

## THE CODE COMPLIANCE PANEL OF PHONEPAYPLUS TRIBUNAL DECISION

Thursday 10 May 2012  
TRIBUNAL SITTING No. 99 / CASE 1  
CASE REFERENCE: 04578

Level 2 provider: A1 Agregator Limited  
Type of service: In-app billing/ Android Trojan app  
Level 1 provider: Ericsson Internet Payment Exchange AB  
Network operator: Mobile Network Operators

### THIS CASE WAS BROUGHT AGAINST THE LEVEL 2 PROVIDERS UNDER PARAGRAPH 4.4 OF THE CODE

#### BACKGROUND

In December 2011, the Executive received 34 complaints from members of the public in relation to unknown charges being triggered after downloading apps advertised as “free”. The apps were replicas of popular games and entertainment services, such as ‘Angry Birds’ and ‘Cut the Rope’. The replica apps were developed to include coding, which triggered the sending of text messages from the users’ handsets to a premium rate number. In response the Level 2 provider’s system sent premium rate messages to the users at a cost of £5 each. The charges continued to be triggered until users uninstalled the replica app from their phone. The replica apps also appeared to restrict visibility of incoming and outgoing messages associated with the shortcode 79067, this resulted in complainants not being aware of charges until receipt of their phone bills.

The Executive observed research on the internet that documented similar incidents to those described by the complainants. The research had been conducted by F-secure.com (“**F-secure**”), TotalDefence.com (“**Total Defence**”) and Lookout Mobile Security. The research provided by F-secure and Total Defence was of particular assistance as it included screenshots which documented the use of shortcode 79067 in Trojan apps similar to those described in the complaints.

The Level 1 provider, Ericsson Internet Payment Exchange AB, who holds the relevant shortcode – 79067, identified the Level 2 provider as being A1 Agregator Limited (“**A1 Agregator**”). At the time of investigation the Level 2 provider had not completed its registration with PhonepayPlus.

#### The Investigation

The Executive conducted this matter as a Track 2 procedure investigation in accordance with paragraph 4.4 of the PhonepayPlus Code of Practice 12<sup>th</sup> Edition (“**the Code**”).

The Executive sent a breach letter to the Level 2 provider on 13 April 2012. Within the breach letter the Executive raised the following potential breaches of the Code:

- Rule 2.3.2- Misleading;
- Rule 2.3.3- Charges without consent;
- Rule 2.2.5- Pricing;
- Paragraph 3.1.4- Directions and requests;
- Paragraph 3.4.1- Registration; and,
- Paragraph 3.1.1(b)- General responsibilities

The Level 2 provider responded on 30 April 2012. On 10 May 2012, and after hearing informal representations from the Level 2 provider, the Tribunal reached a decision on the breaches raised by the Executive.

## **SUBMISSIONS AND CONCLUSIONS**

The Tribunal accepted that A1 Agregator was the Level 2 provider.

### **ALLEGED BREACH ONE**

#### **Rule 2.3.2**

*“Premium rate services must not mislead or be likely to mislead in any way.”*

1. The Executive observed from the complaints that consumers had downloaded apps described as “free” from Android app marketplaces. The complainants stated that pricing information was not included in any promotional material they had viewed. The complainants stated that they did not see any incoming or outgoing messages on their phones. In some instances, the complainants suggested that there was a link between an app they had downloaded and the charges being triggered.

The Executive submitted that the occurrences described in the complaints were supported by the F-secure report.

The Executive submitted that the apps appeared to have been designed so as to include a Trojan, which resulted in charges being levied from consumers. The promotions for the apps did not appear to explain the cost of the service and instead advertised the apps as being “free”. The Executive maintained that consumers appeared to have been misled into downloading the apps in the belief that they were “free”, only to be charged £5 per text message received from shortcode 79067. This shortcode was allocated to the Level 2 provider.

2. The Level 2 provider did not dispute the breach had occurred in its correspondence or orally during its informal representations. The Level 2 provider stated that the apps were created by its partner, a Russian organisation named Mobile Technologies Limited. It was submitted that the partner organisation used “prefixes” obtained from the Level 2 provider to promote malware without their knowledge. On discovering the service did not correspond to the services it had approved, the Level 2 provider stated that it had blocked the service, stopped relations with the provider and withheld payment.

