive asserted that the pressing of a video play button on a website could not be viewed as giving consent to be charged for a premium rate subscription service.

Given the above, the Executive submitted that a breach of Rule 2.3.3 of the Code had occurred.

2. The Level 2 provider did not admit the breach. It criticised the Executive's monitoring, stating that it did not represent a typical user journey. However, the Level 2 provider accepted that its payment pages had been compromised at the time of the Executive's monitoring and suggested that it too had been a victim of click-jacking.

It was submitted by the Level 2 provider that a rogue affiliate must have accessed its servers and placed the iFrame over its payment page. The Level 2 provider stated that this was possible as it had provided Files Transfer Protocol ("**FTP**") access to its servers, giving 72 affiliates editing control of its payment pages. It argued that the iFraming only made up small proportion of the traffic to the Service as, Empello did not find many, and MCP did not find any,

of the promotions in their monitoring. The Level 2 provider also pointed to one occasion in the Executive's monitoring which showed a compliant payment page.

The Level 2 provider asserted that its conversion rate, of clicks to the landing page converting to subscribers, was in line with industry standards. It argued that if there had been a widespread abuse of its pages, this conversion rate would likely have been higher. The Level 2 provider did not supply evidence in support of this assertion.

The Level 2 provider argued that the Executive's analysis of the scale of consumer harm was flawed. It submitted that the URLs found in the monitoring, which had been compromised by click-jacking, were not static and the pages were modified over time and therefore not compromised for the entire period.

3. The Tribunal considered the Code and all of the evidence in the case.

It noted that the Level 2 provider had accepted that its payment pages for the Service had been compromised. The Tribunal found therefore that the payment page had been compromised and that there had been a click-jacking exploit on the Level 2 provider's server.

The Tribunal accepted the monitoring carried out by the Executive. It did not have before it direct evidence that the Level 2 provider had, itself, placed the iFrame over its payment page. However, it considered that whether it did so, or was so reckless as to allow FTP access to so many affiliates, giving them full editing control of its payment pages, the Level 2 provider was liable for the exploit.

The Tribunal noted the Level 2 provider's assertion that there had been a widespread problem with rogue affiliates at the time of the breach (these submissions were repeated in the Level 2 provider's application for Judicial Review referred to above and considered by the Tribunal). The Tribunal did not consider that this assisted the Level 2 provider's case and instead queried why, particularly in those circumstances, it would take the risk of allowing full editing access to its payment pages to its affiliates. Neither did the Tribunal accept that, in operating such a high risk business model (by allowing uncontrolled FTP access), it was sufficient simply to engage the audit houses MCP and Empello to carry out monitoring. The Tribunal did not consider the monitoring carried out by those companies to be sufficient to discharge the Level 2 provider's responsibilities under the Code as MCP had not managed to find the Service, despite it being promoted, and Empello had accepted that it did not capture entire monitoring journeys.

The Tribunal was further concerned that the Level 2 provider had submitted in its response to the Warning Notice that it had been the victim of a rogue affiliates but in earlier correspondence, on 1 November 2016, had informed the Executive that it did not use affiliate marketing. The Tribunal considered that this undermined the credibility of the Level 2 provider's submissions.

The Tribunal accepted the monitoring evidence conducted by the Executive and the evidence of the scale of the consumer harm. It found that, based on the analysis conducted by the Executive and date range of the consumer complaints that 7944 consumers had been subscribed to the Service without their consent. The monitoring journey showed that they had not been made aware that there was a chargeable service on offer or that clicking on the video play button would initiate a subscription to a PRS. The Level 2 provider was found to be wholly liable for the click-jacking exploit on the Services' payment pages.

Accordingly, the Tribunal was satisfied that there was cogent evidence presented by the Executive. Applying the civil standard of proof, it found that it was more likely than not, that

the affected consumers had not given their informed consent to be charged and upheld a breach of Rule 2.3.3 of the Code.

Decision: Upheld

Alleged breach 2

Rule 2.2.1 of the Code

"Consumers of PRS must be fully and clearly informed of all information likely to influence the decision to purchase, including the cost, before any purchase is made."

1. The Executive asserted that the Level 2 provider had breached Rule 2.2.1 of the Code because key information which would likely influence a consumer's decision to subscribe to the Service was not provided prior to the initiation of the Service subscription charges.

The Executive relied on complaints received stating that unsolicited charges had been incurred and the Promoting PRS Guidance.

The Executive relied on the monitoring of the Service, set out above, which demonstrated that the use of iFraming on the Service payment page effectively hid all Service information that would have been required by a consumer to make an informed decision whether to purchase the Service.

The Executive therefore submitted Service information was not provided consumers, as required under the Code, and specifically, that the Level 2 provider had breached rule 2.2.1 of the Code for failing to fully and clearly inform consumers of all information likely to influence the decision to purchase, including the cost, before any purchase was made.

2. The Level 2 provider did not accept the breach. It argued that it was directly linked to the Alleged breach of Rule 2.3.2 and that the Executive was seeking to artificially inflate its case in order to achieve a greater fine. It advanced the same arguments as for the above breach.

3. The Tribunal considered the Code and all the evidence before it. Applying the civil standard of proof, the Tribunal found that where consumers had accessed the Service as a result of iFraming/click-jacking, they would not have received information required under Rule 2.2.1 of the Code. The Level 2 provider was therefore found to have failed to fully and clearly inform consumers of all information likely to influence their decision to purchase the Service, including the cost, before any purchase was made.

Accordingly, the Tribunal upheld a breach of Rule 2.2.1 of the Code.

The Tribunal noted the submission of the Level 2 provider in relation to the overlap between the breach of Rule 2.3.2 and this breach. It referred to the Supporting Procedures which states at footnote 33 to paragraph 180:

"Where the CAT considers that a breach is proven but substantially overlaps with another upheld breach raised in the Warning Notice the CAT will make a determination to this effect, which will be reflected in the sanctions imposed."

The Tribunal decided that there was some overlap between the breaches and determined to take this into account at the sanction stage.

Decision: Upheld

Alleged breach 3

Rule 2.3.1 of the Code

"Consumers of PRS must be treated fairly and equitably."

1. The Executive asserted that the Level 2 provider had breached Rule 2.3.1 of the Code because consumers were not provided with the facility to engage with the video portal service, despite incurring premium rate charges.

The Level 2 provider had informed the Executive the following regarding the Services:

"Xcite & Xvidland, -These are both a "video on demand" glamour service. Users can watch videos."

"A user subscribes to watch videos through the Xcite and Xvidland glamour portals. User will have access to this content, until he/she unsubscribes."

"Porn Kingz and SexxyMob are both adult VOD services – the same as Xcite and Xvidland."

In addition, the terms and conditions for the Services supplied to the Executive by the Level 2 provider on 7 March 2017 indicated that the Services provided access to online videos and services in exchange for a one-off or regular fee (Memberships).

The Level 2 provider's description of the Service and the Service terms and conditions suggested that the Service operated by providing a facility to access a portal which contained video content.

The Executive noted from complainant message logs and from monitoring conducted by the Executive that a URL, or other means of accessing the Service portal, was not issued to Service subscribers.

The Executive submitted that the evidence therefore indicated that all subscribers incurred Service charges, purportedly to access a video portal service, but without having the means to access the service or its content. The Executive's case was that this failure to provide a facility which allowed all Service subscribers to enter the video portal amounted to the unfair and inequitable treatment of the consumers of the Service.

Accordingly, the Executive submitted that the treatment of consumers had not been fair and equitable, and that a breach of Rule 2.3.1 of the Code had therefore occurred.

2. The Level 2 provider argued that there was a service and that the Executive, when carrying out the monitoring, should have been directed to a content portal but perhaps

moved to a different window on the handset. It asserted that this was not the expected behaviour of a real user. The Level 2 provider supplied a link to a purported portal for the Service.

3. The Tribunal considered the Code and all the evidence, including the terms and conditions for the Service, message logs and the Executive's monitoring report.

It concluded that no link to any portal had been supplied to consumers. The message sent to the Executive in its monitoring journey did not contain a URL to a portal, or any other method of accessing the Service, and neither was there any method of access to the Service demonstrated in the sample of message logs.

There was cogent evidence presented by the Executive, applying the civil standard of proof, that it was more likely than not, that while the Level 2 provider had supplied links to a portal to the Executive in the course of the investigation, these did not demonstrate that subscribers had been given access to them.

The Tribunal therefore concluded that consumers were not treated fairly or equitably and accordingly upheld a breach of Rule 2.3.1.

Decision: Upheld

Alleged breach 4

Paragraph 3.4.14 (a) of the Code

"Level 2 providers must, within two working days of the service becoming accessible to consumers, provide to the PSA relevant details (including any relevant access or other codes) to identify services to consumers and must provide the identity of any Level 1 providers concerned with the provision of the service."