During informal representations, the Level 2 provider further submitted that its directors and personnel had been replaced as a result of previous irregularities. However, going forward, the Level 2 provider was committed to sound compliance

with the Code. To this end, the Level 2 provider stated that it had made refunds to all complainants brought to its attention, introduced strict compliance measures and put in place methods for both internal and external scrutiny of all parts of its business.

3. The Tribunal considered the evidence and noted the Level 2 provider did not dispute the breach but did dispute that they were responsible. The Tribunal noted the position but concluded that they were responsible under the Code. On the basis of the Executive's submissions and the apparent admission by the Level 2 provider, the Tribunal concluded that consumers were misled into believing that downloading the app would not result in any charges. The Tribunal upheld a breach of rule 2.3.2 of the Code.

**Decision: UPHELD**

## **ALLEGED BREACH TWO**

### **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 submitted that the complainants had downloaded apps from Android app marketplaces believing them to be free of charge. The complainants stated that the apps were described as "free" and no further pricing information was included in any promotional material they viewed.

The Executive referred to screenshots provided by F-secure and Total Defence which appeared to support the complainants' accounts. The Executive submitted that the apps appeared to have been designed so as to include a Trojan to trigger text messages resulting in charges being incurred by consumers. It was submitted that without knowledge of these charges, which had been triggered automatically by the apps, the consumer was unable to provide consent for the charges.

In addition, the Executive relied upon a report from Total Defence, which stated: *"In order to avoid the infected victim getting alerted by any response messages, the Trojan also registers an SMS receiver that intercepts the messages coming from the specific numbers and interrupts them from reaching the victim's inbox"*.

The Executive alleged that the evidence appeared to show a deliberate attempt to hide pricing information and also restrict the consumer's awareness of charges for as long as possible. Therefore, consumers were not in a position to consent to the charges.

2. The Level 2 provider did not dispute the breach. The Level 2 provider did not address the alleged breach specifically but supplied the general response as outlined in respect of rule 2.3.2 of the Code.
3. The Tribunal considered the evidence and noted the Level 2 provider did not dispute the breach but did dispute that they were responsible. The Tribunal noted the position but concluded that they were responsible under the Code. On the basis of the Executive's submissions and the apparent admission of the breach by the Level 2 provider, the Tribunal concluded that consumers were not made aware of any charges and had therefore been charged for premium rate services without their consent. Accordingly, the Tribunal upheld a breach of rule 2.3.3 of the Code.

**Decision: UPHELD**

## ALLEGED BREACH THREE

### Rule 2.2.5

*“In the course of any promotion of a premium rate service, written or spoken or in any medium, the cost must be included before any purchase is made and must be prominent, clearly legible, visible and proximate to the premium rate telephone number, shortcode or other means of access to the service.”*

1. The Executive submitted that the complainants had downloaded apps from Android app marketplaces believing them to be free of charge. The complainants stated that the apps were described as “free” and no further pricing information was included in any promotional material they viewed.

The Executive referred to screenshots provided by F-secure and Total Defence which appeared to support the complainants’ accounts. The report from Total Defence showed a screenshot taken from an Android app marketplace labelled: “*Fig 1: Permissions that must be granted by the victim for the Trojan to get installed*”. The screenshot showed one permission request stating, “*Services that cost you money – send SMS messages*”. However, this does not fully and/or clearly inform the consumer of the cost of the service.

In addition, the report from Total Defence stated: “*In order to avoid the infected victim getting alerted by any response messages, the Trojan also registers an SMS receiver that intercepts the messages coming from the specific numbers and interrupts them from reaching the victim’s inbox*”.

The Executive alleged that the evidence appeared to show a deliberate attempt to hide pricing information and also restrict consumers’ awareness of charges for as long as possible.

In addition, the Executive stated that the Level 2 provider had failed to provide promotional material and details of the coding found in the APK File, which had limited the scope of the investigation.

Accordingly, the Executive submitted that the complainant evidence, supported by the reports made in relation to the Trojans associated with shortcode 79067, illustrated that the service operated in breach of rule 2.2.5 of the Code.

2. The Level 2 provider did not dispute the breach. Save for stating that there was no deliberate attempt to hide pricing information, the Level 2 provider did not address the alleged breach specifically but supplied the general response as outlined in respect of rule 2.3.2 of the Code.
3. The Tribunal considered the evidence and noted that the Level 2 provider did not dispute the breach but did dispute that they were responsible. The Tribunal noted the position but concluded that they were responsible under the Code. On the basis of the Executive’s submissions and the apparent admission that the breach had occurred by the Level 2 provider, the Tribunal upheld the breach of rule 2.2.5 of the Code.