1. The Executive asserted that the Level 2 provider had breached paragraph 3.4.14 (a) of the Code for failing to register Service information with the PSA.

The Executive asserted that the Level 2 provider had breached paragraph 3.4.14 (a) of the Code for failing to register Service information with the PSA.
The Executive relied on the PSA guide on how to register your numbers (the "**Guide**"). The Guide states:

"Why am I registering my numbers?

The Phone-paid Service authority ("PSA") operates a Number Checker service, ensuring that consumers are provided with the most appropriate customer care contact details for any enquiry about a phone-paid service.

This enables anyone to enter a premium rate number ('PRN') onto our website and receive information about that number, such as an appropriate telephone number to call with an enquiry (a customer service phone number).

In order to improve the accuracy and comprehensiveness of the information returned on Number Checker, The PSA launched a new Number Checker service back in 2011 (as part of

the Registration Scheme) which is populated with up-to-date information provided directly by providers. Providers are responsible for registering and maintaining this…

…When must I register all of my numbers by?
All new PRNs must be registered before, or within two working days of, any new phone-paid service going live…

…ADD PAYFORIT ID
A Payforit ID is the PRN generated by the mobile direct billing platform, Payforit. Each Mobile Network generates its own unique Payforit reference for each service.

You must add each Payforit ID as it appears on a consumer's telephone bill, for each Mobile Network. This will allow consumers to identify the service accessed without having to contact the Mobile Network and then the billing platform provider."

The Level 2 provider had informed the Executive that it started taking Service subscribers on 4 August 2016. The Executive noted that the Service had been registered on the PSA Registration Scheme, however the Service had been registered by the Executive after the receipt of complaints about the Service. This was in line with the standard procedure of the Executive so that complaints about an unregistered PRS could be logged appropriately.

The Executive noted that shortcode 65065, which was used by the Level 2 provider as the shortcode by which consumers could send 'STOP' to cease Service subscription charges, was registered on the PSA Registration Scheme but it was a shared shortcode. The information listed alongside this shortcode related to 13 organisations, none of which was the Level 2 provider and there were no details of the Service.

A consumer using the PSA's Number Checker (now called Service Checker) to search for shortcode 65065 would therefore not have received any information about the Level 2 provider or the Service.

The Executive argued that, although the Service STOP shortcode 65065 had been registered on the PSA Registration Scheme, this was of no value to consumers as it did not allow them to access the required information about who had charged them and why.

The Executive submitted that a breach of paragraph 3.4.14 (a) of the Code had occurred.

2. The Level 2 provider denied the breach and argued that it had been registered with the PSA since 27 January 2015. It stated that the Services had been delivered by the Level 1, which was one of the organisations listed against shortcode 65065. It argued that if users required customer support, they could contact the Level 1 provider, which managed its customer enquiries.

3. The Tribunal considered the Code and all of the evidence in relation to this Alleged breach including the documents sent through by the Level 2 provider on 21.9.18 in support of its Judicial Review application.

It acknowledged that the Level 2 provider was registered with the PSA since 27 January 2015. It noted that the Service had been entered onto the Registration Scheme by the Executive. The

Tribunal found that, as the shortcode for the Service was a shared shortcode and not linked to the Level 2 provider or the Service, a consumer using the PSA Number Checker, would not have been able to find out important information about the Service, including which provider had charged them.

Applying the civil standard of proof, the Tribunal concluded that the Level 2 provider had not supplied to the PSA, via the Registration Scheme, relevant details to identify the Service to consumers. Accordingly, it upheld a breach of Paragraph 3.4.14(a) of the Code.

Decision: Upheld

Revenue

The Executive submitted that at least £88,575.60 of the Services' revenue flowed from the apparent Code breaches of Rule 2.2.1 and Rule 2.3.3.

Further, the entirety of the Service revenue, of £234,750.44, flowed from the apparent breach of 2.3.1 given that it appeared Services' subscribers were not provided with the facility to engage with the quiz competition, despite incurring charges.

Sanctions

Initial Assessment

1. The Executive's initial assessment, before any potential adjustment considering aggravating or mitigating features or for proportionality, was that the following sanctions were appropriate:

    - a formal reprimand
    - 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 PSA that such refunds have been made
    - a fine of £850,000, the breakdown being as follows:

      Rule 2.3.3 - £250,000
      Rule 2.2.1 – £250,000
      Rule 2.3.1 – £250,000
      Paragraph 3.4.14(a) – £100,000

      based on a preliminary assessment of breaches as Very Serious.