**Decision: UPHELD**

## ALLEGED BREACH FOUR

### Paragraph 3.1.4

*“All Network operators, Level 1 and Level 2 providers must... act on any direction, instruction, notice or request for information given by PhonepayPlus in pursuance of its duties as a regulator. Where PhonepayPlus specifies a timeframe for action or response that timeframe must be adhered to or an extension promptly requested in writing setting out clear reasons. Any such extension will be granted only in exceptional circumstances.”*

1. The Executive outlined the following:

On 14 March 2012, the Executive issued a letter to the Level 2 provider making 11 specific requests for information. The letter explicitly warned that: *“[F]ailure to supply the information specified above may result in a breach of paragraph 3.1.4 and/or 4.2.5 of the Code being upheld against you”*. The deadline set for a full response was 22 March 2012. The Executive submitted that the response to the letter was sent in a piecemeal fashion over a period of seven days from 20 to 27 March 2012.

After some information had been supplied in emails dated 20 March and 21 March, the Executive sent an email, dated 22 March, notifying the Level 2 provider that some information had not been disclosed as requested. It stated: *“Please note that I still consider more information is necessary in relation to questions 1, 4, 7, 10, and 11...Considering the missing information in the round, the Executive is concerned that this app was developed by The Level 2 provider staff and not a partner as suggested. The Executive is concerned that this Trojan was used with the intention to generate large amounts of revenue for A1 Agregator.”*

The Executive reminded the Level 2 provider of the need for: *“[A]ll the information requested in my letter dated 14 March [to be] provided by the end of today”*.

However, no additional information was supplied, except for some additional data relating to message logs. The Executive submitted that this information did not address the concerns mentioned above or fulfil the request made on 14 March 2012.

The Executive submitted that the failure to supply the necessary information had limited the scope of PhonepayPlus’ investigation and left a number of assertions made by the Level 2 provider without any supporting evidence. As a result the Level 2 provider had breached paragraph 3.1.4 of the Code.

2. In its response to the breach letter dated 24 April 2012, the Level 2 provider submitted that it provided all the required information on time. In informal representations the Level 2 provider stated that it did not dispute any of the breaches. It was stated that the directors and personnel at the Level 2 provider were replaced three weeks ago and previous to this date there was an issue with the length of time taken to respond to correspondence.

3. The Tribunal considered the evidence, including the Level 2 provider’s submissions. The Tribunal concluded that the Level 2 provider had not provided an adequate response to the Executive’s request, and in particular had not responded to its further email correspondence dated 22 March 2012. The Tribunal noted that the responses received had not been complete and further requests for information had not been adequately dealt with. The Tribunal upheld the breach of paragraph 3.1.4 of the Code.

**Decision: UPHELD**

**ALLEGED BREACH FIVE**

**Paragraph 3.4.1**

*“Before providing any premium rate services all Network operators, Level 1 and Level 2 providers must register with PhonepayPlus subject only to paragraph 3.4.3 below.”*

1. The Executive submitted that the Level 2 provider was notified of the obligation to register on five occasions between 24 June 2011 and 22 December 2011. The registration of the Level 2 provider was not completed until 1 February 2012, five months after the 12<sup>th</sup> Edition of the Code came into force. Message logs demonstrated that the Level 2 provider had operated premium rate services between 1 September 2011 and 31 January 2012.
2. In its written responses, the Level 2 provider submitted that it had received the notification to register on 22 July 2011 and registered itself with PhonepayPlus on 29 July 2011. The Level 2 provider stated it had made several attempts to complete the “last step” and pay the registration fee by credit card. It submitted that it had requested assistance from PhonepayPlus. On 30 September 2011 the Level 2 provider was advised to try a different browser for payment. This was unsuccessful. After further correspondence, PhonepayPlus issued an invoice to be paid by bank transfer in January 2012. By this time the Level 2 provider had obtained a different credit card and paid the registration fee by February 2012.

During its informal representations, the Level 2 provider stated that it did not dispute and fully accepted all of the breaches. However, in relation to this breach, the Level 2 provider maintained it did register with PhonepayPlus on time and only the payment failed. It was alleged that this was a lapse of administration. However it was accepted that payment should have been followed up in September 2011.