2. The Level 2 provider did not accept the initial assessment of sanctions. It submitted that the Executive's proposed fine was "grossly disproportionate". It argued that a fine of this magnitude should be reserved for cases where a degree of intent or complicity could be proven and cited the case of *Mobigo Limited* ("***Mobigo***"). It went on to argue that the Executive had arrived at a large figure for a fine by treating each of the Level 2 provider's services as a separate service, notwithstanding that the same issue had affected each of them, thereby increasing the maximum fine potential. It was the Level

2 provider's case that it was the victim of a rogue affiliate and as such, the severity was, at worst, Moderate and the fine should be no more than £20,000.

The Level 2 provider also referred to the case of *Cellso Ltd ("**Cellso**")*, in which a fine of £250,000 had been imposed on a Level 2 provider for a since breach of Rule 2.3.3, where there was no evidence of rogue affiliate activity and the revenue flowing from that service had been over £1.5million. It argued that the Executive's recommendation on the fine amount was disproportionate when compared with *Cellso*.

3. The Tribunal reminded itself that each case presented different case scenarios and the conduct was sometimes nuanced. Each case had to be judged on its own facts. The Tribunal's initial assessment of the breaches of the Code was that they were, overall, Very Serious. In coming to this assessment, the Tribunal found the following:

Rule 2.3.3

- This breach was Very Serious
- The breach was likely to severely damage consumer confidence in PRSs
- Consumers have incurred a wholly unnecessary cost
- The breach was committed intentionally or recklessly.

Rule 2.2.1

- This breach was Very Serious
- The breach was likely to severely damage consumer confidence in PRSs
- There was a considerable impact of consumers being provided with no service information on which to make a free and informed decision before incurring charges.

Rule 2.3.1

- This breach was Very Serious
- The breach was likely to severely damage consumer confidence in PRSs
- The Service was incapable of providing any value to consumers. Consumers had no means of accessing the Service and the Tribunal was of the view that it was unlikely that there was a service at all, given the absolute lack of evidence of any consumer interacting with the Service.

Paragraph 3.4.14(a)

- This breach was Serious
- It had a detrimental impact on consumers who would not have been able to find out which service had charged them
- The breach was likely to severely damage consumer confidence in PRSs
- The breach indicates a wider problem in the procedures and controls of the Level 2 provider.

The Tribunal considered the case of *Mobigo*, in which there had been intentional 'click-jacking, a lack of pricing information and a failure to disclose information requested by the Executive. A

total fine of £250,000 had been imposed in that case, under a previous sanctioning regime. The Tribunal was content that under the new regime, there was a greater emphasis on achieving effective sanctions, including meaningful deterrence. At paragraph 212 of the Supporting Procedures it is made clear that previously imposed financial penalties do not set an upper threshold on the fine that may be imposed on a subsequent case. In any event, the Tribunal did not accept the Level 2 provider's argument that it had been the victim of a rogue affiliate. The breaches of Rules 2. 2.3, 2.2.1 and 2.3.1 were found to have been either intentional or due to such recklessness that they amounted to the same level of culpability.

The Tribunal also considered the case of Cellso. The Tribunal noted that the Tribunal in that case had remarked that, "*it would likely have imposed a substantially higher fine in this case had it not been for the limitation imposed by the statutory maximum fine amount, which in this case was £250,000.*" The Tribunal did not consider that the case assisted in its initial assessment of the fine.

The Tribunal acknowledged that here, there was some overlap between the breaches of Rules 2.3.3 and 2.2.1 and would take that into account when considering totality and proportionality. It was of the view that, while there was some overlap, the breaches were quite distinct and focused on particular types of conduct. It followed that it was appropriate for them to be alleged separately.

Based on its initial assessment of the severity of the breaches, the Tribunal considered that the following sanctions were appropriate and proportionate:

- a formal reprimand
- a prohibition on the Level 2 provider from providing, or having involvement in, any PRS for a period of five years, starting from the date of publication of the Tribunal decision, or until payment of the fine and administrative charges, whichever is the later
- a general refund
- a fine of £850,000, comprised of £250,000 on each of breaches 2.3.3, 2.2.1, 2.3.1 and £100,000 on the breach of 3.4.14(a).

Assessment of mitigating and aggravating factors

1. The Executive noted that refunds had been provided to some consumers, although these had been made by DMB and Dimoco as well as the mobile network operators.

The Executive submitted that the following were aggravating factors:

- the Level 2 provider had failed to follow PSA Guidance
- the Level 2 provider must have been aware of the 'click-jacking' on its payment pages as it was on its own website. The Executive therefore argued that the breaches continued after the provider became aware of them.
- The Executive considered the Level 2 provider to have supplied contradictory and potentially confusing information to it during the investigation as it stated on one occasion that it did not engage affiliates but subsequently blamed affiliates for the 'click-jacking' exploit

- The promotion of the Service was suspended in October 2016, but billing of subscribers continued until January 2018, when it was suspended by the Level 2 provider.

2. The Level 2 provider submitted that the following mitigating factors were present:

    - It had refunded consumers who had requested a refund. These refunds amounted to more than £150,000.
    - It had engaged two compliance monitoring specialists: Empello and MCP
    - It took steps to close the Service after "falling victim to the click-jacking attack".

3. The Tribunal found that the 'click-jacking' being hosted on the Level 2 provider's own website was already part of the narrative of the case and did not consider this to be a separate aggravating feature. It accepted that the remainder of the aggravating factors identified by the Executive were present.

The Tribunal accepted that some refunds had been made. It did not consider the instruction of the two compliance specialists to be a mitigating factor, given the, at the very least, reckless breaches of Rules 2.3.3 and 2.2.1 and the lack of robust monitoring by either Empello or MCP.

The Tribunal did not accept that the Level 2 provider had been the victim of a rogue affiliate.

Having considered the circumstances of the case, the Tribunal concluded that it should be regarded, overall, as Very Serious.

Financial benefit/need for deterrence

1. The Executive had submitted that the entirety of the Service revenue had flowed from the breaches in the case (at least £53,830.40 in relation to breaches 2.2.1 and 2.3.3 and the full revenue of £318,192.73 in relation to the breach of 2.3.1). It argued that there was a need to remove this financial benefit as the Level 2 provider should not benefit from its non-compliant conduct. Further it was submitted that there was a need to deter the commission of such breaches by the Level 2 provider and others in the wider industry in future.

2. The Level 2 provider submitted that the Executive's conclusions as to the revenue stemming from the breaches was flawed. It argued that the number of consumers impacted was significantly lower. It also referred to the refunds that had already been paid and the costs it had incurred when beginning judicial review proceedings in relation to the interim measures.

3. The Tribunal accepted the Executive's calculation of the revenue flowing from the breaches. It had already found that the number of consumers affected was 4160. The Tribunal decided that it was necessary to remove the financial benefit made as a result of the breaches and a need to prevent the reoccurrence of such breaches by the Level 2 provider, as well as those in the wider industry. The Tribunal acknowledged that the fine amount in its initial assessment exceeded the revenue held to have flowed from the breaches and that the imposition of any fine would have a financial impact on the

Level 2 provider. It also considered that there was a need for a punitive element to the sanctions, given the widespread harm and the continued billing of consumers when there was clearly no service being provided.

Sanctions adjustment

The Tribunal determined that it was appropriate to reduce the fine amount to ensure that it was proportionate. In doing so, it considered the overlap between breaches 1 and 2 as well as the revenue generated by the Service. The Tribunal also considered the overlap with other services provided by the Level 2 provider. The Executive had discovered, in the course of its monitoring, six services, all provided by the Level 2 provider, which had an iFrame over their payment pages. The Level 2 provider had argued that to separate the services into three cases as it did was unfair, and artificially increased the maximum fine potential. The PSA Code Rules refer to individual PRSs and as such, it was open to the Executive to bring each of the six services to the Tribunal separately. The Tribunal was of the view that there were six separate services, across three service types, with separate and distinct consumer harm; however, it noted that there was an overlap of the method of promoting the services. The Tribunal did not accept that the separation into three cases for the purposes of the hearing was inherently unfair or motivated by increasing the fine levels. However, conducting a balancing exercise and importantly, the principle of proportionality, the Tribunal would ensure that the overlap between not only the breaches within each case, but also the separate service methods, was reflected in its final decision on sanctions.

Final sanctions

Having regard to all the circumstance of the case, including that there was some overlap between the breaches of the Code raised, the Tribunal decided to impose the following sanctions:

- a fine of £350,000 (comprised of £100,000 on each of breaches 2.3.3, 2.2.1, 2.3.1 and £50,000 on the breach of 3.4.14(a))
- a formal reprimand
- a prohibition on the Level 2 provider from providing or having any involvement in any PRS for a period of five years from the date of the Tribunal decision or until payment of the fine and administrative charges, whichever is the later
- 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 PSA that such refunds have been made .

Administrative charge recommendation **100%**