3. The Tribunal considered the evidence, including the Level 2 provider’s submissions. The Tribunal concluded that, on the facts of the case, the Level 2 provider had provided premium rate services before completing the registration process. The Tribunal noted the difficulties encountered by the Level 2 provider but considered that the steps they had taken were neither timely nor adequate to deal with the problem. Accordingly, the Tribunal upheld the breach of paragraph 3.4.1 of the Code.

**Decision: UPHELD**

**ALLEGED BREACH SIX**

**Rule 3.1.1(b)**

*“All Network operators, Level 1 and Level 2 providers must... ensure that PhonepayPlus regulation is satisfactorily maintained by... carrying out their own obligations under the Code promptly and effectively.”*

1. The Executive submitted that PhonepayPlus emailed the Level 2 provider’s primary contact on five occasions to request that they complete the registration. The correspondence stated: “[O]nce you have validated your data and paid the fee, your PhonepayPlus number will be: ORG828-36516-57730”.

The registration of the company was not completed until 1 February 2012, five months after the new 12<sup>th</sup> Edition of the Code came into force.

The Executive contended that the Level 2 provider was notified of its obligations on 24 June 2011, but did not carry out those obligations under the Code promptly and effectively. The Executive submitted that as a result the Level 2 provider was in breach of paragraph 3.1.1(b) of the Code.

2. The Level 2 provider made the same submissions as those outlined in respect of paragraph 3.4.1.
3. The Tribunal considered the evidence. The Tribunal concluded that the breach had been properly raised by the Executive, but on the particular facts of the case it considered that it was not appropriate to uphold the breach as the mischief had been sufficiently addressed under paragraph 3.4.1 above. Accordingly, the Tribunal exceptionally decided not to uphold a breach of paragraph 3.1.1(b) of the Code.

**Decision: NOT UPHELD**

## **SANCTIONS**

### **Initial Overall Assessment**

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

#### **Rule 2.3.2- Misleading**

The initial assessment of rule 2.3.2 of the Code was **very serious**. In determining the initial assessment for this breach of the Code the Tribunal applied the following criterion:

- The service was designed with the specific purpose of generating revenue streams for an illegitimate reason.

#### **Rule 2.3.3- Charges without consent**

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 criterion:

- The service was designed with the specific purpose of generating revenue streams for an illegitimate reason.

#### **Rule 2.2.5 – Pricing transparency**

The initial assessment of rule 2.2.5 of the Code was **very serious**. In determining the initial assessment for this breach of the Code the Tribunal applied the following criterion:

- The service was designed with the specific purpose of generating revenue streams for an illegitimate reason.

#### **Paragraph 3.1.4- Directions and requests**

The initial assessment of paragraph 3.1.4 of the Code was **serious**. In determining the initial assessment for this breach of the Code the Tribunal applied the following criterion:

- The Level 2 provider had negligently and/or repeatedly failed to comply with a PhonepayPlus requirement, which had a detrimental impact on the investigation and enforcement of the Code.

### **Paragraph 3.4.1- Registration**

The initial assessment of paragraph 3.4.1 of the Code was **serious**. In determining the initial assessment for this breach of the Code the Tribunal applied the following criterion:

- The Level 2 provider has negligently and/or repeatedly failed to comply with a PhonepayPlus requirement, over a five month time period.

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

### **Final Overall Assessment**

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

- The Level 2 provider failed to follow guidance issued in relation to registration.
- The Level 2 provider continued to be in breach of registration requirements after notification of breaches by PhonepayPlus.

The Tribunal noted the assurances given by the Level 2 provider in relation to future compliance. However, the Tribunal concluded that there were no mitigating factors.

The revenue in relation to this service was in the mid range of Band 5 (£5-50,000).

Having taken into account the aggravating factors, 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, the Tribunal decided to impose the following sanctions:

- A formal reprimand;
- A fine of £50,000;
- A requirement for the Level 2 provider to submit all premium rate services to PhonepayPlus for prior permission for 12 months; and,
- A requirement that the Level 2 provider make refunds, within three months, to all consumers who have used the service for the full amount spent, regardless of whether or not they have claimed a refund. Refunds should be directly credited to the users' mobile accounts and the Level 2 provider must provide evidence to PhonepayPlus that the refunds have been made.